Imam Ja'afar Al-Sadiq University Journal of Legal Studies

Volume 5 | Issue 1 Article 1

2025

The Role of Cyber Threats in Shaping National Security in Iraq

Athraa Mohammed Jaber
The Presidency of Al-Nahrain Univ, athraa.m@nahrainuniv.edu.iq

Aliaa Hameed Khayon
The Presidency of Al-Nahrain Univ, aliaahameed267@gmail.com

Recommended Citation

Jaber, Athraa Mohammed and Khayon, Aliaa Hameed (2025) "The Role of Cyber Threats in Shaping National Security in Iraq," *Imam Ja'afar Al-Sadiq University Journal of Legal Studies*: Vol. 5: Iss. 1, Article 1.
DOI: https://doi.org/10.64682/3104-9419.1108
Available at: https://ijsu.researchcommons.org/ijsu/vol5/iss1/1

IMAM JA'AFAR AL-SADIQ UNIVERSITY JOURNAL OF LEGAL STUDIES 2025;5:1–10

RESEARCH ARTICLE

The Role of Cyber Threats in Shaping National Security in Iraq

Athraa Mohammed Jaber *, Aliaa Hameed Khayon

The Presidency of Al-Nahrain Univ

ABSTRACT

Cybersecurity has become one of the most critical issues in our contemporary life due to its direct connection with various sectors of public life, such as politics, economy, security, culture, and others. Most countries rely on cybersecurity to protect their official and non-official institutions, especially their infrastructure. Focusing on cybersecurity and addressing vulnerabilities has become one of the top priorities for national security in any country.

Iraq's national security suffers from major crises, some stemming from new technological transformations, creating additional security, economic, and social burdens. Cybersecurity has emerged as a modern and vital element of Iraq's national security framework.

The most dangerous aspect of cyber threats is that they represent invisible challenges. In the age of advanced technology, information security plays a crucial role in preventing and countering cyberattacks. Iraq, especially since 2003, due to increased global connectivity and technical advancements, has become more exposed to cyberattacks and security challenges threatening its national security.

Keywords: National security, Cybersecurity, Strategy, Challenges

1. Introduction

Cybersecurity in our contemporary world has become more than merely a concern about information safety, computers, and communication networks. Due to its direct relationship with the political, economic, social, and cultural fields, most vital institutions in any country rely heavily on information technologies in their daily operations.Consequently, these institutions inherently depend on cybersecurity.

The rapid development of cyberspace, coupled with the extensive use of technology by individuals, organizations, and governments at the local, regional, and international levels, has made cybersecurity critically important and irreplaceable.

However, cyberspace is highly vulnerable to various challenges, especially cyberattacks targeting vital infrastructures.

Received 12 February 2025; revised 10 April 2025; accepted 1 May 2025.
Available online 13 May 2025

* Corresponding author.
E-mail addresses: athraa.m@nahrainuniv.edu.iq (A. M. Jaber), aliaahameed267@gmail.com (A. H. Khayon).

https://doi.org/10.64682/3104-9419.1108

The organic link between cybersecurity and cybercrime means that deliberate damage to infrastructure constitutes a direct threat to national security.

This explains why most countries have classified cybersecurity as a top priority within their national security agendas.

Since 2003, Iraq has witnessed notable development and openness in the technical and informational fields, making its institutions—both public and private—more exposed to cyber threats.

Cybercrime activities have grown, leading to new challenges that have significantly impacted Iraq's national security system.

2. Importance of the study

The importance of this study lies in the fact that cybersecurity has become one of the most critical issues for the national security of any country, due to its direct connection with its institutions, infrastructure, and citizens.

Any exposure to cyberattacks can directly impact a country's national security and may lead to significant losses.

In Iraq, the importance of cybersecurity has increased particularly since 2003, due to the widespread use of cyberspace and the simultaneous escalation of cyberattacks.

Thus, cybersecurity has become a fundamental pillar for ensuring the protection of Iraq's national security amidst evolving global technological landscapes.

