IRAQ'S CYBER LANDSCAPE : FRAGMENTED POWER, EXPOSED NETWORKS

Shan Mohammed | April 15, 2026

Key Takeaways

- Iraq ranks 129th globally in cybersecurity preparedness, implementing only 24% of recommended measures.
- Critical infrastructure (oil/gas), electoral systems, and 30 million citizens' data remain severely vulnerable.
- Muhasasa sectarian governance fragments authority, stalls legislation, and prioritizes patronage over expertise.
- Recent institutional progress (2022 strategy, 2025 directive) is insufficient without urgent political commitment and funding.

Introduction

Cyberspace is now a central domain of geopolitical rivalry, with Iraq occupying a particularly vulnerable and contested position within it. Neighboring Iran, a highly cyber-capable country, along with Russia and China, has demonstrated both the capacity and the intent to exploit Iraq's weakness. Yet Iraq navigates this competitive cyber environment critically underprepared. This paper contends that Iraq's cyber weaknesses stem not from technical shortcomings but from government and institutional gaps. The Muhasasa, a sectarian power-sharing arrangement, has divided authority, delayed cybercrime legislation, and prioritized political patronage over technical expertise. Without addressing the governance failures, neither technical investment nor foreign support will create cyber resilience.

“ Muhassasa (or muhassasa al-ta'ifia) is Iraq's post-2003 sectarian power-sharing system, where government posts, ministries, and resources are divided among ethnic and religious groups (Shia, Sunni, and Kurds). It acts as a quota system, entrenching corruption and patronage, as political parties prioritize controlling state spoils over merit-based governance.”

Global Cyber Warfare and the Stakes for Iraq

Cyberattacks and online intrusions are key, not just tools of modern state power in the 21st century. Leading world powers like China, Russia, and Iran are considered the most prominent examples of nations actively engaged in cyber warfare. The world is no longer confronting only the major powers in the conflict: Iraq finds itself on the front line of digital conflict. Digital threats cross the geopolitical boundaries; cyberattacks travel instantly through the internet. Energy infrastructure and government systems are appealing targets for both hostile neighboring countries and major global powers, which use them as staging grounds for operations against others.[1] An issue that was historically considered a technical problem, not a high-stakes national security issue, has now become a fundamental question of whether the nation can continue to exist or thrive with the lack of access to international cyber standards. Iraq's digital networks, internet infrastructure, and government databases will increasingly shape whether it can operate as a self-governing country.[2]

Iraq's geopolitical location and its relations with neighboring countries magnify its cyber exposure. Iran has developed significant offensive and defensive cyber capabilities as a pillar of its strategic doctrine. There is well-documented evidence of Iran using these digital tools to conduct cyberattacks multiple times, including the attack on the Saudi Arabian oil company in 2012 and attacks on Israeli infrastructure.[3] Beyond regional threats, the worldwide cyber operations conducted by Russia and China have demonstrated a willingness to attack critical infrastructure. Beijing's sustained espionage campaigns prove that any nation's digital networks and outdated systems are vulnerable to exploitation globally.[4] In the modern security landscape, safeguarding digital infrastructure is inseparable from protecting national security. Iraq remains in the process of strengthening its institutions and striving for lasting political stability after years of turmoil. The capacity to detect, deter, and respond to cyberattacks has become essential for Iraq's national security and long-term stability.

Iraq's Cybersecurity Standing in International Perspective

Global assessments highlight Iraq's weak cyber defenses, as evidenced by the UN's Global Cybersecurity Index (GCI). Iraq ranked 129th out of 194 countries in 2021, underscoring its persistent vulnerabilities. Iraq briefly improved its cybersecurity ranking to 107th in 2020; this improvement did not last long.[5] Iraq's cybersecurity weaknesses are as severe as, or worse than, those observed in other conflict-affected states. In 2024, Iraq received a score of 53.1 out of 100 by the Global Cybersecurity Index (GCI), ranking in the lowest category for cyber readiness. The low ranking highlights Iraq's deficiencies in legal frameworks, technical safeguards, institutional organization, and collaborative mechanisms.

