

Digital intelligence and international relations: strategic mechanisms and global power dynamics

Review of
Economics and
Political Science

Alshaimaa Mohamed Mahmoud Hassan

*Department of Public Law, College of Law, King Faisal University,
Al-Ahsa, Saudi Arabia*

Received 5 August 2025
Revised 10 January 2026
8 March 2026
Accepted 4 May 2026

Abstract

Purpose – This article aims to examine how national digital intelligence capacity is translated into foreign-policy-relevant crisis governance through three mechanisms – crisis anticipation, policy coordination and external signalling. It addresses a research puzzle: Why Egypt and Saudi Arabia, two regional powers facing comparable digital interdependence, display divergent patterns of anticipatory crisis governance and external digital influence?

Design/methodology/approach – The article develops a mechanism-oriented conceptual framework that draws selectively on established international relations concepts related to strategic competition, institutional coordination and digital sovereignty. It applies a structured, focused comparison of Egypt and Saudi Arabia, drawing on cross-national indices (artificial intelligence (AI) readiness, GovTech maturity, cybersecurity capacity and global AI benchmarks) alongside publicly available national strategies and institutional arrangements as contextual indicators rather than as tools for hypothesis testing or causal inference.

Findings – Higher digital intelligence capacity is associated with stronger early-warning routines, tighter coordination and greater capacity to mobilise digital infrastructures for diplomatic signalling; outcomes vary with institutional centralisation and data-governance practices.

Research limitations/implications – The framework is theory-driven and exploratory. It relies on composite indices and author-generated profiles rather than on micro-level process tracing or longitudinal data, which limits the scope for strong causal inference. Future research could operationalise the proposed mechanisms in within-case and time-series designs.

Practical implications – The framework helps Global South policymakers identify where digital intelligence investments strengthen anticipatory crisis governance and where governance gaps erode strategic gains.

Originality/value – The article specifies digital intelligence capacity as an information retrieval-relevant capability bundle and traces mechanisms linking digital readiness to foreign-policy-relevant crisis governance in a Middle East comparison.

Keywords Digital intelligence, Crisis governance, Digital sovereignty, Cyber power, Algorithmic governance, Saudi Arabia, Egypt, Global South, Geo-digital divide

Paper type Research article

1. Introduction

The accelerating integration of digital technologies into state governance challenges conventional International Relations approaches centred on material power and reactive decision-making. While existing theories recognise technological change as contextual, they remain limited in explaining how digitally mediated capacities translate into foreign-policy behaviour under conditions of crisis and strategic uncertainty.

Recent scholarship has highlighted the growing political significance of artificial intelligence, big data analytics, and cyber infrastructures for power projection, institutional coordination, and global governance. Yet much of this literature remains technologically

© Alshaimaa Mohamed Mahmoud Hassan. Published by Emerald Publishing Limited. This article is published under the Creative Commons Attribution (CC BY 4.0) licence. Anyone may reproduce, distribute, translate and create derivative works of this article (for both commercial and non-commercial purposes), subject to full attribution to the original publication and authors. The full terms of this licence may be seen at <http://creativecommons.org/licences/by/4.0/>

Funding: This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Grant No. KFU254799).



Review of Economics and Political
Science
Emerald Publishing Limited
e-ISSN: 2631-3561
p-ISSN: 2356-9980
DOI 10.1108/REPS-08-2025-0083

descriptive or normatively oriented, often treating digital capacity as a background condition rather than as an analytically specified component of statecraft—particularly in Global South contexts marked by institutional fragmentation and contested sovereignty.

Accordingly, this article is organised around a research puzzle: despite comparable regional ambitions and exposure to shared patterns of digital interdependence, Egypt and Saudi Arabia exhibit divergent trajectories in anticipatory crisis governance—especially in early-warning practices, inter-agency coordination, and external digital signalling—and, consequently, different capacities to translate digital readiness into foreign-policy-relevant influence. Existing International Relations scholarship offers no clear explanation for why similar levels of technological exposure generate such differentiated strategic outcomes.

Rather than advancing a unified theoretical model, this article adopts a conceptual framework that draws selectively on established International Relations concepts. Concepts such as strategic competition under anarchy, institutional coordination, and digital sovereignty are employed as analytical reference points to interpret state behaviour in digitally mediated crisis governance, without extending these concepts into a formal or predictive theory.

The central question guiding the analysis is therefore: under what governance and sovereignty conditions does digital intelligence capacity become a strategic mechanism shaping anticipatory crisis governance and foreign-policy behaviour, rather than remaining a predominantly technical modernisation project? To address this question, the article traces three observable governance mechanisms: crisis anticipation, policy coordination, and external signalling.

Empirically, the article applies a structured, focused comparison of Egypt and Saudi Arabia, drawing on cross-national indices of AI readiness, GovTech maturity, and cybersecurity capacity alongside publicly available national strategies and institutional arrangements. These sources are used as contextual

indicators rather than as quantitative data for hypothesis testing or causal inference, supporting an analytically transparent, Global South-centred comparative perspective.

2. Literature review and conceptual foundations

Over the past decade, the rise of digital technologies has profoundly transformed the landscape of international relations. However, traditional IR theories—including realism, liberalism, and constructivism—have shown limitations in capturing the implications of data-driven governance, algorithmic influence, and cyber power in shaping foreign policy and strategic interaction. While early works addressed the role of communication technologies in public diplomacy, more recent studies have begun to consider the structural impact of artificial intelligence, big data, and cyber systems on global power configurations (Nye, 2020, p. 27; Choucri, 2021, pp. 33–34).

Recent literature has emphasised the strategic role of digital intelligence—defined as the integration of big data analytics, algorithmic automation, and real-time decision-making capabilities—in enhancing states' abilities to predict crises, shape strategic environments, and project influence (Kello *et al.*, 2022, p. 71). Scholars increasingly examine how informational capabilities function as levers of soft power, legitimacy, and strategic agency. Yet, despite these advancements, the literature remains fragmented and under-theorized in connecting digital intelligence to the foundational constructs of international relations, particularly with respect to power dynamics in the Global South (Nye, 2020, p. 30; Choucri, 2021, p. 38).

Recent International Relations scholarship increasingly treats digital infrastructures and cross-border data flows as arenas of power, dependence, and strategic contestation, where network position can be translated into coercive leverage and asymmetrical interdependence. This perspective aligns with work showing how states can weaponize networked structures of interdependence to gain strategic advantage in the cyber-information domain (Farrell and Newman, 2019, pp. 43–47) and with analyses that locate internet governance within broader struggles over authority and geopolitical control (DeNardis, 2014, pp. 1–3, 7–8).

A second strand examines algorithmic governance and the international politics of Big Tech, highlighting how platform-based authority shapes agenda-setting, policy autonomy, and rule-making across borders. Here, algorithmic governance is treated not as a purely technical issue but as an international political problem tied to transnational corporate power and the externalisation of regulatory constraints (Srivastava, 2023, pp. 989–992).

A third debate focuses on digital sovereignty as a set of practices through which states seek control over data governance, localisation, and standards, often through infrastructural and regulatory strategies that reassert state authority in digital space. This strand emphasises sovereignty as “infrastructured” practice and highlights the politics of standards and architectures that condition autonomy (Musiani, 2022, p. 787). Alongside security-driven approaches to “cyber sovereignty” as a strategic doctrine in international politics (Topor, 2024, pp. 45–73). Complementing these approaches, recent work on polycentric data governance underscores how rule-making is distributed across overlapping institutions and actors rather than a single hierarchical regime (Aguerre *et al.*, 2024, pp. 101–128). While legal–political debates on the nature of data (as economic good vs commons) illuminate why governance choices carry distributive and power consequences (Purtova and van Maanen, 2024, pp. 1–42).

For Global South states, these dynamics intersect with asymmetric technological dependencies and what critical scholarship describes as data colonialism, producing geo-digital asymmetries that shape room for manoeuvre and constrain strategic autonomy (Coudry and Mejias, 2019, pp. 1–2).

Against this backdrop, the article grounds its three mechanisms in adjacent, IR-relevant bodies of scholarship: crisis governance research on coordination under uncertainty, strategic warning studies on anticipatory failure and early-warning translation, and signalling theory on externally oriented crisis messaging.

Building on this definition, rather than proposing a grand, unified theory, this article adopts a conceptual and mechanism-oriented framework that draws selectively on established International Relations concepts. These concepts are used as analytical reference points to interpret how digital intelligence capacity is mobilised in crisis governance and are employed heuristically to trace governance mechanisms—crisis anticipation, policy coordination, and external signalling—without being integrated into a formal explanatory or predictive theory.

