Intersections of Faith and Culture: AMERICAN Journal of Religious and Cultural Studies
Volume 4, Issue 04, 2026 ISSN (E): 2993-2599

The International Legal Framework for Combating Cybercrimes Affecting National Security and The Judicial Cooperation Between Countries

Sawsan Hussein Abed
Babylon Technical Institute, al-Furat al-Awsat Technical University
sawsan.abed.iba@atu.edu.iq

Abstract: The purpose of this research is to provide an analytical study of the international legal framework for combating serious electronic crimes in national security, focusing on the current Iraqi legislation within this framework in the light of the rapid changes known in cyberspace. The research starts from determining the legal concept of electronic crimes affecting national security through the connection between the attack on digital infrastructure, communication networks, money and energy and the violation of the constitutional rights to life, security and freedom, explaining how to expand the traditional protection of national security to include the digital space as part of the strategic sphere of the state. The research is based on descriptive, analytical and comparative analysis of the provisions of the Iraqi Constitution, the Anti-Terrorism Law No. 13 of 2005, the Anti-Money Laundering and Terrorist Financing Law No. 39 of 2015, the Penal Code, and the Law on Principles of Criminal Trials, and then comparing them with what is established in the international agreements related to combating organized crime, money laundering, terrorist financing, and information crimes. The research covers the role of international and regional organizations in the drafting of the regulatory standards for the digital space and the justification of the national legislator for the number of draft laws on electronic crimes, while stopping at the major observations and criticisms raised around the legislative formulas that may lead to the expansion of criminalization at the expense of digital rights and freedoms. Also, the research addresses the forms of judicial cooperation between countries in the prosecution of electronic crimes of national security, through the study of the mechanisms of mutual legal assistance, the surrender of the accused, the exchange of digital evidence, and the formation of joint investigation teams, and the analysis of the legislative, technical, and institutional challenges we face related to the dualization of criminalization, jurisdiction of the judiciary, the validity of digital evidence, and the protection of confidentiality and personal information. The conclusion of the study is that building an effective protection for national security in the face of electronic crimes requires a balanced development of the national legislative system and the activation of the obligations of the convention and the strengthening of the capacities of justice institutions and technical agencies to deal with digital evidence, while a comprehensive approach to meet the requirements of cyber security and at the same time ensure respect for rights and freedoms in the digital environment.

Keywords: electronic crimes; national security; Cyber Security; international judicial cooperation; international agreements; Digital evidence

Introduction

Section One: The Conceptual Framework of Cybercrimes Affecting National Security

To effectively tackle cybercrimes that undermine national security, it is necessary to create a clear conceptual framework that separates concepts that have close relationship like information crime, cyberthreats and attacks on critical communication infrastructure, energy infrastructure and financial infrastructure. The ambiguity of these concepts has a detrimental impact on the accuracy of

criminalization and efficacy of legal safety. This part seeks to provide a systematic description of the basic components that make up the concept of cybercrime where it compromises national security by elucidating its technical nature; the nature that makes it transnational, fast spreading, and hard to trace, and by relating these nature to the constitutional, criminal, and procedural aspects of national security. The differences between the attacks whose consequences are restrained to personal or economic gains, and the ones whose impact is related to the state stability, political integrity, and trust of people in its administration are also discussed, which allows developing an objective criterion according to which it is possible to distinguish between common cyberattacks and those that begin to affect the level of the infringement of the state security. This theoretical framework is the key to the interpretation of how national laws and international norms react to this phenomenon and how the weaknesses and strengths of the legal system under consideration are to fight the strategically important cybercrimes.

Part I: The Legal notion of Cybercrimes and its effect on the national security. The legal term of cybercrimes that damage the national security starts with the understanding that state security has ceased to be confined to safeguarding its land, sea, and air borders, but has extended to the virtual world where networks of communication, banking, energy, and governmental administration are located. The use of computer and communication systems-or any other digital setting- as an instrument or vehicle of perpetrating a criminal act which leads to an injury to an interest safeguarded by law is the basis of a cybercrime, in legal terms. In case of national security, this interest is translated to the stability of the state, its political unity, integrity of its critical infrastructure, and the trust of its people in its institutions. In this meaning, any aggressive action that uses digital tools with the purpose to interrupt state facilities, paralyze its services or cause fear and chaos among the population is considered as cybercrimes related to national security, although the act does not result in direct physical destruction.