Other benchmarks confirm Iraq's weak digital preparedness; on the national cybersecurity index, Iraq ranks 109th globally with an implementation score of only about 24% of recommended cybersecurity safeguards. Meanwhile, the UN's E-Government Development Index places Iraq at 148th out of 193 countries, indicating Iraq's poor online public services and poor digital governance capacity.[6] According to the World Bank GovTech Maturity Index, Iraq remains in the lower category of digital government readiness: most Middle Eastern states have moved into the top two tiers.[7] By contrast, Gulf states like Saudi Arabia and the UAE have invested heavily in cybersecurity and e-government, consistently ranking among the world's top cyber-ready nations.

Country	Cyber Budget	GCI Tier	Cyber Law	CERT	National Agency
SA Saudi Arabia	$4.1B market / $1.3B govt.	Tier 1	Yes (2017)	Yes (SACS)	Yes — NCA (2017)
AE UAE	~$590M / 30% ME market	Tier 1	Yes (2012)	Yes (aeCERT)	Yes — NESA (2012)
JO Jordan	~$80M est.	Tier 1	Yes (2015)	Yes (JoCERT)	Yes — NITC
IR Iran	Classified	Tier 3	Yes	Yes (MAHER)	Yes — AFTA
IQ Iraq	**NOT DISCLOSED**	**Tier 4**	**No (stalled since 2011)**	**Partial (2017)**	**Partial — Directorate 2025**

Table 1: Multi-Indicator Cybersecurity Readiness — Regional Comparison

Iraq's gap with cybersecurity is not just technical; it also reflects governance challenges. Freedom House, which measures democracy and rights worldwide, rates Iraq as "Not Free" in overall democratic governance with a score of 31/100.[8] In terms of internet restriction, Iraq fares somewhat better, earning a "partly free" rating. Iraq's specific score for its freedom on the net stands at 41/100, which is low, and the reasons include frequent government internet shutdowns and censorship that control and hamper online rights.[9] In 2023, Iraq led the world in internet shutdowns, recording 66 incidents, primarily during exam periods. Although

authorities defended this decision as reasonable and well-intentioned, they framed it as a way to maintain exam integrity. By shutting down the internet entirely, the move exposed a far more serious underlying issue: businesses could not operate, and people lost access to essential services. This underscores Iraq's weak and underdeveloped system for digital policymaking. International assessments show that Iraq is still highly vulnerable in cyberspace and inadequately protected against cyberattacks and lacks the institutional strength to respond effectively as those threats continue to grow.

Indicator	Iraq's Performance
ITU Global Cybersecurity Index (2021)	Ranked 129th globally (Tier 4 – low commitment); score ~53/100 (2024 update)
National Cyber Security Index (2025)	Ranked 109th globally; ~24% fulfillment of cybersecurity capacity indicators
UN E-Government Development Index (2022)	Ranked 148th globally (very limited online public services)
Freedom House, "Freedom on the Net" (2024)	Score 41/100 – Partly Free (significant obstacles to internet freedom)
World Bank GovTech Maturity (2022)	Placed in lower tier (Group C/D)—indicates below-average digital government maturity

Table 2: Iraq's Cyber Capacity in Numbers (Selected Indicators)

Current evidence shows that Iraq remains a soft target in cyberspace, lacking the resilience needed to deter attacks.[10] Iraq's poor standing in cyber defenses presents a real danger, like weak protection of infrastructure and agencies without the skills or framework to respond to the attacks, along with the inability to protect personal data. For Iraqi policymakers the message is to treat cybersecurity as national security to prevent the country from remaining perpetually vulnerable to hostile cyber activity.