Insights associated with structural realism highlight how states may seek informational and organisational advantages under conditions of anarchy, suggesting that digital capabilities can shape crisis-related positioning (Waltz, 1979, p. 121). Institutional liberalism draws attention to how digital infrastructures and platforms structure cooperation, rule-making, and norm diffusion in governance arenas (Keohane and Nye, 2001, pp. 45–48). Digital sovereignty scholarship conceptualises control over infrastructures, data, and standards as a practical extension of state authority (Musiani, 2022, pp. 785–800; Topor, 2024, pp. 1–20). Together, these concepts function as complementary analytical lenses for tracing mechanisms—rather than competing hypotheses or a causal model—in the Egypt–Saudi comparison.

In operational terms, these perspectives function as complementary lenses that structure a mechanism-oriented analysis rather than a causal model. The Egypt–Saudi comparison is used to trace how digital intelligence capacity may shape crisis anticipation, policy coordination, and external signalling through governance arrangements, institutional cooperation, and sovereignty practices, without claiming statistically confirmed causal effects.

In this article, digital intelligence capacity refers to the state’s ability to govern and mobilise relevant data, sustain analytical and computational infrastructures, coordinate institutions for timely crisis interpretation and response, and maintain cyber and information-security resilience in ways that are foreign-policy relevant.

3. Methodology

This article adopts a descriptive–analytical and comparative research design. The methodological approach is structured around three main components: conceptual framing, comparative case analysis, and the use of cross-national indicators as contextual sources.

For clarity, this article uses four terms in an IR-specific sense. Digital intelligence capacity refers to the state's ability to access relevant data, analyse it, and embed analytics into institutional workflows for crisis governance and foreign-policy support. Anticipatory crisis governance denotes early-warning and forecasting routines, rapid coordination procedures, and decision-cycle compression during shocks. Geo-digital asymmetry captures unequal dependencies on external platforms, cloud infrastructures, and standards that shape states' room for manoeuvre. Localisation strategies refer to governance and regulatory measures—such as data localisation, national platform rules, and cybersecurity policies—through which states seek greater autonomy over infrastructures, data, and standards.

To delimit the scope of analysis, the article draws primarily on two categories of crises with direct foreign-policy relevance: transnational public health crises (such as pandemics) and strategic economic disruptions (such as major trade or logistics shocks). These crisis types differ not only in temporal horizons and coordination demands, but also in the foreign-policy decision pathways they activate—for example, Egypt's pandemic response relied on international health coordination and information-sharing, whereas disruptions such as the Suez Canal blockage triggered digitally mediated economic signalling and crisis diplomacy.

3.1 Conceptual framework

This article adopts a descriptive–analytical and comparative research design, operationalised as a structured-focused comparison. It is conceptual and mechanism-oriented: it uses secondary indicators and policy documents to build comparable national profiles of digital intelligence capacity and to assess how that capacity is plausibly linked to crisis-governance and foreign-policy mechanisms. The design does not claim statistical causal inference or original data collection; instead, it provides an analytically transparent framework that can be tested in future work.

3.2 Case selection

The article adopts a comparative case analysis of two influential emerging economies in the Global South: Egypt and Saudi Arabia. These countries show significant variation in digital infrastructure investment, policy frameworks, and AI readiness, yet share regional proximity, geopolitical relevance, and strategic aspirations.

Egypt and Saudi Arabia are selected as most-relevant cases because they share key background conditions—regional ambitions, exposure to the same digital interdependence, and comparable pressures of Global South dependency—while differing in the institutional centralisation and sovereignty strategies through which digital intelligence capacity is governed. This “most-similar systems” logic is used not to infer causality, but to sharpen mechanism-tracing: observable divergence under broadly comparable constraints helps identify the institutional pathways and sovereignty practices that condition whether digital intelligence translates into anticipatory crisis governance and external digital influence.

3.3 Data sources and indicators

The analysis is based on several validated datasets. First, the Government AI Readiness Index by Oxford Insights provides a baseline measure of national digital preparedness. Second, the [World Bank's GovTech Maturity Index \(2022\)](#) evaluates institutional capacity for digital service delivery. Third, the National Cybersecurity Index (produced by the e-Governance Academy) assesses cyber resilience. Fourth, the Digital Economy and Society Index offers regional benchmarking insights. These are complemented by additional data from national digital strategy documents, United Nations Development Program datasets, and the World Bank's governance indicators. Together, these sources allow for a multidimensional assessment of digital readiness, institutional modernisation, and strategic adaptability.

3.4 Analytical strategy

This article does not employ a formal causal model based on independent, dependent, and control variables. Instead, it adopts a mechanism-oriented analytical design commonly used in International Relations scholarship, relying on analytical dimensions and observable governance mechanisms rather than formal independent and dependent variables. Digital intelligence capacity is treated as an analytical condition, while crisis anticipation, policy coordination, and external signalling are examined as observable governance mechanisms in relation to foreign-policy-relevant behaviour.

The Egypt–Saudi comparison is conducted through a structured, focused comparison in which the same analytical questions are applied to both cases to examine how digital intelligence capacity is reflected in crisis governance that bears on foreign-policy decision-making. Cross-national indices (AI readiness, GovTech maturity, cybersecurity capacity and global AI benchmarks) are used as descriptive proxies to map relative digital capabilities; however, the analysis does not infer causation from scores alone. Rather, it triangulates these proxies with publicly available national strategies and institutional arrangements to trace three IR-relevant mechanisms: crisis anticipation (early-warning and forecasting routines), policy coordination (inter-agency integration and decision workflows), and external signalling (the mobilisation of digital tools and narratives for diplomatic messaging and strategic positioning). The contribution is therefore analytical: it explains how, and under what governance conditions, digital intelligence capacity is examined in crisis-time foreign-policy behaviour while explicitly acknowledging limits to causal inference.

Operationally, the comparison applies the same analytical questions to both cases by tracing how data and analytics are channelled into crisis decision-making through institutional pathways, how governance arrangements enable or constrain inter-agency coordination in practice, and how digital capabilities and associated narratives are mobilised for external diplomatic signalling during foreign-policy-relevant shocks.

3.5 Limitations of data and design

This article examines digital intelligence as a bundled state capability—combining data infrastructures, analytics capacity, institutional arrangements and cyber governance—through a descriptive–analytical, structured comparison of Egypt and Saudi Arabia. To contextualise enabling conditions for digital intelligence, the analysis draws on composite cross-national indices that capture adjacent capability domains (e.g. digital government/GovTech maturity, national cybersecurity capacity and AI-readiness as a partial proxy for analytics preparedness) alongside publicly available secondary sources and official policy materials. Because such indicators are multi-component and in part perception-based, they may entail measurement error, uneven country coverage and time-lagged updates; moreover, they register broad capacity signals rather than micro-level crisis routines, informal coordination practices or within-crisis decision sequences. Accordingly, index scores are treated as contextual proxies, and are triangulated with national strategies and institutional arrangements to strengthen the empirical grounding of the mechanism discussion. Within these scope conditions, the comparative analysis remains mechanism-oriented and conditional: it specifies how governance configurations (institutional centralisation, data governance and localisation practices) are associated with variation in the observable pathways emphasised in the article—crisis anticipation, policy coordination and external signalling—without advancing counterfactual claims or definitive process-tracing of decision sequences.

4. Digital intelligence and analytical mechanisms in international relations

International Relations are increasingly shaped by technological acceleration and rising epistemological complexity, generating new challenges for crisis analysis and strategic decision-making. This section examines how digital intelligence contributes to these

transformations by reshaping crisis governance and foreign-policy responses, outlining its conceptual evolution, core mechanisms, and strategic relevance.

4.1 Digital intelligence: origins and development

The emergence of digital intelligence reflects its growing significance within contemporary International Relations, particularly in relation to realist and neo-realist concerns with power, security, and strategic competition. Neo-realist scholarship identifies cyberspace as a strategic domain in which states seek both influence and resilience, as the digitisation of infrastructures expands strategic capabilities while exposing states to new forms of vulnerability (Adams, 2001, p. 98).

In this context, digital intelligence refers to the integration of computational tools into geopolitical forecasting, crisis anticipation, and adaptive decision-making processes, enhancing institutional foresight in foreign policy without displacing human judgement (Shafiq, 2020, p. 17). This understanding aligns with John McCarthy's definition of intelligence as "the computational aspect of the ability to achieve goals in the world" (McCarthy, 2007, p. 2).