3. Problem statement

3.1. This study is based on the central problem

What are the major challenges facing Iraqi national security in the era of cybersecurity?
Accordingly, the study seeks to answer the following sub-questions:

1. What is the concept of national security?
2. What is the concept of cybersecurity?
3. What is the cybersecurity strategy in Iraq?
4. What are the cybersecurity challenges affecting Iraqi national security?

3.2. Hypothesis of the study

The study is based on the hypothesis that cybersecurity has become an essential part of the national security strategy of any state.

Therefore, countries make considerable efforts to protect cybersecurity against various threats.

Nevertheless, national security remains continuously exposed to cyberattacks. Accordingly, Iraqi national security faces influential and destabilizing cybersecurity challenges that threaten its stability.

3.3. Structure of the study

First: The Concept of National Security and the Concept of Cybersecurity

1- The Concept of National Security:

First Axis: The Concept of National Security and Cybersecurity

Second Axis: Cybersecurity Strategy in Iraq
Third Axis: Cybersecurity Challenges Affecting Iraqi National Security

First: The Concept of National Security and the Concept of Cybersecurity

1- The Concept of National Security:

The concept of "security" in the Arabic language appears in sources as meaning "freedom from fear" representing a state of tranquility. It is said that one who feels safe is at ease and without fear, i.e., he is "secure" (amina). Some scholars argue that restricting the meaning of security to mere tranquility and absence of fear, as found in traditional language dictionaries, reflects a narrow and negative view that does not fully capture the true essence of security.[1]

In Arabic, the word "security" carries multiple meanings, including peace of mind, emotional comfort, a sense of satisfaction, stability, absence of fear, as well as meanings related to honesty and trustworthiness.

The term "security" appears frequently in the Holy Qur'an, in more than fifty verses, such as in Allah's saying:

In the English language, the term "security" is defined in "Webster's Dictionary" as "freedom from fear and anxiety, working in an atmosphere of reassurance and peace". The "Oxford Dictionary" defines security as "joint activities to protect a country, infrastructure, or individuals from danger or attack". Meanwhile, "Chambers Dictionary" defines it as "freedom from worry and anxiety, the elimination of danger, achieving confidence, reassurance, safety, and stability".[2]

4. The concept of security terminologically

Historically, the term "security" was not given a specific definition by early scholars, with their descriptions remaining closer to the linguistic meaning rather than to a technical one. Thus, modern definitions of security vary widely in their expressions and contents. Some define security as procedures and policies, others as a feeling or sensation, while a third group views it as a state experienced by a nation and its individuals, as will become clearer later.[3]

According to Dr. Ali Abbas Murad, the general meaning of security, both theoretically and practically, refers to:

> "peace, tranquility, the continuity of life's manifestations, and the preservation of its essential elements and conditions, away from threats."

Threat Factors and Sources of Danger In the same context, **Dr. Hamid Rabie** states that the term "security" refers to tranquility, encompassing everything related to the expression of political existence and the commitment to loyalty and obedience towards authority and leadership.[4]

The Encyclopedia Britannica defines security as "the protection of a nation from the threat of subjugation by a foreign power.[5]" Meanwhile, **Henry Kissinger** defines it as "any actions by which a society seeks to preserve its right to existence."[6]

5. The concept of national security

The concept of national security is closely linked to the concept of the state and to the social, economic, and political structure of societies, as well as to internal and external threats, whether potential or actual, against this structure. It also relates to the overall

public interests of society and the state within a regional and international environment where conflicts and imbalances of power occur.

National security is not necessarily directed solely against external threats, but also addresses internal threats, including social and economic issues.

Internal cohesion is a fundamental process for social resilience against both internal and external threats. Thus, national security refers to a state's ability to maintain its territory, economy, natural resources, and various systems—political, social, and economic.