Governance Structures and the Muhasasa Effect on Cyber Capacity

Why has Iraq struggled to build cybersecurity capacity? Iraq's political system divides power and resources among sectarian groups, notably the legacy of Ta'iffya, the power that has been controlling Iraqi politics since 2003. Muhassasa divides senior posts and resources and creates competition between factions rather than unified governance, which leads to weak institutional coordination. In the cybersecurity realm, it is an indication of a lack of responsibility in national cyber policy. Until recently, Iraq didn't have high-level officials in cyber policy; instead, the variation in IT experts created overlapping gaps and inefficiencies. The Estonia-based index assessment (NCSI) scored Iraq 0 out of 3 on coordination mechanisms in Iraq's government, which is the basis for cyber governance.[11]

Beyond weak institutions, corruption and political paralysis obstruct the reform. Powerful actors sometimes benefit from the status quo of weak regulation. Ambiguity allows them to exploit cyberspace for illicit economic activities and resistance to stronger oversight. As one analysis warned, those who gain from weak laws deliberately could delay progress in Iraq's cybersecurity reforms.[12] Iraq doesn't have modern cyber laws; there is no dedicated framework for personal data protection. When cybercrimes happen, cases rely on outdated codes (like the 1969 Penal Code), which don't really cover cyber crimes. A cybercrime law was introduced in parliament in 2011, but it has never been passed.[13] Political disputes and civil society have raised concern about restricting fre e speech. The present stalemate over cyber laws shows a bigger problem in Iraq's governance. Modernizing law and strengthening institutions where consensus is nearly impossible.

Significantly, ministries responsible for this area failed to sustain commitment to cybersecurity as a national imperative. This reflects a persistent mindset that has not adapted to the modern realities of cyberattacks and digital threats. Recent history has shaped priorities in security around terrorism and armed insurgency, even though cyber threats pose dangers that are equally immediate since physical terrorism requires operatives, weapons, and planning —easier to detect and stop. Iraq's government has failed to prioritize the funding for cybersecurity; instead, it continues to rely on old, obsolete technology systems with known vulnerabilities.

However, Iraq's progress in cybersecurity has unfolded step by step:

- In 2017, a national incident-response team was created.
- In 2020, policy frameworks were drafted.
- In December 2022, the Ministry of Interior approved Iraq's first national cybersecurity strategy, which led to the creation of a Cybersecurity Center.
- Finally, in 2025, this center was elevated to a Cybersecurity Directorate under Brigadier General Dr. Hassan Hadi Lazeez, marking a strategic response to digital threats.[14]

The Muhasasa power-sharing arrangement prioritized party loyalty over national interest and appointed individuals to IT and security roles based on their party affiliation rather than on their technical qualification or background. In 2025, the Minister of Communications warned that the lack of qualified cybersecurity experts is leaving Iraq further behind as cyber threats outpace defense capabilities. The lack of qualified cybersecurity personnel is obvious in the field and admitted by industry professionals.

The Iraqi government is attempting to address the skill gap through the specialized training programs for young professionals and partnerships with universities.[15] Still, developing a skilled workforce is a gradual process. Private sector leaders argue that public awareness and improving digital literacy are the first line of defense. As Asoz Rashid, CEO of Iraq's iQ telecommunications group, added, Iraq's digital expansion is outpacing public cyber awareness, showing the importance of education and good online practices.[16] In sum, problems inside Iraq's government—sectarian fragmentation and a lack of investment in society and laws—have hindered cybersecurity progress.

Building a Cyber Defense Apparatus: Progress and Gaps

Despite Iraq's difficulties, the country has started laying the foundation of the structures needed for a national cyber defense system. These efforts are still in their early stages, but they represent crucial progress toward aligning with global cybersecurity standards. A pivotal milestone was achieved when it created its first cyber incident response team, a key step toward developing CERT. By forming this team, Iraq acknowledges the significance of cybersecurity within the national security system. Progress continued in 2020, with the drafting of Iraq's initial cybersecurity framework. Yet bureaucratic delays with the emergence of COVID-19 slowed down the strategy.