Although still a relatively nascent field, digital intelligence can be traced to the late 1940s and early 1950s and has evolved through successive technological and conceptual shifts that gradually connected computation to governance, strategy, and decision-making in international affairs:

4.1.1 Phase one: foundational theorizing (1940–1950s). Early work in cybernetics and computational theory laid the foundations of digital intelligence by linking feedback, control, and machine reasoning to decision-making under uncertainty (Wiener, 1965, pp. 1–44; Turing, 1950, pp. 433–434). This intellectual trajectory gained institutional recognition with the 1956 Dartmouth Conference, led by John McCarthy, which reframed machine reasoning as a tool for strategic forecasting and decision-support in national security, foreign policy analysis, and crisis anticipation (Moor, 2006, pp. 87–88).

4.1.2 Phase two: the golden age (1960–1970s). The 1960 and 1970s marked a phase of strategic optimism regarding digital intelligence, as confidence grew in its relevance for governance, policy analysis, and strategic forecasting. Early applications, including Joseph Weizenbaum's ELIZA, reinforced expectations that computational systems could support policy dialogue and administrative decision-making (Simon, 1965, p. 2). At the same time, early debates on autonomous adaptation raised questions of control and resilience that later informed discussions of cyber security and digital sovereignty in international relations (von Neumann, 1966, pp. 288–296; Mousa and Bilal, 2019, p. 39).

4.1.3 Phase three: the Digital Intelligence Winter (1980s). The 1980s, often described as the "Digital Intelligence Winter," were marked by reduced funding and declining academic confidence, prompting a reassessment of digital intelligence as a support tool for policy analysis and strategic decision-making under uncertainty. Expert systems retained limited governance utility despite their rigidity (Newquist, 1994, pp. 189–192), while Searle's "Chinese Room" critique underscored normative concerns about delegating political judgement to algorithmic systems (Searle, 1980, p. 417). At the same time, advances in neural network modelling laid conceptual foundations for later applications in crisis simulation and policy analysis within international contexts (Russell and Norvig, 2003, p. 25).

4.1.4 Phase four: market recession and conceptual reassessment (1987–1993). Between 1987 and 1993, digital intelligence experienced a marked downturn following the collapse of the specialised AI hardware market, which failed to deliver scalable systems suitable for strategic governance (Newquist, 1994, pp. 359–379; Crevier, 1993, pp. 209–210). This contraction exposed the fragility of early digital intelligence infrastructures and prompted a reassessment of their strategic value for decision-making under uncertainty, as reflected in widespread firm closures by the early 1990s (Newquist, 1994, p. 440). During this period, Brooks' critique of symbol-based models redirected attention toward adaptive approaches

better suited to real-world complexity, reinforcing the importance of institutional embedding and flexibility in crisis governance and international decision-making (Brooks, 1990, p. 3).

4.1.5 Phase five: recovery and expansion (1997–Present). The recovery of digital intelligence began in 1997 with renewed confidence in machine-based strategic reasoning for foreign-policy analysis, followed by its deeper integration into security and governance domains in the early 2000s (McCorduck, 2004, pp. 480–483; Mousa and Bilal, 2019, p. 37; Thrun et al., 2007, p. 1). By 2008, predictive tools such as the Integrated Crisis Early Warning System institutionalised digital intelligence within international crisis governance (O’Brien, 2010, p. 88).

Its geopolitical significance intensified in the 2010s as cyber operations, disinformation campaigns, and advances in data-driven analysis demonstrated how digital capabilities could undermine sovereignty and reshape strategic competition. Developments such as Alibaba’s performance on the Stanford Question Answering Dataset (SQuAD) signalled qualitative shifts in analytical capacity, reinforcing asymmetries between digitally advanced and dependent states (Hari et al., 2018, p. 7). These shifts contributed to a broader reconfiguration of international order around digital capabilities and informational sovereignty, reinforcing structural asymmetries in global politics (Buchanan, 2020, pp. vi–2).

Recent International Relations scholarship therefore conceptualises digital intelligence as a domain of power, governance, and sovereignty shaped by algorithmic authority and data control (Srivastava, 2023, pp. 989–990; Musiani, 2022, pp. 785–800; Topor, 2024, pp. 1–20).

In International Relations terms, these developments represent not merely technological change but political transformations in how authority is produced and exercised across borders, particularly in relation to agenda-setting, infrastructural control, and governance arrangements. Accordingly, recent IR scholarship increasingly conceptualises digital intelligence as a domain of power, institutional rule-making, and sovereignty practices.

Within this literature, one strand examines algorithmic governance and the international politics of Big Tech, highlighting how platform power and data-driven systems generate new forms of private authority and reshape cross-border agenda-setting (Srivastava, 2023, pp. 989–990). Another focuses on digital sovereignty as practical efforts to “infrastructurize” self-determination through data governance, localisation, and standards, alongside security-oriented approaches that frame cyber sovereignty as a strategic doctrine in international politics (Musiani, 2022, pp. 785–800; Topor, 2024, pp. 1–20).

This article contributes to these debates by advancing a conceptual framework that treats digital intelligence capacity as a bundle of state capabilities—data access, analytics, institutional coordination, and governance—through which states pursue strategic agency, shape norms, and defend sovereignty under conditions of geo-digital asymmetry.

4.2 Strategic implications for international relations

The growing relevance of digital intelligence reflects a structural shift in international relations rather than a merely technical development. As data infrastructures, predictive systems, and algorithmic tools become embedded in diplomacy and crisis response, states increasingly rely on them to improve situational awareness, shorten decision cycles, and manage uncertainty in external environments (Chessen, 2017, p. 5; O’Brien, 2010, pp. 87–88). In this sense, digital intelligence matters in IR because it affects how states anticipate threats, interpret strategic signals, and calibrate foreign-policy responses.

This strategic role has become more visible as major powers integrated intelligent systems into security and governance agendas. US. policy discussions linked AI ecosystems to national security and crisis preparedness, while subsequent scholarship emphasised the relevance of algorithmic support for emergency and policy response (National Science and Technology Council, 2016, pp. 1–48). China, in turn, has connected machine learning and data infrastructures to broader questions of state capacity, diplomatic reach, and strategic coordination, while the

United States has embedded similar tools in security and foreign-policy planning (El-Shafei, 1999, p. 10; Ashmawy, 2013, p. 2; Salem, 2022, pp. 8–9).

What follows is not the replacement of traditional geopolitics, but its reconfiguration within a hybrid order in which states, platforms, cyber units, and data infrastructures increasingly shape conflict management and political influence. Initiatives such as China's Digital Silk Road further illustrate how digital infrastructure can serve geopolitical purposes by extending influence through connectivity, standards, and technological dependence (Kello, 2017, pp. 112–118; Allison, 2017, pp. 147–153; Kania, 2017, pp. 45–55). Digital intelligence thus enters IR as a variable linked to strategic behaviour, asymmetrical dependence, and the distribution of influence under conditions of geo-digital inequality.

5. Digital intelligence and the shifting architecture of international relations: toward a multipolar global order

5.1 Digital intelligence as a catalyst of systemic change

Over the past decade, the international system has undergone a techno-political transformation in which digital infrastructures increasingly shape diplomacy, security, and strategic competition. This development challenges conventional understandings of sovereignty and power because influence no longer depends only on material capabilities, but also on the ability to collect data, process information, coordinate cyber systems, and exercise algorithmic control across borders (Khalifa, 2023, p. 29). In this context, digital intelligence has become increasingly relevant to how influence is produced and exercised across the international system.

Digital intelligence has emerged as a strategic driver of this transformation, increasingly displacing traditional metrics of power such as military capability and economic size. In today's global environment, the capacity to harness and project digital intelligence—through data collection, algorithmic control, and cyber coordination—has become central to influencing geopolitical dynamics.

The spread of digital tools—big data analytics, real-time surveillance, and predictive modelling—alters how states interact and compete. Advanced actors can now influence political and security outcomes in other states without physical intervention. By embedding algorithmic logic into transnational infrastructures, states exercise influence through data-driven dynamics rather than direct domination.

As a result, the architecture of international relations is not merely shifting in institutional terms, but in the evolving dynamics of strategic behaviour, authority, and engagement. States that successfully operationalise digital intelligence acquire asymmetric power advantages, particularly in shaping decision flows, manipulating digital environments, and redefining the parameters of global interaction.