The conceptual aspect of these crimes is seen as clear when the constitutional rights to security and basic rights are associated with the aggressive actions that involve the use of the digital space to execute the attack. Article 15 of the constitution of the republic of Iraq of the year 2005 provides that all persons have a right to life, safety and liberty and no one can be denied such right without the law and by a judicial decision, giving to the right to security an individual and general nature. Provided that cyberattacks occur to the digital infrastructure people depend on to access the basic services like electricity, banking, and communications networks, it would influence the very nature of this right and turn the attack on an information system into a direct attack on the right of society to security and stability. Therefore, cybercrime is broadened to comprise of any digital behavior, which subjects these constitutional rights to physical or potential threat whenever it is deliberate and hostile in nature.

Article 38 of the Constitution introduces another facet of the legal notion of such crimes since it requires the state to ensure freedom of expression and freedom of the press and media by any means provided that the freedoms do not contravene the state order and morality. With such a limitation, it is possible to draw the line between the digital content falling in the realm of the lawful expression of opinion and participation in the public debate and that content that, due to its content, intent, and the tools of its delivery, becomes a tool of destabilizing the state or causing hatred or violence or instigating sectarian conflict. The utilization of digital space to spread the systematic calls to attack critical facilities or even organize widespread disinformation campaigns that damage the reputation or even disrupt the normal operation of information systems that may endanger peace and security in the state may be considered a type of cybercrime against national security since the resulting threat extends beyond damaging reputation or the normal operation of information systems.

Reading these constitutional provisions in light of modern technological developments allows for the formulation of a composite concept of cybercrime that harms national security, based on interrelated material and moral elements. The material element consists of any unlawful use of information systems, networks, or digital platforms that leads to damaging infrastructure, endangering public security, or creating a state of confusion and disruption in the performance of the state's vital facilities. The moral element consists of the offender's intent to direct these acts toward harming security or stability, whether this occurs directly through infiltrating and disrupting systems or indirectly by

exploiting public opinion through extensive digital incitement campaigns. This definition entails that cyberspace is no longer a neutral medium for data transmission but has become part of the state's strategic domain, and any organized attack on it acquires the characterization of a crime related to national security whenever the legal conditions governing the balance between safeguarding this security and respecting constitutional rights and freedoms in the digital environment are met [1].

The interpretation of the legal notion of cybercrimes in the context of the national security also brings to the fore their complex character, at once, both harming individual interests and damaging the supreme ones of the state. These crimes can be categorized based on the object of the attack into those that target the vital infrastructure includes energy, water and communication systems; those that impact state information systems and sensitive information held within them and those that erode public trust in the financial and administrative system. A crime might be achieved simply by getting unlawful access to an information system of a strategic facility prior to the actual sabotage but as a component of a larger hostile program to collect intelligence data to be used to further attacks. This renders the simple violations of online security fences a deliberate offence that is directly linked to national security.

The effects of cybercrimes on national security can also be seen in its growth over time and space than traditional crimes since the nature of digital space could enable the initiation of simultaneous attacks on several facilities within the state or even in several states simultaneously. The consequences they produce might also remain even after the initial act is over because of the distrust they create towards systems and services. An attack on the control system of the electricity grid, such as, does not restrict its threat to a temporary power outage but spills to disrupting hospitals, transportation facilities, and communications, and the social and economic disruption that can require an extended period to clean up. In turn, the idea of cybercrime as a threat to national security should reflect this chronological character of damage, which regards the digital act as a part of the system of structures and does not attribute it to an individual circumstance independent of all other elements of the national system.

These factors prompt the need to revisit the nature of criminal responsibility of cybercrimes to national security to ensure that the responsibility of such crimes does not end with the individual who commits the offense but goes further to include organizations that violate key preventive duties in the operation and maintenance of digital infrastructure. The owners of electronic payment systems, internet service providers and administrations that handle the security of government networks are all stakeholders of the protection equation and their laxity in enforcing standards of safety, oversight and risk management leaves loopholes through which attacks against national security can be successfully executed. This solution supports the tendency to introduce special obligations into these entities in the legislative acts on communications and cybercrimes and to connect the serious violation of these obligations with general legal responsibility in case it is established that such violations were a primary cause of the successfulness of cyberattacks on national security, thereby making the legal notion of crime in this area to correspond to the technological and political reality in which the state will be functioning in the era of the digital world.