Insight – Building Capacity: According to its top officials, the Cybersecurity Directorate has been actively working since it was founded, discovering 166 security weaknesses in government websites and keeping track of more than 330 criminal activities online.[17] In addition, the Directorate is also investing in society by organizing the first cybersecurity competition and large-scale training programs that reach both military/security and civilian fields. The impacts show a meaningful improvement in Iraq's ability to defend itself

with cybersecurity capabilities. Despite this progress, the threat is growing faster than the response and regulations that delay it. AI is making cyberattacks more sophisticated, and the limited budget makes it difficult to keep skilled professionals on board. Gen. Latheeth, Head of the Ministry of Interior's Cybersecurity Directorate, is saying that cybersecurity is a race —we may find ourselves defeated even before the time that the confrontation happens.

The recently developed strategy and directorates are being backed and reinforced by support from international cooperation. Iraq has worked alongside experts and organizations to essentially give its cybersecurity system a checkup. Such as NATO and the Oxford-based Global Cyber Center.[18]This kind of external assessment is valuable, as it provides maturity and guides improvement. On a regional level, Iraq is also learning from Gulf states like the UAE and Saudi Arabia for the best practices. In the year 2023, Iraq signed onto the emerging UN convention on cybercrime as a sign of intent to collaborate on international borders. Joint international programs, such as the UN's CT Teach+ program with Interpol, provide Iraq with support in educating its law enforcement and developing frameworks consistent with human rights.

On the Legal Front

Iraq lacks a contemporary legal framework specifically addressing cybercrime. Prosecutors are relying on old, inadequate legislation that was written decades ago for traditional crimes. Since there is no law to protect data, the situation shows citizens' personal information has few legal safeguards.[19] Cybersecurity tools could be turned against citizens to spy on political opponents, especially in a country where trust in state institutions is low. Both Iraqi analysts and international experts stress that cybersecurity efforts must not become a pretext to violate people's fundamental rights and freedoms. Surveillance might

help the government catch criminals or terrorists, but in the Iraqi context, it might simultaneously undermine the fragile process of rebuilding that trust between the government and its people. Iraq must walk a tightrope, balancing security with privacy. Freedom of speech and their right to express themselves freely will be essential if Iraq's cybersecurity programs are to respect their fundamental rights.

Another persistent problem is coordinating between various branches and departments in government. Iraq's federal system and Muhasasa have resulted in multiple security organizations, such as the Defense Ministry, Interior Ministry, intelligence services, and the Kurdistan Region's security authority. Government positions are distributed based on ethnic and religious quotas, which hinder sharing information smoothly. The newly created Cybersecurity Directorate is tasked with reducing this fragmentation within the government. by establishing clear protocols, working together, and responding to cyber incidents. Importantly, the team must include private companies that own the infrastructure. According to Minister al-Yasiri's announcement, the center has been given the responsibility to serve as a central authority "when a comprehensive legal framework is fully in place."[20] Provided it is given sufficient authority, the center could standardize security practices across ministries and lead unified responses to major incidents, a capability that was missing previously.