5.2 Cyber threats and informational supremacy in global order

In 2023, the World Economic Forum's annual report highlighted a growing expert consensus that a major cyber disruption is likely within two years. This projection is driven by escalating geopolitical tensions, including the Russia–Ukraine war, the intensifying strategic rivalry between the United States and China, and ongoing cyber hostilities between Iran and Israel as of mid-2025. These tensions are further compounded by the rising sophistication of cyber threats, including transnational attacks and state-sponsored digital operations (Mahmoud, 2023a, b).

Amid this shifting strategic landscape, global competition has extended beyond territorial geography into the digital domain. Technologically advanced states now compete to dominate digital infrastructure, secure exclusive access to analytical platforms, and develop predictive algorithmic tools capable of shaping global policy in advance. In this

arena, power is increasingly defined by digital intelligence deployment and cyber reach rather than material capabilities alone.

This evolution is reinforced by the spread of intelligent software across modern defence systems—ranging from air defence and UAVs to nuclear command and missile platforms (Al-Mansi, 2020). As such systems become integral to military architectures, they are transforming how power is distributed, perceived, and contested in the global order (Mahmoud, 2023a, b, p. 65).

Building on this analysis, the article adopts a perspective that views digital intelligence as a driver of strategic forecasting, enabling states to anticipate crises instead of merely reacting. The integration of algorithmic models and big data into national security infrastructures enhances early threat detection and allows simulation of escalation scenarios. This signals a shift toward governance rooted in anticipation and real-time digital insights—reshaping the logic of international engagement.

5.3 Reconfiguring power and actorhood in the digital age

Digital intelligence is reshaping international relations through three interrelated dynamics. First, it expands the range of influential actors, as major technology corporations and digital platforms increasingly affect agenda-setting and cross-border governance (Schmidt and Cohen, 2013, pp. 45–50). Second, it transforms influence itself, as algorithmically curated information environments mediate persuasion, visibility, and reputational power in foreign policy (Floridi, 2014, pp. 128–133). Third, it alters the architecture of decision-making in security and diplomacy by embedding predictive and data-driven tools into crisis management and strategic planning (West, 2018; Kello, 2017, pp. 142–148). Accordingly, digital intelligence is no longer a merely supportive resource; it has become a strategic dimension of global positioning in which states and non-state actors compete over infrastructures, narratives, and informational control (Floridi, 2014, pp. 85–93; Kello, 2017, pp. 112–118).

5.4 Strategic role of digital intelligence in global influence

Digital intelligence has emerged as a core pillar of global influence, reshaping how power is produced, projected, and preserved. States and non-state actors capable of engineering data systems and controlling digital infrastructure now play decisive roles in shaping international outcomes and influencing decision-making processes (Schmidt and Cohen, 2013, pp. 44–50). In today's environment, supremacy is no longer determined solely by military or economic assets, but by the ability to harness digital intelligence across three critical domains: crisis tracking, public sentiment analysis, and informational control (González, 2020, pp. 583–588).

This evolution signals a broader transformation in the architecture of international relations. The global system is gravitating toward a hybrid configuration where conventional power metrics intersect with digital capabilities. Technology corporations, digital platforms, and cyber actors are becoming influential players in matters of conflict, diplomacy, and global governance. This shift reflects not only the redistribution of power but also a redefinition of who constitutes a strategic actor (Allison, 2017, pp. 197–204).

As competition intensifies, the strategic utility of digital intelligence is driving a recalibration of power hierarchies. Analysts warn that this digital race may escalate geopolitical tensions, with cyber and information domains emerging as potential arenas for confrontation (World Economic Forum, 2023, pp. 11–15).

In this context, digital intelligence is no longer a passive analytical resource but a strategic determinant of global positioning. For developing countries, this reality underscores the urgency of national strategies focused on localising digital technologies, building cyber resilience, and asserting digital sovereignty. In the contemporary order, dominance increasingly hinges on control over the technopolitical domain—the defining frontier of power in the digital age.

6. Localising digital intelligence in the Global South: mechanisms and strategic pillars

6.1 Strategic role of digital intelligence in global influence

Digital intelligence has become an essential component of strategic forecasting by enabling states to anticipate crises, simulate dynamic scenarios, and extract real-time insights. These capabilities facilitate a shift from reactive diplomacy to proactive crisis management, enhancing states' ability to act preemptively in volatile environments.

Localising digital intelligence is therefore increasingly critical for emergency preparedness, strategic governance, and the protection of national infrastructures. Scholars emphasise that countries controlling their digital data flows are better equipped to respond to rapidly changing policy landscapes (West *et al.*, 2023, p. 11). Although these systems mimic certain cognitive processes, they do not replicate human agency. However, recent advancements in machine learning (ML), natural language processing (NLP), and machine translation (MT) have significantly augmented their functional autonomy (Hutchinson, 2022a, b, p. 107).

In recognition of these strategic imperatives, many digital-importing countries across the Global South have initiated national strategies to embed digital intelligence across political, economic, and societal domains. These efforts are supported by targeted investments in cybersecurity and institutional resilience. For instance, Rwanda established the Centre for the Fourth Industrial Revolution to bolster its digital readiness, while Kenya expanded its digital public infrastructure to strengthen national data ecosystems (World Economic Forum, 2022, p. 5; GSMA, 2023, p. 9).

6.2 Strategic relevance to the Global South

The localisation of digital intelligence in the Global South is central to enhancing sovereignty and reducing reliance on external actors. Saudi Arabia and Egypt offer distinct strategic pathways: the former integrates digital governance with Vision 2030 via its National Strategy for Data and Artificial Intelligence (NSDAI) under the Saudi Data and Artificial Intelligence Authority (SDAIA); the latter targets justice and healthcare through national platforms. According to the Organization for Economic Co-operation and Development (OECD 19, 2023) and the United Nations Development Program (UNDP, 2024, p. 27), both exemplify state-led resilience and anticipatory governance.

6.3 Benchmarking national readiness: global indices and regional rankings

The growing emphasis on localising digital intelligence is reflected in global benchmarking tools that assess national capacities for adopting and governing intelligent systems. Among the most prominent are the Tortoise Global AI Index (Tortoise Media, 2021, pp. 3–8) and the Oxford Insights AI Readiness Index (Oxford Insights, 2024, pp. 9–22), developed in partnership with the International Development Research Centre (IDRC). These indices offer comparative insights into institutional preparedness across governance, infrastructure, and digital strategy domains.

Early assessments positioned Saudi Arabia at the forefront of Arab countries—ranking 26th globally and 1st regionally in the 2021 Tortoise Index—ahead of the UAE (34th) and Qatar (47th) (Tortoise Media, 2021, pp. 3–6; Mousavizadeh *et al.*, 2020, pp. 2–3). Updated 2025 projections, based on national strategy documents and the Oxford Insights Index, indicate shifting dynamics (Oxford Insights, 2024, pp. 18–22):

- (1) The United Arab Emirates leads the region with a score of 69.5 (25th globally).
- (2) Saudi Arabia follows with 66.2 (34th), and Qatar with 63.8 (38th).
- (3) Egypt ranks 61st (59.1), ahead of Oman (60.4, 59th) and Jordan (57.4, 64th).
- (4) Lower positions include Bahrain (62nd), Morocco (68th), Tunisia (70th), and Algeria (84th).

These figures underscore enduring asymmetries in digital governance across the Arab world: Gulf states demonstrate stronger institutional alignment, while North African and Levantine countries face structural fragmentation.

Although originally designed for AI preparedness, the 2025 index is employed here as a proxy within a broader digital intelligence framework. Comparative rankings—summarized in [Table 1](#) and visualized in [Figure 1](#)—highlight how institutional capacity continues to shape regional positioning in the evolving digital order.

6.4 Strategic pillars of digital intelligence localisation

6.4.1 Pillar one: governmental strategy and policy commitment. This pillar evaluates the extent of governmental engagement in digital intelligence localisation. Key indicators include:

- (1) Development of national strategies for digital intelligence.
- (2) Regulatory and ethical governance frameworks.
- (3) Public investment in digital infrastructure and innovation ecosystems.
- (4) Institutional readiness and digital human capital.

The 2022 AI Readiness Index shows that several middle-income countries—such as Thailand, Malaysia, Peru, and Jordan—have launched national frameworks, signalling a rise in policy engagement across emerging economies. However, most low-income countries still lack foundational digital governance, underscoring the need for inclusive global cooperation ([Rogerson et al., 2022](#), pp. 6, 10).