From the perspective of **Harold Brown** in his famous book Thinking About National Security, national security is defined as:

> "the ability to preserve the nation, its dignity, territory, economy, protect its natural resources, and safeguard its constitution from any external aggression."[7]

The main problem with the concept of national security lies in the practical programs aimed at enhancing national security in many countries, as these often focus on certain aspects of the issue while neglecting other crucial factors. The solution lies in adopting a comprehensive concept that emphasizes the need for a balanced consideration of multiple internal and external factors, all of which inevitably influence the formation of a secure state.[8]

Thus, national security has two concepts: a narrow, negative one and a broad, positive one.The comprehensive concept of national security includes what is indicated by the narrow concept but extends beyond it to wider dimensions.[9]

Kegley and Wittkopf define national security as: "A sense of reassurance provided by the objectives and programs through which the government seeks to ensure the nation's security and survival in an international environment that is very likely to harbor hostile elements."[10]

The comprehensive concept emphasizes the importance of the international environment as a framework that contains fundamental variables affecting national security.It alerts that the international environment may harbor elements that can pose direct or indirect threats to the national security of a state. At the same time, it asserts that the factors most strongly influencing a nation's security are connected to the nature and characteristics of its own internal environment (political, economic, social, etc.).[11]

2- The Concept of Cybersecurity:

Linguistically, it is important to first understand the origin and meaning of the word "cyber." It refers to the method of communication and control among machines and living beings, From this word, many terms emerged, commonly used in science fiction stories and films related to cyberspace a virtual or imaginary space often associated with the Internet and Accordingly, the U.S. Department of Defense (the Pentagon) provided a definition for the term cybersecurity, considering it:

All the necessary organizational measures to ensure the protection of information in all its electronic and physical forms from various crimes, attacks, sabotage, espionage, and incidents.Similarly, Richard Temmer defines cybersecurity as:

Defensive means aimed at detecting and thwarting hacking attempts, Meanwhile, Edward Morceau defines it as, Means designed to reduce the risk of attacks on software, computer devices, or networks, including the tools used to combat hacking and detect viruses.[12]

The International Telecommunication Union (ITU), in its report Trends in Telecommunication Reform (2010–2011), defines cybersecurity as A set of tasks that include collecting security tools, policies, procedures, and guidelines to protect the cyber environment, organizational assets, and users, Based on the above, cybersecurity can be defined, based on

its objectives as The activity that ensures the protection of human and financial resources related to communication and information technologies, guaranteeing the ability to reduce potential losses and damages in case risks and threats materialize, and enabling the swift restoration of the situation to its original state, thus preventing damages from turning into permanent losses. Achieving an adequate level of information security to face technological and informational risks is essential for the proper performance of governments and organizations.[13]

In essence, cybersecurity is A collection of mechanisms, procedures, tools, and frameworks aimed at protecting software and computer systems from various attacks and intrusions that may threaten national security.[14]

Second: The Cybersecurity Strategy in Iraq

Iraq's cybersecurity strategy is based on a fundamental principle: ensuring the security of Iraq and protecting its existence in cyberspace, safeguarding critical information infrastructure, building a trusted Internet community, nurturing it, and addressing cyber challenges that may affect Iraq's national security and integrity through fulfilling a set of key objectives, The measures aim to protect and defend Iraq's cyberspace.

Official statistics on cybercrimes in Iraq began to be recorded in 2006 due to the rapid spread of online services and operations, which led to an increase in Internet crimes and activities harmful to Iraq's system and society, In fact, Iraq has the highest rate of cyber piracy in the Middle East.

The types of cybercrimes in Iraq have varied, including:[15]

- Online fraud,
- Money laundering,
- The rise of hacking websites,
- Illegal cyber trade,
- Network intrusions,
- Cyberterrorism.

Accordingly the technological development Iraq witnessed in the field of information and communications after 2003 was accompanied by weak electronic security and fragile infrastructure, making Iraq strategically exposed to many countries, This vulnerability made it easy to penetrate and spy on institutional information, to the extent that Iraq became a launching ground for cyberattacks targeting the information security of other countries and their electronic security systems, Furthermore, information theft and its use for purposes of blackmail, or for executing and supporting hacking operations, became prevalent.

It is also notable that most Iraqi institutions contract for their information services through satellites operated by service providers based outside Iraq.

As a result, Iraqi data flows through servers in foreign countries before returning, causing a serious breach of Iraq's information security. o avoid such serious breaches in the flow of information, it is necessary to build a comprehensive information security system.[16]

Thus, Iraq must establish an electronic security system aimed at protecting its national cyberspace, ensuring the availability of information systems, strengthening privacy protections, safeguarding the confidentiality of personal data, and taking all necessary measures to protect the security of citizens and institutions from the risks present in cyberspace.[17]

Accordingly, the national cybersecurity strategy in general can be defined as: All measures related to the confidentiality of information and data that are processed, stored, and transmitted through electronic or similar means.