Section Two: The Evolution of Cyber Threats in International Legal Practice

The transformation of cyber threats in international legal practice can be viewed as the transition of crimes against the national security and the traditional conceptual framework of using direct physical force to the new one, when digital space and information networks are used to accomplish the same goal, i.e., to weaken the internal state and to endanger the safety of the society and the state. The digital revolution and the proliferation of sophisticated platforms and software has resulted in the appearance of aggression forms that do not presuppose the physical presence of the aggressor in the area of activity of the targeted systems, since the possibility to access the systems and manipulate or interfere with data streams is enough. This development has influenced security literature in international organizations and the provisions of many conventions and resolutions that now address cyberattacks as one form of transboundary threats directed against international peace and security. Thus, international legal discourse began linking the concepts of terrorism and organized crime on

the one hand, with the cyber nature of the tools of execution on the other, in light of the growing instances in which digital infrastructure has been used to target the security of states and their vital facilities [2].

The Anti-Terrorism Law No. 13 of 2005 is a clear reflection of this shift in the national legislative framework in light of the international legal experience. The definition of terrorism in Article 1 of the law as a criminal act committed to disrupt security, stability and national unity and to create fear among people in order to achieve terrorist goals is relatively broad and includes acts that use cyberspace as the main medium for carrying out the attack, as long as the intent is to weaken stability and security. In this context, hacking the websites of ministries and sovereign bodies, the databases of security forces, or the voting systems may be categorised as terrorist acts if the intent is to undermine public confidence in the state or to bring about a situation of political or security instability. This interpretation is consistent with international reports that highlight that terrorism no longer only involves the use of explosives and armed attacks, but also planning, financing, recruitment, propaganda, and partial or full execution of terrorist actions through cross-border cyber platforms.

The law's Article 2, Paragraph 1 and Paragraph 2 further strengthen this link between the notion of terrorism and cyber threats when they define terrorist acts as the commission of violence or threat with an intention to create terror, endanger security and destroy public buildings and facilities. The digital equivalent of these acts include cyberattacks on power plants, oil refineries, and critical service facilities through penetration of industrial control systems, manipulation of operating data or destruction of these data in order to shut down these facilities. If a cyber assault leads to blackouts in power supply, national shutdown of telecommunications or a major disruption to the banking system, the effect, in this case, is equivalent to bombing a power station or burning a public building.This has driven international legal practice to recognize cyberspace as a new arena for executing traditional forms of crimes that affect national security. Several international instruments have adopted this view by emphasizing the need to protect critical information and communication infrastructure as part of the national security system of each state [3].

The development of cyber threats in international legal practice is also reflected in the growing discussion about the criterion for legal qualification of cyberattacks: whether some types of these attacks should be qualified as acts of war, acts of terrorism or merely organised transnational crimes, and the subsequent differences in the legal regime and international responsibility. Some of the guidelines and reports of international organisations have followed an approach that takes into account the nature of the target, the level of harm and the purpose of the attack to determine whether it constitutes an attack on national security or international peace. This approach has resulted in states introducing changes to their anti-terrorism and transnational crime laws to cover cyberattacks, and commencing the negotiation of agreements to promote cooperation in tracking down offenders, gathering digital evidence and sharing such evidence. This is indicative of the evolution of international legal practice from considering cyberspace as a neutral technological environment to seeing it as a strategic environment that needs special rules for protection in the national and collective security of states.

The development of cyber threats in international legal practice is also expressed in the increasing involvement of non-state actors in using cyberspace for hostile activities impacting the national security of states. Terrorist groups and criminal networks are increasingly exploiting open and encrypted channels to plan and implement activities, recruit new members, disseminate propaganda, raise funds, and transfer money through untraceable financial technologies. This widespread utilization of new technologies has led some states to extend their criminal jurisdiction to acts committed outside their territory by foreign nationals if these acts have a significant impact on their domestic security. It has also facilitated the adoption of innovative forms of judicial cooperation that enable the exchange of information regarding user identification and connections within a legal framework. In this regard, the focus has shifted from considering only the material conduct of the cyberattack to considering the entire sequence of digital activity that culminates in the attack, from incitement and preparation to actualisation and the use of the results of the cyberattack to threaten

peace and security on the national and international levels.

This shift in the nature of threats is paralleled by the development of soft regulatory instruments in international legal practice aimed at formulating general principles of responsible conduct in cyberspace, but not yet a comprehensive treaty binding on all states. Some international and regional bodies adopt documents that recommend states refrain from attacking the critical information infrastructure of other states in peacetime, take measures to ensure their territory is not used to launch cyberattacks against other states, and respect fundamental human rights when implementing cybersecurity measures. While these documents are usually not directly binding, their frequent referencing in statements and decisions of international bodies helps them to become gradually institutionalised as normative sources that courts and national authorities can rely upon in interpreting state obligations in the area of countering transboundary cyber threats.