Iraq Cybersecurity Threat Matrix

Threat Category	Primary Target	Real-World Example	Potential Impact	Severity
Critical Infrastructure Attack	Oil/gas, power grids, pipelines	Lebanon supply chain attack (Sept. 2024): 42 killed, 4,000+ injured. Cited by Iraqi officials as a warning for Iraq's own systems.	Cascading failures, public unrest, loss of government trust	CRITICAL
Electoral System Interference	IHEC, voter databases, digital result systems	Iraq established a 'digital security unit' ahead of the 2025 parliamentary elections to counter espionage and sabotage.	Delegitimized elections; deepened sectarian mistrust, and foreign interference	CRITICAL
Government Data Breach	National citizen databases	2024: A threat actor claimed possession of ~30 million Iraqi citizen records on the dark web, including national IDs and family data.	Identity theft; coercion of officials and activists	CRITICAL
Government Website Defacement	Ministries of Interior, Defense, Foreign Affairs, Health	2019: ~30 Iraqi government websites defaced —described as the largest cyberattack of its kind in the country's history.	Reputational damage; propaganda spread, and exposed system vulnerabilities	HIGH
Cybercrime & Extortion	Women, youth, journalists, officials	Documented surge in blackmail schemes. Militias have used hacked compromising material (kompromat) to coerce officials and journalists.	Social harm; silencing of press; militia leverage over public figures	**HIGH**
Disinformation & Influence Ops	General public, social media users	Persistent bot networks pushing sectarian narratives. Online rumors have directly triggered real-world violence.	Incitement to violence; foreign manipulation of domestic politics	**HIGH**
Cross-Border Network Exploitation	Iraq's telecom and internet infrastructure	Iran-aligned groups reportedly use Iraqi networks as a routing launchpad to obscure the origin of attacks on other countries.	Regional conflict implication; retaliatory cyber threats; surveillance	**HIGH**

Internet Shutdowns	General public, economy, civil liberties	Authorities shut down the internet dozens of times per year —for exam periods and protest suppression — costing millions in economic losses.	Economic losses, suppressed free expression, undermined public trust	**MEDIUM**

Table 3: Critical Infrastructure, Elections & Emerging Cyber Threats

Conclusion: Implications for Iraq's National Security

The root of Iraq's cybersecurity problems is a governance failure. Even with reforms and international partnerships, Iraq's political system fragments authority, prioritizes loyalty, and neglects basic digital legislation. The Muhasasa system doesn't just slow down Iraq's cyber; it entrenches long-term structural obstruction. The establishment of the new directorates in 2025 is underway, yet it remains under-resourced, without a clear mandate or unified command —mirroring the system's flaws. Bridging Iraq's cyber weakness demands political will alongside the following recommendations, which reflect this reality:

- Cybersecurity is now integral to national security: according to the International Telecommunication Union's Global Cybersecurity Index (ITU), Iraq is ranked in Tier 4 out of 5, making it one of the least prepared nations for a potential target without physical confrontation. Cybersecurity must be given much higher priority; unlike before, security focuses more on physical threats.
- Governance reforms are essential, not optional: having advanced technology and security tools alone is not enough to be secure. Iraq's fragmented political structure leaves agencies being controlled by different political factions, which slows coordinated responses. Enacting up-to-date cybersecurity laws, defining clear agency responsibility roles, and fostering collaboration between different ministries are essential requirements for meaningful progress.

- Civil liberties must not be sacrificed for security: the Iraqi government's practice of cutting off internet service and conducting surveillance has significantly deepened the level of distrust. All future cybersecurity policies and programs must be grounded in law and monitored by independent bodies to prevent abuse. They should also establish regular advocacy groups that have a voice in shaping these policies—otherwise, they risk the credibility of the government's entire cybersecurity system.

To complement the comparative analysis, the following practitioner insights draw on an interview with Rawaz A. Muhammed

Rawaz A. Muhammed An AI, software engineering, and cybersecurity professional with over 16 years of experience, holding certifications including CISM, CompTIA SecurityX (CASP+), CCNP, HCIP, and multiple Microsoft credentials. He has authored four peer-reviewed research papers on the intersection of artificial intelligence and cybersecurity and has served as a cybersecurity trainer at the university level. He currently serves as Data Protection Supervisor at IQ Group, Iraq's largest internet service provider, where he oversees data privacy, regulatory compliance, and the protection of critical information assets across a complex telecommunications infrastructure.

From your experience in the private sector, do you see Iraq's cybersecurity challenges as primarily a technical problem or a governance and institutional one—and what are the major inefficiencies and deficiencies?