And to protect them, along with the systems associated with them, from external or internal threats.

This strategy aims to develop and implement cybersecurity capabilities to enhance and sustain the following areas: [18]

1. Protecting citizens' privacy and other data from loss, harmful alterations, and unauthorized use.
2. Enhancing the resilience of government services, systems, and infrastructure against cyber threats.
3. Ensuring government continuity during and after serious cyber incidents.
4. Safeguarding the security of digital services provided to citizens.
5. Coordinating responses to threats against infrastructure.
6. Securing and ensuring the safety of the government's critical infrastructure.

The issue of cybersecurity is considered one of the critical and sensitive issues directly linked to the national security of every state, whether individually or collectively, Thus, no country in the world—whether developed or developing—can afford to neglect or ignore this matter, Given the importance of having a national cybersecurity strategy, Iraq is in urgent need of establishing such a strategy.

Third: Cybersecurity Challenges Impacting Iraq's National Security

The unstructured challenges to national security generally consist of the various factors that pose a direct threat to the foundational values and infrastructure of any society.

Iraq's national security faces a number of cybersecurity challenges that pose a direct danger to the strategic security system, We can observe and directly sense the dimensions and impacts of these challenges,The most significant threats to Iraq's national security strategy are often those whose impacts aren't immediately visible to national security units. Among these are the "invisible" challenges that affect key strategic sectors of the state, such as infrastructure, which directly impacts citizens' lives. Additionally, [19] looming threats to Iraq's digital systems, particularly cyber threats are of paramount concern. [20]

Cyber threats represent unseen challenges that influence Iraq's national security framework. In today's technological era information security plays a pivotal role in repelling and preventing cyberattacks that could target various state systems. It's also essential for protecting operational systems from unauthorized access with malicious intent. Since 2013, Iraq has witnessed technological advancements in information and communications. However, this progress coincided with a lack of robust cybersecurity measures within the national infrastructure be it security, banking, or personal systems. This vulnerability has rendered Iraq strategically exposed to numerous global entities, making it susceptible to breaches and espionage targeting sensitive information within security institutions. Moreover, Iraq has been exploited as a platform for launching cyberattacks against other nations, compromising their information security. Such breaches also facilitate the theft of information for purposes like blackmail or supporting terrorist activities. Notably, many Iraqi institutions procure their data services from satellites operated by providers based outside Iraq. This practice results in data transmission through foreign servers before returning to Iraq, posing significant risks to the nation's information security. To mitigate such substantial breaches in Iraq's data flow, it's imperative to establish a comprehensive information security system. Therefore, Iraq's cybersecurity framework should encompass legal and regulatory structures, organizational frameworks, and technological tools. This collective effort should involve both the public and private sectors, domestically and internationally, aiming to safeguard Iraq's digital sovereignty.

Protection of the national cyberspace focuses on ensuring the availability of information systems, strengthening privacy measures, safeguarding the confidentiality of personal information, and taking all necessary actions to protect citizens from the dangers of cyberspace.[21]

Official statistics on cybercrimes in Iraq began to be recorded in 2006 due to the rapid expansion of online services and activities. With this growth came an increase in cybercrimes and harmful activities that affect Iraq's system and society. In fact, Iraq has the highest rate of cyber piracy in the Middle East. The types of cybercrimes observed in Iraq include online fraud, money laundering:[22] the rise of hacking websites, illicit cyber trade, network intrusion, cybersex crimes, and cyberterrorism.

According to records from the Iraqi Criminal Investigations Office covering the years 2006 to 2011, there was a steady increase in cybercrime cases in Iraq, with an average annual growth rate of approximately 2,246%. This period also saw a rapid rise in internet users, which coincided with an increase in cybercriminal activities.