6.4.2 Pillar two: innovation and the research and development ecosystem. This pillar assesses a country's capacity to generate innovation in digital intelligence through five indicators:

- (1) Peer-reviewed publications and citation performance (e.g. H-index).
- (2) Conference and journal contributions (e.g. IEEE involvement).
- (3) Strength of research institutions and local innovation communities.
- (4) Participation in open-source initiatives.
- (5) Patent activity and technological originality.

Table 1. AI readiness scores for selected Arab countries (2025)

Country	AI readiness score (2025)	Global rank
United Arab Emirates	69.5	25
Saudi Arabia	66.2	34
Qatar	63.8	38
Oman	60.4	59
Egypt	59.1	61
Bahrain	58.7	62
Jordan	57.4	64
Tunisia	54.3	70
Morocco	55.6	68
Algeria	51.2	84

Note(s): 2025 values are author-generated estimates based on trend analysis of official national AI strategies and comparative indicator trajectories

Source(s): Author's elaboration based on data from [Oxford Insights \(2022\)](#), [World Bank \(2023\)](#), [Tortoise Media \(2024\)](#) and author-generated estimates

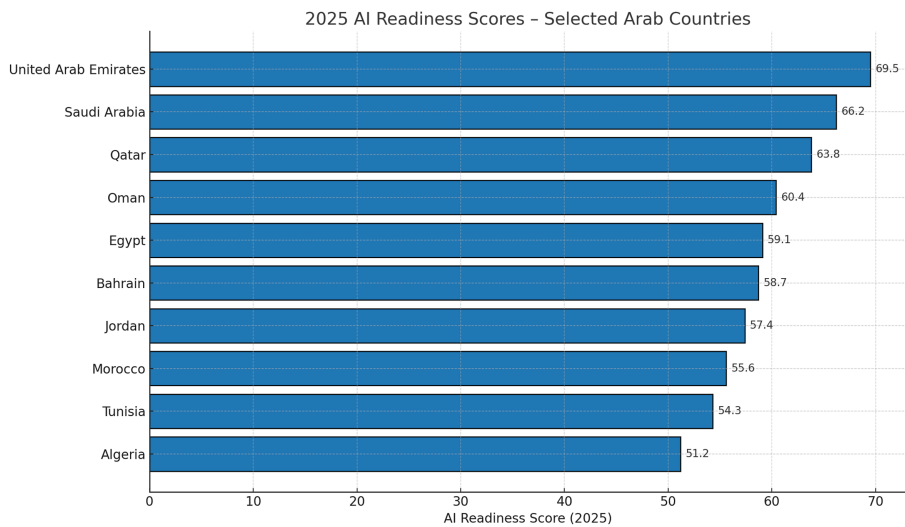


Figure 1. The 2025 comparative AI readiness scores for selected Arab countries. Note: 2025 values are author-projected based on historical trends and national policy documentation. **Source(s):** Author’s, using data from [Oxford Insights \(2019–2024\)](#), [SDAIA \(2023\)](#), [Egypt MCIT \(2023\)](#) and AI global index forecasts (2024–2025)

Innovation bridges theoretical research and practical application, enabling the development of digital intelligence tools for governance, strategic forecasting, and public service delivery. Countries with mature R&D ecosystems—often those scoring high in digital readiness—are better positioned to translate foundational research into operational technologies. According to the Organisation for Economic Co-operation and Development ([OECD, 2023](#), pp. 22–26) and the United Nations Educational, Scientific and Cultural Organization ([UNESCO, 2024](#), pp. 9–14), strong innovation systems underpin national capacity to deploy digital intelligence effectively.

6.4.3 Pillar three: infrastructure and the operating environment. This pillar evaluates the foundational systems required to support digital intelligence implementation. Key indicators include:

- (1) High-performance computing and network infrastructure.
- (2) Availability and quality of public-sector digital datasets.
- (3) National digital literacy and capacity-building initiatives.
- (4) Regulatory mechanisms for ethical and transparent algorithm use.

While many advanced economies have invested heavily in infrastructure, gaps remain in aligning these capabilities with governance frameworks. The [Oxford Insights AI Readiness Index \(2022\)](#) notes that countries such as the Netherlands and Sweden—despite their technological sophistication—lack comprehensive strategies for algorithmic accountability and regulatory integration, raising concerns about sustainable digital governance. Conversely, countries like Malaysia and Oman demonstrate stronger STEM capacity and data readiness, offering more balanced digital operating environments ([Rogerson et al., 2022](#), p. 12).

6.5 Strategic reflection and concluding insights

The comparative analysis of the [Tortoise Intelligence Index \(2021\)](#) and the [Oxford Insights Government AI Readiness Index \(2022\)](#) reveals a persistent policy challenge: the absence of

standardized frameworks for digital readiness across many states promoting digital intelligence. Despite political intent, progression across the three strategic pillars—technical infrastructure, governance, and innovation—remains uneven, limiting national capacity to integrate digital intelligence into development agendas (Oxford Insights, 2022, pp. 8–14; Tortoise Media, 2021, pp. 5–7).

This fragmentation has direct implications for long-term competitiveness and digital sovereignty. Countries that struggle to bridge these gaps may experience constrained strategic autonomy and reduced influence in data-driven global governance (Oxford Insights, 2022, pp. 18–22).

In contrast, states advancing across multiple dimensions are positioned to build resilient ecosystems and generate positive policy synergies. For countries in the Global South, this integration is critical not only for digital adoption but also for embedding digital intelligence into inclusive, capacity-focused, and cooperative development strategies (Tortoise Media, 2021, pp. 6–8).

6.6 Comparative analysis: Egypt and Saudi Arabia in the digital intelligence readiness landscape

A comparative assessment of Egypt and Saudi Arabia reveals a notable divergence in digital intelligence readiness across strategic dimensions. According to the 2024 Government AI Readiness Index—developed by Oxford Insights and the International Development Research Centre—Egypt ranks 62nd globally with a score of 57.3, indicating gradual but uneven progress. Egypt’s National AI Strategy, developed in partnership with UNESCO and the Ministry of Communications and Information Technology, represents a key step toward institutional alignment. However, limited policy integration and persistent institutional fragmentation constrain Egypt’s capacity to embed digital intelligence into long-term development agendas (UNESCO, 2024, pp. 12–17; MCIT, 2023, pp. 4–9).

In contrast, Saudi Arabia ranks 36th with a score of 64.8, positioning it among the leading Arab states in digital intelligence readiness. This reflects the integration of digital intelligence within Vision 2030, supported by the Saudi Data and Artificial Intelligence Authority (SDAIA) and its National Strategy for Data and Artificial Intelligence (NSDAI). Saudi Arabia’s progress is underpinned by (Oxford Insights, 2024, pp. 8–14; SDAIA, 2023):

- (1) High-level political commitment and sustained investment in digital infrastructure and platforms.
- (2) Deployment of digital intelligence tools across sectors such as health, justice, and urban systems (e.g. NEOM).
- (3) Regulatory and ethical governance frameworks for algorithmic oversight and data integrity.

This divergence is illustrated in Table 2 and Figure 2, which trace the evolution of AI readiness as a proxy for digital intelligence capacity between 2019 and 2025.

6.7 Comparative AI readiness scores for Saudi Arabia and Egypt (2019–2025)

Despite structural and strategic differences, both countries exemplify the broader momentum across the Global South to establish sovereign digital ecosystems. Egypt reflects a model of gradual institutional adaptation, shaped by international cooperation and policy emphasis on digital inclusion. Saudi Arabia, by contrast, demonstrates a centralised approach, underpinned by a national vision, strong institutional coordination, and significant resource mobilisation.

This comparison reinforces the view that the effective localisation of digital intelligence is not solely determined by economic capacity or technological advancement. Rather, it hinges on the presence of coherent governance structures, sustained investment in human capital, and the integration of ethical, regulatory, and operational frameworks into national strategies.