-Iraq's cybersecurity challenges are fundamentally a governance and institutional problem, not a technical one. The core weaknesses are the absence of a national cybersecurity strategy, leaving every ministry operating in isolation; no cybercrime law, meaning no legal framework to prosecute attackers or compel organizations to secure data; poor inter-institutional coordination between overlapping agencies; and political decision-making

overriding technical judgment in procurement and staffing. Technical deficiencies — outdated systems, weak monitoring, inconsistent patching — exist, but they are symptoms of these governance failures. Technology investment without governance reform is like building a house without a foundation.

The paper identifies a significant skills gap in Iraq's cybersecurity workforce, partly attributed to patronage-based appointments. From a private sector perspective, how severe is this gap, and is the private sector able to fill in where the government cannot?

-The skills gap is severe in both sectors but for different reasons. In government, patronage appointments place unqualified individuals in critical cybersecurity roles, resulting in misconfigured systems and failed incident response. In the private sector, the problem is retention — qualified professionals leave for better salaries in the Gulf, Europe, or North America. Universities also lack practical cybersecurity curricula, and international certifications receive no recognition in the public sector career structure. The private sector partially fills the gap through consultancy and managed security services but cannot replace sovereign government functions like critical infrastructure protection or national threat intelligence. It also remains too small and underdeveloped to fully compensate. Government must create an enabling environment through legislation, incentives, and education investment.

Iraq's critical infrastructure — particularly oil and gas — is largely state-owned but increasingly dependent on private contractors and technology vendors. Who is actually responsible for securing it, and is that responsibility clearly defined?

-Responsibility for securing Iraq's critical infrastructure is not clearly defined, and this ambiguity is a serious threat. State-owned entities own the infrastructure but lack the technical capacity to secure it. Foreign technology vendors maintain the systems but limit

their responsibility to equipment they installed. Private contractors provide operational support but have vague, inconsistently applied security duties. In practice, when incidents occur, response is delayed because no party knows who is accountable. This is compounded by outdated SCADA and ICS systems not designed with cybersecurity in mind, a cultural bias toward physical rather than cyber security, and contracts that lack clear cybersecurity obligations. A regulatory framework defining responsibilities, setting minimum standards such as IEC 62443 or NIST, and mandating incident reporting is urgently needed.

Iraq signed the UN cybercrime convention in 2023 and established a Cybersecurity Directorate in 2025, yet still has no cybercrime law. From a private sector standpoint, what practical difference does that legal vacuum make to how companies operating in Iraq protect themselves?

-The absence of a cybercrime law has concrete, daily consequences for private sector operations. It means no legal penalties for cybercriminals, making Iraq an attractive target; no mandatory security standards, leaving protection entirely voluntary and uneven across organizations; reduced foreign investment due to legal uncertainty; no enforceable data protection rights for individuals; a non-existent cyber insurance market due to unquantifiable legal risk; and no obligation to report incidents, causing widespread underreporting. As a data protection supervisor, best practices such as ISO 27001 and NIST are applied voluntarily, not legally. This creates a dangerous gap between security-conscious companies and those with none. The legal vacuum is not a bureaucratic inconvenience—it is a fundamental barrier to a safe digital environment in Iraq.

Given Iraq's current trajectory—the 2025 Directorate, international partnerships, and growing private sector investments—do you believe that Iraq can meaningfully close its

cyber gap? And how long would that process take? And what would have to change politically for that to happen?

-Closing the cyber gap is possible but requires fundamental political change, not just institutional steps. The 2025 Cybersecurity Directorate, international partnerships, and growing private sector activity are necessary foundations, but insufficient alone. What must change: cybersecurity appointments at all levels must be merit-based, not politically driven; a cybercrime and data protection law must be passed; dedicated cybersecurity budgets must be established; genuine public-private partnerships must replace the contractor model; a fully operational national CERT must be created; and international agreements must translate into real deliverables, not ceremonial signings. Realistically, achieving a cybersecurity posture comparable to regional neighbors would take 7–10 years; closing the gap with global leaders, 15–20 years. The most critical political shift required is for the highest levels of government — Prime Minister, Cabinet, and parliament—to recognize cybersecurity as a national security priority and back that recognition with law, funding, institutional reform, and the political will to depoliticize technical appointments. Without that, the gap will not close. It will widen.