Most of these crimes were committed by individuals holding high school diplomas (63.4%), followed by those with bachelor's degrees (27.8%), while the remaining 8.8% were committed by others. Theft represented the highest proportion among these cybercrimes. Youth made up the largest demographic of offenders, with 44.8% of the crimes committed by individuals under the age of 24. Males were overwhelmingly the perpetrators, responsible for 81.1% of all cybercrimes in Iraq.

These indicators clearly show that cybercrime prevention programs in Iraq should focus heavily on youth and adolescents. Additionally, Iraq's internet market remains largely unregulated, which is largely attributed to the country's transitional phase and prevailing security conditions. These factors have severely impacted the infrastructure of internet services, compelling users to rely on multiple, often uncoordinated, sources for internet access.

It is also evident that Iraq is still in the early stages of addressing cybercrime effectively.[23]

This type of crime has not traditionally been a primary concern of Iraqi society. However, the Iraqi Ministry of Planning announced that in 2013, a large portion of cybercrimes committed involved the use of social media platforms, especially Facebook. These crimes included kidnapping, threats, breaches of personal information, drug-related activities, fraud, and more. Some individuals involved in these cybercrimes were arrested.

It is noteworthy that, coinciding with the war against the terrorist organization ISIS starting in 2014, cybersecurity firms observed the emergence of a cyberwarfare front in Iraq. Social media platforms were increasingly used for mobilizing supporters, spreading propaganda, and collecting security-related information through groups of hackers. These hackers deceived individuals by sending manipulated messages and malicious software via social media. Once opened, the attackers would gain full control over the victim's device stealing files, or using the computer's camera or microphone to monitor the target.

In this context, **Andrew Komarov**, CEO of the U.S.based cybersecurity firm IntelCrawler, stated that some groups in Iraq were using malicious software, and identifying them was difficult. These groups had already targeted specific cities, communities, and even families. The attacks were highly selective and largely influenced by the ongoing internal conflicts. He added that the attackers focused on victims via social media and also searched for routers inside Iraq to sabotage them or gain unauthorized access,[24] Most of these cyberattacks were concentrated in Baghdad, Basra, Mosul, and Erbil. Their aim was to collect intelligence about local protests, political parties, and communications between civilians and government bodies, and vice versa. IntelCrawler had collected this information through monitoring Iraqi cyberspace activity and regional security communications,[25] Additionally, a 2014 report by **IntelCrawler** confirmed that actors based in Iraq were

involved in various illicit cyber activities and operated as mercenaries. These activities had significantly increased, and the individuals involved had connections with other groups both within and outside Iraq.

From countries such as Egypt, Lebanon, Libya, Iran, and Syria as well as through the actions of Islamic groups spread across various nations cybersecurity analysts have observed that factions linked to terrorist organizations, including ISIS, have launched cyberattacks against multiple countries around the world. These attacks have targeted media outlets, government institutions, universities, companies, and non-governmental organizations. This has sparked debate among Western experts regarding what they describe as a "cyber jihad" being waged by terrorist organizations against the West.

In this regard, the U.S. Federal Bureau of Investigation (FBI) issued a warning on April 7, 2015, confirming that continuous disruption of search engines was being carried out by individuals sympathetic to ISIS. These operations impacted search engines and social media platforms used by news agencies, commercial enterprises, religious institutions, and both federal and local governments in various Western countries. Aside from the damage caused, removing the effects of these cyberattacks has proven to be costly.

The cyberwar against ISIS has served as a practical test for the future of cyberwarfare against terrorist groups, violent extremist movements, insurgents, and transnational criminal organizations. In this context, cyberattacks have played a significant role in thwarting terrorist operations. In reality, cyber threats represent invisible challenges that affect Iraq's national security system. [26]

Although Iraq has opened up to the world and witnessed technological progress especially in communications and information the country still suffers from weak infrastructure when it comes to cybersecurity. This vulnerability has left Iraq exposed to infiltration and espionage by numerous foreign actors, particularly in areas concerning security institutions, To address this, Iraq has worked with international partners to enhance its cybersecurity capabilities by drawing on their expertise. Specifically, the Iraqi government coordinated with the North Atlantic Treaty Organization (NATO) to train 16 members of the Cyber Incident Response Team from November 21 to December 2, 2016. The training program included theoretical sessions and hands-on lab exercises focused on the fundamentals of cyber defense, data leak protection, cryptographic analysis, digital evidence handling, and enhancing technical expertise for cybersecurity protection.