Table 2. Comparative AI readiness scores for Saudi Arabia and Egypt (2019–2025)

Year	Saudi Arabia	Egypt
2019	52.3	49.0
2020	55.8	50.7
2021	58.9	52.0
2022	61.9	55.1
2023	63.5	56.2
2024	64.8	57.3
2025 (est.)	66.2	58.1

Note(s): 2025 values are author estimates derived from trend analysis and national strategy documents

Source(s): Author’s own, based on [Oxford Insights \(2019–2024\)](#), [MCIT \(2023\)](#) and [SDAIA \(2023\)](#)

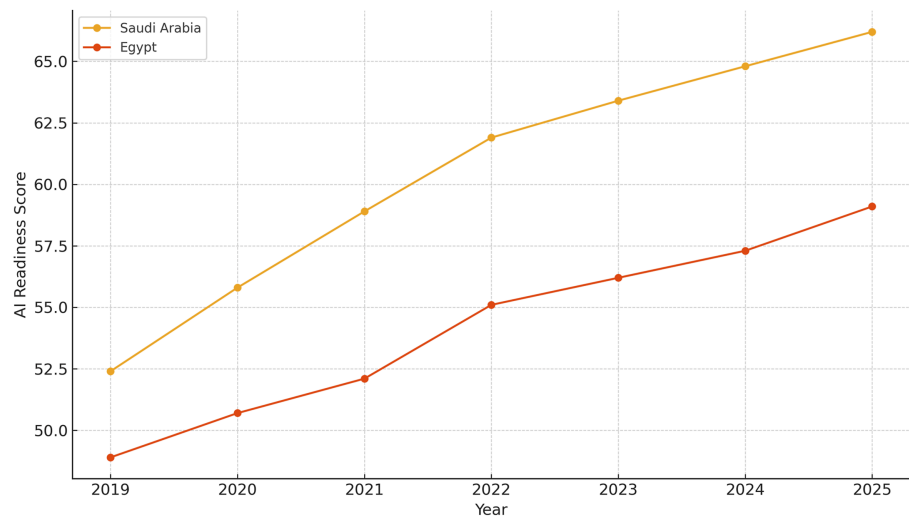


Figure 2. Comparative AI readiness scores for Saudi Arabia and Egypt (2019–2025). Note: 2025 values are authorial projections based on historical data and official policy sources. **Source(s):** Author’s, using data from [Oxford Insights \(2019–2024\)](#), [MCIT \(2023\)](#), [SDAIA \(2023\)](#) and AI global index forecasts (2024–2025)

7. Discussion

This article contributes to a growing body of scholarship that treats digital infrastructures as arenas of power and governance in international relations. Consistent with the proposed conceptual framework, the comparative analysis suggests patterned differences in anticipatory governance and crisis-analytics integration that appear to be associated with variations in digital intelligence capacity, including differences in decision-making tempo and external signalling practices. At the same time, the findings indicate that institutional design and sovereignty practices condition how digital capabilities are mobilised in practice, shaping patterns of policy coordination and strategic positioning without implying automatic or uniform strategic gains.

The comparative evidence is organized around three observable pathways through which digital intelligence capacity becomes foreign-policy relevant in crisis contexts. First, crisis anticipation refers to the way data infrastructures and forecasting routines can support earlier situational awareness during transnational shocks. Second, policy coordination captures how whole-of-government digital platforms and centralised data governance can enable faster inter-agency alignment during crisis episodes. Third, external signalling denotes how digitally

mediated crisis communication and economic diplomacy can shape external audience perceptions—illustrated here by the March 2021 Suez Canal blockage as a logistics shock that rapidly generated international crisis diplomacy and signalling pressures (United Nations Conference on Trade and Development, 2021, p. 6). In the Egypt–Saudi comparison, these pathways are reflected in the case material in three corresponding ways. Regarding crisis anticipation, Saudi Arabia’s more centralised data-and-analytics governance, anchored in national data/AI institutionalisation, aligns with earlier situational awareness routines during COVID-19 (Memish *et al.*, 2021, p. 141; Khan *et al.*, 2021, p. 3924), whereas Egypt’s anticipatory routines are discussed through a ministry- and plan-based response architecture under the national COVID-19 emergency response framework (World Bank, 2020, pp. 5, 22–23). Regarding policy coordination, Saudi Arabia’s institutional centralisation and platform-enabled crisis management are associated with faster inter-agency alignment, while Egypt’s crisis response is discussed through formal response planning and steering arrangements that structure coordination across implementing entities (World Bank, 2020, p. 5). Regarding external signalling, the Suez disruption is treated as an illustrative episode of logistics-driven crisis diplomacy and signalling pressures that foregrounds the role of digitally mediated communication in shaping international perceptions (United Nations Conference on Trade and Development, 2021, p. 6).

The analysis further highlights how differences in localisation strategies between Egypt and Saudi Arabia reflect varying degrees of digital autonomy, governance coherence, and knowledge production capacity. In Global South contexts, weak institutional frameworks and limited research capacity can compound obstacles to asserting strategic agency within a data-driven international order.

The comparative findings also point to a broader pattern of geo-digital asymmetry. While some emerging economies have integrated digital intelligence into national development and governance agendas, others remain constrained by fragmented policies, uneven investment, and underdeveloped digital ecosystems. Such disparities have significant implications for international relations, as informational asymmetries increasingly shape diplomatic leverage, economic competitiveness, and resilience in security and crisis management.

Ultimately, the article underscores the importance of context-sensitive digital capacity-building strategies in the Global South to reduce structural asymmetries and enable more inclusive participation in emerging forms of global governance. The localisation of digital intelligence is therefore not only a technical process, but also a politically consequential dimension of contemporary international relations.

8. Conclusion and implications

This article set out to examine how digital intelligence shapes strategic mechanisms and power dynamics in international relations by tracing three analytically specified governance mechanisms: crisis anticipation, policy coordination, and external signalling. Grounded in a comparative and theory-informed framework, it positions digital intelligence not as a peripheral technological development but as an increasingly consequential dimension of contemporary global politics.

8.1 Key findings

Building on the article’s research puzzle and central proposition, the following results summarise mechanism-aligned comparative patterns, interpreted as conditional associations rather than causal estimates.

8.1.1 Finding 1 – Digital intelligence becomes IR-relevant when translated into crisis-statecraft mechanisms. The Egypt–Saudi comparison shows that digital intelligence matters for foreign policy when it is operationalised through three observable mechanisms: crisis anticipation (routinised early-warning and forecasting), policy coordination (whole-of-government alignment

and interoperable decision routines), and external signalling (coherent outward-facing messaging under shock). The article's contribution is thus not "digital adoption" *per se*, but the translation of digital capacity into mechanism-based crisis statecraft.

8.1.2 Finding 2 – Governance conditions shape cross-case divergence under broadly similar shock exposure. Under broadly comparable exposure to transnational disruptions, variation in institutional centralisation, authoritative public-sector data governance, and cross-agency interoperability aligns with differences in the consistency of the anticipation and coordination mechanisms—especially the speed/coherence of crisis assessment and the reliability of inter-agency alignment across the two cases.

8.1.3 Finding 3 – Sovereignty practices and geo-digital asymmetry condition signalling and strategic autonomy. External signalling is conditioned by how digital infrastructures and narratives are governed as instruments of statecraft—through localisation choices, state-technology relations, and informational-sovereignty safeguards (cyber resilience, disinformation protection, and privacy governance). The March 2021 Suez Canal disruption is used as an illustrative episode of high-salience crisis diplomacy, highlighting the premium placed on credible, coherent signalling. At the structural level, the North–South geo-digital divide operates as a constraint on Global South strategic autonomy by embedding asymmetric dependence on external platforms, infrastructures, and standards—thereby delimiting policy space during crises even when domestic digital capacity improves.

8.2 Policy recommendations

- (1) Translate digital intelligence into an IR-relevant crisis-statecraft capability (strategic warning; rapid alignment)

Embed digital intelligence as a strategic-warning and crisis-decision function within the foreign-policy and national-security apparatus by institutionalising early-warning/forecasting routines that feed directly into crisis assessment and option selection. Operationalise whole-of-government alignment through authoritative public-sector data stewardship, shared operational standards, and interoperable coordination channels—reflecting the article's mechanism claim that institutional design and data-governance architecture structure crisis anticipation and policy coordination.

- (2) Consolidate crisis-time external signalling as a sovereignty-conditioned instrument of statecraft (credible diplomacy; narrative resilience)

Adopt a standing crisis-signalling protocol that aligns digital diplomacy with public messaging during transnational shocks, sustaining coherent and credible external communication. Anchor signalling in informational-sovereignty practices—defined state-technology relations, localisation choices, and safeguards for cyber resilience, disinformation protection, and privacy governance—rather than episodic media management. This aligns with the article's treatment of external signalling as conditional on sovereignty practices, as illustrated by the March 2021 Suez Canal disruption under intense international attention.