International legal practice also shows that the nature of cyber threats has forced states to deal with a sensitive question regarding the attribution of cyberattacks to individuals or groups, due to the technical and legal problems associated with the verification of their origin - referred to as the attribution problem in cyberspace.This difficulty not only affects the ability to hold individuals and criminal networks accountable, but also extends to the domain of state responsibility when states are accused of hosting or supporting hostile cyber operations that harm the national security of other states. In response to this issue, numerous practices have moved toward strengthening cooperation among technical, judicial, and diplomatic bodies to build more coherent evidence regarding the origin of attacks, and toward developing consultation frameworks prior to taking countermeasures that may provoke political or security tensions. This trend reflects a growing awareness that addressing cyber threats cannot be merely a security or technical matter, but rather a complex legal and political process requiring precise international coordination to balance the protection of national security with respect for the rules of international law [4].

Section Two: The International Legal Basis for Combating Cybercrime

In considering the international legal framework for the fight against cybercrime, we should start from the premise that cyberspace has become a collective space in which the interests of states converge and in which threats are interconnected beyond national borders, making it impossible to rely solely on national legislation to ensure the protection of national security against organized cyberattacks. Given the use of networks and information systems to fund, plan and commit crimes of a transboundary nature, there has been a need to build an international treaty regime that sets out common rules for criminalization and sets forth principles for judicial and law-enforcement cooperation, as well as principles for the exchange of evidence and technical information. This section aims to examine the most relevant international and regional instruments that have dealt with cybercrime directly or indirectly, and to explain how they have helped to consolidate or harmonize legal notions concerning attacks on information systems and data, as well as to outline the obligations imposed by these treaties on states regarding criminalization, prevention, and international cooperation. This overview helps to establish the role of national legislation in this normative framework, and to evaluate to what extent it is in line with the international legal practice in the area of combating cybercrimes that affect national security.

Section One: International Conventions Addressing Cybercrime

The international treaty framework for combating cybercrimes affecting national security consists of a set of global and regional instruments that do not limit themselves to regulating information crime in its narrow technical sense, but extend to criminalizing the financing of terrorism, money laundering, and transnational organized crime when digital platforms and electronic channels are used as tools for execution. These conventions establish the principle that cyberspace has become a primary environment for the movement of illicit funds, the coordination of hostile activities, and the exchange of sensitive data, which imposes on states a dual obligation: to adapt their domestic laws to international criminalization standards, and to strengthen mechanisms for judicial and law-enforcement cooperation and near-real-time information exchange. The preambles of many of these conventions indicate that cybercrimes constitute a direct threat to peace and security at both the

national and international levels due to their transboundary nature and the ease with which perpetrators can conceal their identities through encryption technologies, remote servers, and digital financial intermediaries [5].

These international obligations are reflected in national legislation through laws on combating money laundering and the financing of terrorism, which constitute the primary gateway for pursuing financially oriented cybercrimes linked to organized criminal networks. The Anti-Money Laundering and Counter-Terrorism Financing Law No. 39 of 2015 embodies this approach in Iraqi legislation, as Article 2 defines the crimes of money laundering and terrorism financing in a broad manner that includes the transfer or movement of funds derived from crimes through electronic channels and banking systems, and obliges financial and non-financial institutions to adopt due-diligence procedures regarding suspicious transactions conducted via digital platforms. This definition is in line with what international conventions and the technical standards of financial action groups recommend regarding the need to monitor international transactions (particularly those that take place through electronic systems) and to oblige financial institutions to report suspicious transactions and to freeze funds related to terrorism or other forms of organised crime, even if those are conducted solely through electronic means.

The relevance of international conventions on cybercrime emerges more specifically in instruments that directly regulate conduct related to information systems and data, and contain models of legislation for the criminalization of unlawful access to information systems, interception of communications, data destruction and service denial. These instruments usually require states to introduce certain crimes into their criminal law and harmonise or bring closer technical definitions in order to apply the principle of dual criminality in extradition and mutual legal assistance requests. They also contain detailed provisions on international cooperation in electronic search and seizure and the urgent preservation of data stored or transmitted across networks, as the short passage of time and the ease of erasing digital traces make the effectiveness of investigations dependent on rapid response and securing evidence before it is lost. This type of convention constitutes a reference for states seeking to enact or revise their national laws related to cybercrime in a manner that ensures their consistency with international legal practice [6].