The national network and increased awareness of cybersecurity are key components in strengthening Iraq's national cyber defense capabilities. These training programs are expected to enhance Iraq's overall cybersecurity resilience. [27]

It is noteworthy that Iraq ranked 158th globally according to the 2017 Global Cybersecurity Index (GCI), issued by the International Telecommunication Union (ITU), the United Nations' specialized agency for information and communication technologies. In 2018, Iraq improved its standing to 107th globally out of 175 countries surveyed, and ranked 13th among Arab countries, indicating positive progress in the country's cybersecurity efforts and reflecting the success of those managing this sector.

In general, the key challenges facing cybersecurity and internet networks in Iraq and potential solutions can be summarized as follows: [28]

1. Weak legal and regulatory frameworks governing information and cybersecurity in Iraq. There is an urgent need to adopt effective legal legislation that can be applied to both the public and private sectors. The government must implement specific security measures across its ministries and institutions. Additionally, involving the private sector is crucial to collectively strengthening Iraq's information and cybersecurity posture.

2. Lack of skilled local professionals in the fields of advanced information security and cybersecurity. This issue requires serious efforts to train and develop a qualified professional workforce in both the public and private sectors capable of addressing cyber challenges.
3. Dependence on foreign internet infrastructure, meaning that Iraq's cybersecurity is ultimately reliant on other countries and external companies. To address this, the Iraqi government should establish effective partnerships with local companies to build trustworthy and efficient relationships that fill existing gaps in this domain.

6. Conclusion

In conclusion, Iraq's openness particularly in the fields of technology and information and its increasing reliance on digital infrastructure have introduced multiple challenges to national security. As Iraq continues to be a primary target of terrorist organizations, both official and unofficial institutions have experienced several breaches and cyberattacks. Among the most pressing challenges confronting Iraq are terrorism and cyber threats. This situation necessitates intensified efforts to enhance and develop a comprehensive cybersecurity strategy and improve national capabilities to counter terrorism and electronic threats.

7. Recommendations

1. Iraq should adopt a national cybersecurity strategy to safeguard national security and protect the Iraqi state in cyberspace.
2. Cybersecurity must be recognized as an integral part of Iraq's national security responsibilities.
3. There is a pressing need to develop Iraq's electronic security to confront the invisible cyber challenges that significantly affect national security agencies.
4. Measures and procedures must be developed to bridge the cybersecurity gap and address its core vulnerabilities.
5. Establish a centralized platform for cybersecurity operations, and increase awareness of cybersecurity and its implications for Iraq's national security.
6. Rely on the Iraqi Cyber Incident Response Team during this phase and work on drafting relevant legislation for cyberspace governance.
7. Promote Iraq's presence in global cybersecurity forums and pursue international cooperation in the field.

Conflict of interest

The authors declare no conflict of interest.

References

1. Muhammad ibn Abi Bakr Al-Razi, Mukhtar Al-Sihah, Dar Al-Kitab Al-Arabi, Beirut, 1st Edition, 1981, p. 26.
2. Adel Abdul-Hamza Thujail, National Security and Human Security: A Study in Concepts, Journal of Political Sciences, College of Political Science, University of Baghdad, Issue (51), 2016, p. 327.
3. Sabah Mahmoud Muhammad, Islamic Security: Studies in Geopolitical Challenges, Al-Mu'assasa Al-Jami'iya for Studies, Publishing, and Distribution, Beirut, 1st Edition, 1994, p. 8.