- (3) Reduce geo-digital asymmetry by narrowing the North–South divide (strategic autonomy; selective localisation)

Treat geo-digital asymmetry as a structural constraint on Global South strategic autonomy, produced by asymmetric reliance on external platforms, infrastructures, and standards. Narrow this constraint through selective localisation and capability-building in public-sector data governance, national analytics ecosystems, and cybersecurity resilience, thereby reducing exposure of foreign-policy room for manoeuvre to external infrastructural dependence.

- (4) Build Arab–African coalitions for rule-shaping in digital governance (standard-setting; platform accountability)

Institutionalise Arab–African coordination for external rule-shaping by harmonising positions on platform accountability, cross-border data governance principles, and standards adoption in relevant multilateral venues. This shifts the response to geo-digital asymmetry from domestic adjustment to international governance influence, expanding policy space through collective standard-setting rather than duplicating internal capacity-building.

References

- Adams, J. (2001), *The Next World War: Computers Are the Weapons and the Front Line is Everywhere*, Simon & Schuster, New York, NY.
- Aguerre, C., Campbell-Verduyn, M. and Scholte, J.A. (Eds) (2024), *Global Digital Data Governance: Polycentric Perspectives*, Routledge, London.
- Al-Mansi, H. (2020), “Can artificial intelligence compensate for strategic shortcomings?”, Arab Homeland Agency, 9 February, available at: <https://cutt.us/eKplw> (accessed 1 April 2025).
- Allison, G. (2017), *Destined for War: Can America and China Escape Thucydides’s Trap?*, Houghton Mifflin Harcourt, Boston, MA.
- Ashmawy, M. (2013), *The Role of Newspapers in Managing Security Crises*, 1st ed., United Arab Company for Marketing and Supplies, Cairo.
- Brooks, R. (1990), “Elephants don’t play chess”, *Robotics and Autonomous Systems*, Vol. 6 Nos 1-2, pp. 3-15, doi: [10.1016/S0921-8890\(05\)80025-9](https://doi.org/10.1016/S0921-8890(05)80025-9).
- Buchanan, B. (2020), *The AI Triad and what it Means for National Security Strategy*, Center for Security and Emerging Technology, Georgetown University, Washington, DC, available at: <https://cset.georgetown.edu/publication/the-ai-triad-and-what-it-means-for-national-security-strategy/> (accessed 22 April 2025).
- Chessen, M. (2017), *The MADCOM Future: How Artificial Intelligence Will Enhance Computational Propaganda, Reprogram Human Culture, and Threaten Democracy... and What Can be Done about it*, Atlantic Council, Washington, DC.
- Choucri, N. (2021), “Cyberpower and sovereignty”, in Mansell, R. and Steinmueller, W.E. (Eds), *Digital Transformation and World Order*, Routledge, London, pp. 33-48.
- Couldry, N. and Mejias, U.A. (2019), *The Costs of Connection: How Data is Colonizing Human Life and Appropriating it for Capitalism*, Stanford University Press, Stanford, CA.
- Crevier, D. (1993), *AI: The Tumultuous Search for Artificial Intelligence*, Basic Books, New York, NY.
- DeNardis, L. (2014), *The Global War for Internet Governance*, Yale University Press, New Haven, CT, doi: [10.2307/j.ctt5vkz4n](https://doi.org/10.2307/j.ctt5vkz4n).
- Egypt Ministry of Communications and Information Technology (2023), *Egypt’s National AI Strategy Report 2023*, MCIT, Cairo, available at: <https://mcit.gov.eg/en/AI> (accessed 12 June 2025).
- El-Shafei, M. (1999), *Crisis Management*, 1st ed., Al-Mahrousa Center for Research, Arabization and Publishing, Cairo.
- Farrell, H. and Newman, A.L. (2019), “Weaponized interdependence: how global economic networks shape state coercion”, *International Security*, Vol. 44 No. 1, pp. 42-79, doi: [10.1162/isec_a_00351](https://doi.org/10.1162/isec_a_00351).
- Floridi, L. (2014), *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*, Oxford University Press, Oxford.
- Global System for Mobile Communications Association (2023), *Digital Transformation in Africa: Infrastructure and Policy Priorities*, GSMA Intelligence, London, available at: <https://www.gsma.com/mobilefordevelopment/resources> (accessed 12 June 2025).
- González, F. (2020), “Artificial intelligence and global power shifts”, *Journal of Strategic Studies*, Vol. 43 No. 4, pp. 579-601, doi: [10.1080/01402390.2019.1705242](https://doi.org/10.1080/01402390.2019.1705242).
- Hari, T., Kim, C., Lin, L. and Lee, J. (2018), *Profiles in Innovation Revisited: AI Hardware*, GS Equity Research, New York, NY.

- Hutchinson, L. (2022a), *Artificial Cognition and The Ethics of Intelligent Systems*, Polity Press, Cambridge.
- Hutchinson, M. (2022b), *Artificial Intelligence and Localization*, VistaTec House, Ireland, available at: <https://vistatec.com> (accessed 14 March 2023).
- Kania, E.B. (2017), *Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power*, Center for a New American Security, Washington, DC, available at: <https://s3.amazonaws.com/files.cnas.org/documents/Battlefield-Singularity-November-2017.pdf> (accessed 12 June 2025).
- Kello, L. (2017), *The Virtual Weapon and International Order*, Yale University Press, New Haven, CT.
- Kello, L., Silver, D. and Zhang, M. (2022), "Cybersecurity dilemmas in the Global South", *Journal of International Affairs*, Vol. 78 No. 1, pp. 67-89.
- Keohane, R.O. and Nye, J.S. (2001), *Power and Interdependence*, 3rd ed., Longman, New York, NY.
- Khalifa, I. (2023), "The fourth industrial revolution and the shift in the international balance of power", *The Egyptian File Journal*, Vol. 8 No. 105, pp. 28-36, available at: <https://acpss.ahram.org.eg/News/20894.aspx> (accessed 12 June 2025).
- Khan, A., alahmari, A., Almuzaini, Y., Alturki, N., Aburas, A., Alamri, F.A., Albagami, M., Alzaid, M., Alharbi, T., Alomar, R., Abu Tayli, M., Assiri, A.M. and Jokhdar, H.A. (2021), "The role of digital technology in responding to COVID-19 pandemic: Saudi Arabia's experience", *Risk Management and Healthcare Policy*, Vol. 14, pp. 3923-3934, doi: [10.2147/RMHP.S317511](https://doi.org/10.2147/RMHP.S317511).
- Mahmoud, K.I. (2023a), "The evolution of AI technologies and the wars of the future", *Lubab Journal of Strategic Studies*, Vol. 5 No. 20, pp. 51-85, available at: <https://search.emarefa.net/detail/BIM-1627814> (accessed 12 June 2025).
- Mahmoud, K.W. (2023b), "Cyberspace: when everything seems possible", *Al Jazeera Net*, 4 September, available at: <https://2u.pw/3VsOjeM> (accessed 12 June 2025).
- McCarthy, J. (2007), *What is Artificial Intelligence?*, Stanford University, available at: <http://www-formal.stanford.edu/jmc/whatisai.pdf> (accessed 12 April 2025).
- McCorduck, P. (2004), *Machines Who Think*, 2nd ed., A.K. Peters, Ltd., Natick, MA.
- Memish, Z.A., Altuwajri, M.M., Almoeen, A.H. and Enani, S.M. (2021), "The Saudi Data and Artificial Intelligence Authority (SDAIA) vision: leading the Kingdom's journey toward global leadership", *Journal of Epidemiology and Global Health*, Vol. 11 No. 2, pp. 140-142, doi: [10.2991/jegh.k.210405.001](https://doi.org/10.2991/jegh.k.210405.001).
- Moor, J. (2006), "The Dartmouth college artificial intelligence conference: the next fifty years", *AI Magazine*, Vol. 27 No. 4, pp. 87-91, doi: [10.1609/aimag.v27i4.1911](https://doi.org/10.1609/aimag.v27i4.1911).
- Mousa, A. and Bilal, A.H. (2019), *Artificial Intelligence: A Technological Revolution of the Era*, 1st ed., Arab Group Publishing, Cairo.
- Mousavizadeh, A., Crum, B., Eling, C. and Horne, R. (2020), *The Global AI Index: Who is Leading the World in AI?*, Tortoise Intelligence, London, available at: <https://www.tortoisemedia.com/2020/12/03/who-is-leading-the-world-in-ai/> (accessed 15 April 2025).
- Musiani, F. (2022), "Infrastructuring digital sovereignty: a research agenda for an infrastructure-based sociology of digital self-determination practices", *Information, Communication and Society*, Vol. 25 No. 6, pp. 785-800, doi: [10.1080/1369118X.2022.2049850](https://doi.org/10.1080/1369118X.2022.2049850).
- Newquist, H.P. (1994), *The Brain Makers: Genius, Ego, and Greed in The Quest for Machines that Think*, Macmillan/SAMS, New York, NY.
- Nye, J.S. (2020), *Soft Power and Global Politics*, Oxford University Press, Oxford.
- Organisation for Economic Co-operation and Development (2023), *Artificial Intelligence in Public Sector Governance: Tools, Practices, and Guidelines*, OECD Publishing, Paris.
- Oxford Insights (2019), *Government Artificial Intelligence Readiness Index 2019*, Oxford Insights and International Development Research Centre, London, available at: https://oxfordinsights.com/wp-content/uploads/2023/12/ai-gov-readiness-report_v08.pdf (accessed 12 June 2025).