References

1. Ward, Mark. “Iraq Conflict Breeds Cyber-War Among Rival Factions.” BBC News, 22 July 2014. Read More ↩
2. Sulaibi, Raad Khudair. "Cybersecurity in Iraq: From Digital Infrastructure Fragility to Building a National Response." ↩
3. Perlroth, Nicole. "Cyberattack on Saudi Oil Firm Disquiets U.S." *The New York Times*, 23 October 2012. Read More ↩
4. Check Point Team. "The Unraveling of an Iranian Cyber Attack Against the Iraqi Government." Check Point Research, September 2024. Read More ↩
5. Shafaq News Staff. "Iraq: A Soft Target in the Middle East's Cyber Battlefield." Shafaq News, September 2025. Read More ↩
6. United Nations Department of Economic and Social Affairs, Division for Public Institutions and Digital Government. "Iraq Country Data Profile, 2024." United Nations E-Government Knowledgebase, 2024. Read More ↩
7. World Bank Group. "2022 GovTech Maturity Index Update: Global Program on GovTech & Public Sector Innovation." World Bank, November 2022. Read More ↩
8. Freedom House. "Iraq: Country Profile – Freedom in the World 2026." Freedom House, February 2026. Read More ↩
9. Al-Dabbagh, Zeyad Samir. "Digital Transformation and E-Government in Iraq: Challenges and Opportunities." *International Journal of Social Sciences and Humanities Research Commons*, 2025. Read More ↩
10. Shafaq News Staff. "Iraq: A Soft Target in the Middle East's Cyber Battlefield." *Shafaq News*, September 2025. Read More ↩

11. Goudsouzian, Tanya, and Ibrahim Al-Marashi. "Cybercrime Is Iraq's Next Big Challenge." *Stimson Center*, November 2025. Read More ↩
12. Ibid ↩
13. Shafaq News Staff. "Iraq: A Soft Target in the Middle East's Cyber Battlefield." *Shafaq News*, September 2025. Read More ↩
14. Ibid ↩
15. Shafaq News Staff. "Cybersecurity Skills Scarcity Weakens Iraq's Digital Security." *Shafaq News*, 27 December 2025. ↩
16. Goudsouzian, Tanya, and Ibrahim Al-Marashi. "Cybercrime Is Iraq's Next Big Challenge." *Stimson Center*, November 2025. Read More ↩
17. Ibid ↩
18. Global Cyber Security Capacity Centre. "Cybersecurity Capacity Maturity Model (CMM) Review: Iraq." *Cybil Portal*, 2025. Read More ↩
19. Mohammed, Shaho. "Cybersecurity Challenges Facing Iraq's Digital Transformation." *Twejer Journal, Soran University*, 2025. Read More ↩
20. Shafaq News Staff. "Cybersecurity Skills Scarcity Weakens Iraq's Digital Security." *Shafaq News*, March 2026. Read More ↩

iNNOV8

ABOUT

Nestled in the mountains of Sulaymaniyah, the Culture Capital of KRI, iNNOV8 Research Center pioneers cutting-edge research and innovation. We aspire for excellence as an independent research center by providing valid, valuable, and timely products to the public. We deliver impactful solutions and contribute to our industry's vibrant and forward-thinking community

IRAQ'S CYBER LANDSCAPE : FRAGMENTED POWER, EXPOSED NETWORKS

CONTACT

CHANNEL8 BUILDING,

KURDSAT QTR., SULAYMANIYAH, IRAQ

+964-773-608-8885

CONTACT@INNOV8.KRD