4. Hassanain Jassim Mohammed Al-Khafaji, The Security Strategies of Iraq's Neighboring Countries and Their Impact on Iraqi National Security After 2014, Unpublished Master's Thesis, Al-Nahrain University, College of Political Science, 2020, p. 8.
5. Ali Abbas Murad, Security and National Security: Theoretical Approaches, Ibn Al-Nadim Publishing and Distribution, Algeria, 1st Edition, 2017, p. 15.
6. Hamid Rabie, The Theory of Arab National Security and the Contemporary Development of International Relations in the Middle East, Majid Publishing House, Cairo, 1984, p. 37.
7. Hassanain Jassim Mohammed Al-Khafaji, The Security Strategies of Iraq's Neighboring Countries and Their Impact on Iraqi National Security After 2014, previously cited source, p. 10.
8. Saad bin Ali Al-Shahrani, Managing Security Crisis Operations, Naif Arab University for Security Sciences, Riyadh, 1st Edition, 2005, p. 15.
9. Thiyab Mousa Al-Badayneh, National Security in the Age of Globalization, Naif Arab University for Security Sciences, Riyadh, 1st Edition, 2011, p. 24.
10. Ahmed Abdul Karim Abdul Wahab, Mahmoud Abdul Rahman, The Problematic Nature of Cybersecurity and the Restricted Regulation of Freedoms, Journal of Political Issues, College of Political Science, Al-Nahrain University, 2020, Issue 60, p. 4.
11. Adel Abdul Moneim, Information Security and National Security, International Politics Journal, 2018, Issue 213, p. 202.
12. Ibn Marzouq Antra, Harshaoui Mohiuddin, Cybersecurity as a New Dimension in Algerian Defense Policy, p. 66, Link: https://dspace.univ-ouargla.dz/jspui/handle/123456789/14052.
13. Adel Abdul Moneim, Information Security and National Security, International Politics Journal, 2018, Issue 213, p. 203.
14. Mona Al-Ashqar Jabbour, Cybersecurity: Challenges and Requirements for Confrontation, Arab Center for Legal and Judicial Research, League of Arab States, Beirut, 2012, p. 2 and onwards.
15. Mustafa Ibrahim Salman Al-Shammari, Cybersecurity and Its Impact on Iraq's National Security, Journal of Legal and Political Sciences, Issue 1, 2021, p. 170.
16. Noor Ali Sakb, Iraq's National Security Under Cyber Infiltration (Information Security), Journal of the College of Law and Political Science, Issue 4, 2019, p. 9.
17. Ahmed Youssef Kattan, The National Cybersecurity Strategy of China: A Reading into the Chinese Cybersecurity Law, Al-Nahrain Center for Strategic Studies.
18. Salah Mahdi Hadi Al-Shammari, Zaid Mohammed Ali Ismail, Cybersecurity as a New Pillar in Iraqi Strategy, Journal of Political Issues, Al-Nahrain University, College of Political Science, Issue 62, 2020, p. 285.
19. Ayman Al-Hayari, "What is Cybersecurity? What are its Standards? And What is its Importance?" Published online at: https://www.mah6at.net. 09-03-2019.
20. Aliya Hamid Khayoun, "Cybersecurity and the Strategy to Combat Terrorism in Iraq," Conference on Iraq's Strategy to Combat Terrorism: From Confrontation to Prevention, Counter-Terrorism Service, Baghdad, First Edition, 2022, p. 589.
21. National Security Advisory, Iraqi Cybersecurity Strategy, published online: https://www.itu.int/en/ITU.
22. Marwan Salem Al-Ali, Challenges and Strategy of Iraqi National Security Amid International Changes, Tikrit Journal of Political Science, Issue 20, 2020, pp. 58–60.
23. Aliya Hamid Khayoun, op.cit, p. 591.
24. Hassan Saad Abdul-Hamid, Public Policies to Combat Terrorism in Iraq After 2003, The Arab Democratic Center for Strategic, Political and Economic Studies, Germany, First Edition, 2017, p. 27.
25. Marwan Salem Al-Ali, Previously Cited Source, p. 61.
26. Asaad Tarish Abd Al-Ridha et al., Cybersecurity and Its Role in the Spread of Terrorism in Iraq After 2003, Journal of International Studies, Issue 80, 2019, p. 159.
27. Jawhar Al-Jamousi, The Virtual and the Revolution: The Role of the Internet in the Emergence of an Arab Civil Society, Doha, Arab Center for Research and Policy Studies, 2016.
28. Mona Al-Ashqar Jabbour, Cybersecurity: Challenges and Requirements for Confrontation, Beirut, League of Arab States, Arab Center for Legal and Judicial Research, 2012, p. 33.