-
- Oxford Insights (2022), *Government AI Readiness Index 2022*, Oxford Insights and International Development Research Centre, available at: <https://www.oxfordinsights.com/government-ai-readiness-index-2022> (accessed 12 June 2025).
- Oxford Insights (2024), *Government AI Readiness Index 2024*, Oxford Insights in Partnership with the, International Development Research Centre, London, pp. 18-22, available at: <https://www.oxfordinsights.com/government-ai-readiness-index> (accessed 12 June 2025).
- O'Brien, S.P. (2010), "Crisis early warning and decision support: contemporary approaches and thoughts on future research", *International Studies Review*, Vol. 12 No. 1, pp. 87-104, doi: [10.1111/j.1468-2486.2009.00914.x](https://doi.org/10.1111/j.1468-2486.2009.00914.x).
- Purtova, N. and van Maanen, G. (2024), "Data as an economic good, data as a commons, and data governance", *Law, Innovation and Technology*, Vol. 16 No. 1, pp. 1-42, doi: [10.1080/17579961.2023.2265270](https://doi.org/10.1080/17579961.2023.2265270).
- Rogerson, A., MacDonald, M., Jafree, S., Valenduc, G. and Morrell, J. (2022), *Government AI Readiness Index 2022*, Oxford Insights and International Development Research Centre, available at: <https://www.oxfordinsights.com/government-ai-readiness-index-2022> (accessed 22 April 2025).
- Russell, S.J. and Norvig, P. (2003), *Artificial Intelligence: A Modern Approach*, 2nd ed., Prentice Hall, Upper Saddle River, NJ.
- Salem, M. (2022), "The impacts of artificial intelligence on the international system and national security", *IDSC Expert Commentary*, Vol. 27, pp. 1-18, available at: <https://library.idsc.gov.ge/bib/97951> (accessed 15 April 2025).
- Saudi Data and Artificial Intelligence Authority (2023), *National Strategy For Data And Artificial Intelligence (NSDAI)*, Saudi Data and Artificial Intelligence Authority, Riyadh, available at: <https://sdaia.gov.sa> (accessed 12 June 2025).
- Schmidt, E. and Cohen, J. (2013), *The New Digital Age: Reshaping the Future of People, Nations and Business*, Vintage, New York, NY.
- Searle, J.R. (1980), "Minds, brains, and programs", *Behavioral and Brain Sciences*, Vol. 3 No. 3, pp. 417-424, doi: [10.1017/s0140525x00005756](https://doi.org/10.1017/s0140525x00005756).
- Shafiq, H. (2020), *AI Journalism and The Future of News Production: The Robot Journalist as the Coming Media Revolution*, Fikr wa Fan Publishing, Cairo.
- Simon, H.A. (1965), *The Shape of Automation for Men and Management*, Harper & Row, New York, NY.
- Srivastava, S. (2023), "Algorithmic governance and the international politics of Big Tech", *Perspectives on Politics*, Vol. 21 No. 3, pp. 989-1000, doi: [10.1017/S1537592721003145](https://doi.org/10.1017/S1537592721003145).
- The Executive Office of the President of the USA, National Science and Technology Council (2016), "Artificial intelligence, automation, and the Economy", available at: https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf (accessed 12 June 2025).
- Thrun, S., Montemerlo, M., Dahlkamp, H., Stavens, D., Aron, A., Diebel, J., . . . and Mahoney, P. (2007), "Stanley: the robot that won the DARPA grand challenge", in Buehler, M., Iagnemma, K. and Singh, S. (Eds), *The 2005 DARPA Grand Challenge*, Springer Tracts in Advanced Robotics, Springer, Berlin, Vol. 36, pp. 1-43, doi: [10.1007/978-3-540-73429-1_1](https://doi.org/10.1007/978-3-540-73429-1_1).
- Topor, L. (2024), *Cyber Sovereignty: International Security, Mass Communication, and The Future of the Internet*, Springer, Cham, doi: [10.1007/978-3-031-58199-1](https://doi.org/10.1007/978-3-031-58199-1).
- Tortoise Media (2021), *The Global AI Index*, Tortoise Media, London, available at: <https://www.tortoisemedia.com/intelligence/global-ai/> (accessed 12 June 2025).
- Tortoise Media (2024), *AI Global Index Forecasts 2024-2025*, Tortoise Intelligence, London, available at: <https://www.tortoisemedia.com/intelligence/global-ai/> (accessed 12 June 2025).
- Turing, A.M. (1950), "Computing machinery and intelligence", *Mind*, Vol. 59 No. 236, pp. 433-460.

- United Nations Conference on Trade and Development (2021), *Review Of Maritime Transport 2021: Overview*, UNCTAD, Geneva, available at: https://unctad.org/system/files/official-document/rmt2021summary_en.pdf (accessed 4 February 2026).
- United Nations Development Programme (2024), *Digital Governance and Institutional Innovation in the Arab States*, United Nations Development Programme, New York.
- United Nations Educational, Scientific and Cultural Organization (2024), *AI Research and Capacity-Building in the Global South: Policy Recommendations*, United Nations Educational, Scientific and Cultural Organization, Paris.
- von Neumann, J. (1966), *Theory of Self-Reproducing Automata*, University of Illinois Press, Urbana, IL.
- Waltz, K.N. (1979), *Theory of International Politics*, Addison-Wesley, Reading, MA.
- West, D.M. (2018), *The Future of Work: Robots, AI, and Automation*, Brookings Institution Press, Washington, DC.
- West, J., Ahmed, S. and Ryu, D. (2023), *Resilient Data Sovereignty: Crisis Management in the Age of AI*, Brookings Institution Press, Washington, DC.
- Wiener, N. (1965), *Cybernetics: or Control and Communication in the Animal and the Machine*, 2nd ed., MIT Press, Cambridge, MA.
- World Bank (2020), *Environmental and Social Management Framework (ESMF): Egypt COVID-19 Emergency Response (P173912)*, World Bank, Washington, DC, available at: <https://documents.worldbank.org/en/publication/documents-reports/documentdetail/332341626110944683> (accessed 4 February 2026).
- World Bank (2022), “GovTech Maturity Index”, available at: <https://govtech.worldbank.org> (accessed 12 June 2025).
- World Bank (2023), *GovTech Maturity Index 2023*, International Bank for Reconstruction and Development/The World Bank, Washington, DC, available at: <https://www.worldbank.org/en/programs/govtech> (accessed 12 June 2025).
- World Economic Forum (2022), *Africa’s Fourth Industrial Revolution: Regional Transformation Hubs*, World Economic Forum, Geneva, available at: <https://www.weforum.org/reports> (accessed 12 June 2025).
- World Economic Forum (2023), *Global Cybersecurity Outlook 2023*, World Economic Forum, Geneva, available at: <https://www.weforum.org/reports/global-cybersecurity-outlook-2023> (accessed 22 April 2025).

Further reading

- Federal Bureau of Investigation (2018), *Russian Interference in 2016 US. Elections*, Washington, DC, available at: <https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections> (accessed 12 June 2025).
- Hadi, H.R. (2023), “The impact of artificial intelligence on international relations”, *Lubab Journal of Strategic Studies*, Vol. 5 No. 20, pp. 35-50, available at: <https://lubab.aljazeera.net/article/the-impact-of-artificial-intelligence-in-international-relations> (accessed 10 June 2025).
- Humanoid Robotics Institute (2022), *WABOT – Waseda Robot*, Waseda University, available at: <https://www.humanoid.waseda.ac.jp> (accessed 28 March 2025).

Corresponding author

Alshaimaa Mohamed Mahmoud Hassan can be contacted at: a.hassan@kfu.edu.sa