The implementation of these conventions is reflected in practice through the expansion of traditional criminal cooperation to include the financial, supervisory, and administrative dimensions related to monitoring cybercrimes that affect national security. Cooperation in applying the financial and regulatory standards reflected in the provisions of anti-money-laundering and counter-terrorism-financing laws becomes complementary to cooperation in investigation and prosecution, because drying up the sources of financing for cyberattacks and transnational criminal networks cannot be achieved through criminal procedures alone; rather, it requires the participation of banks, regulatory bodies, telecommunications authorities, and digital service providers in an integrated preventive system. This requires a constant harmonisation of national laws with these treaties, as well as the direct exchange of information between financial intelligence units, public prosecution offices and other competent authorities to ensure that the international treaty framework becomes an effective instrument for protecting national security from cybercrime rather than a merely theoretical and abstract duty that is disconnected from the needs of practical implementation.

This treaty framework helps redefine the notion of state obligations in the area

of preventing cybercrimes that threaten national security, as the state's role is no longer confined to the adoption of domestic criminal provisions; now it must accede to international treaties in this field and ensure their effective implementation both at the legislative and administrative levels. Many of these treaties require the harmonization of national laws with certain standards within reasonable deadlines, and they recommend the inclusion of specific technical definitions of information crimes and limitation of vague terms that might clash with fundamental rights. This may sometimes lead to the emergence of a conflict between national security and some constitutional provisions or general legal principles, and may require the legislature to find compromise solutions that meet the minimum standards of international harmonization while preserving constitutional constants. This dilemma is

clearly reflected in the legislative debates that usually precede the adoption of any legislative change based on an international convention, which raises concerns about the prevalence of trans-border security interests over national diversities.

It is also observed that a significant number of conventions addressing cybercrime are not limited to the purely criminal aspect, but rather integrate provisions of criminalization with provisions of judicial and police cooperation and, at times, provisions concerning prevention and victim protection. This multi-level character makes compliance with these conventions a broad reform project that requires amending procedural laws, establishing specialized units within public prosecution offices and judicial police, and developing working tools in fields such as financial investigations, digital evidence, and joint investigations. Some of these instruments also encourage the adoption of early mechanisms for the preservation of data and the suspension of its deletion upon the request of another state, which imposes upon national legislations the need to reconsider rules governing data retention by service providers and the limits of the responsibility imposed upon them. This calls for a permanent alignment of national legislation with these conventions and a direct link between financial intelligence units, public prosecution offices, and other relevant authorities in order for the international treaty framework to be a practical mechanism for national security against cybercrime and not a purely theoretical obligation, separated from its implementation through legislation.

Thus, conventions, which are initially normative in nature, become a catalyst for reform of the criminal justice system to meet cyber challenges.

Another way in which the impact of international conventions on cybercrime is reflected is through the monitoring and evaluation mechanisms adopted by some international and regional organizations, whereby states are exposed to a theoretical and practical review process in terms of their level of adherence to the agreed-upon standards. These mechanisms are based on the self-assessment reports of states and the parallel reports of experts or professional bodies and, as a general rule, end in a series of recommendations regarding legislative deficiencies, institutional weaknesses or international cooperation. The acceptance of these mechanisms by a state practically implies that it becomes part of an ongoing reform process that goes beyond ratification of the convention, as the accumulation of observations and recommendations may have an impact on its international reputation and its position in risk maps of money laundering, terrorism financing and other forms of organized crime. Thus, the compliance with international treaties in the area of cybercrime becomes not only a legal duty but also a condition for creating confidence with international partners and ensuring national security in an interrelated network of mutual obligations [7].

The Second Requirement: The Role of International Organizations in Combating Cybercrimes

The role of international and regional organisations in the fight against cybercrimes manifests in their contribution to the development of general legal norms in the information sphere, as well as in the development of the international discourse around the balance between national security and human rights in the information environment. Through conventions, declarations, and recommendations, these organizations establish general guidelines for defining cybercrimes, determining their scope, and outlining states' obligations in the fields of criminalization, protection, and prevention, and they then monitor—at varying levels—the extent to which states comply with these standards when enacting their national legislation. This role is embodied in the preparation of guidance manuals and model laws for information crimes, in addition to organizing capacity-building programs and the exchange of expertise among judicial and security bodies in member states. These soft tools become an indirect means of exerting legal and moral pressure on national legislators to incorporate concepts such as necessity, proportionality, and legality into the provisions of criminalization and punishment related to cyberspace, thereby reducing the risks of transforming cybercrime control laws into instruments for restricting public freedoms [8].

This is clearly reflected in the history of the draft Iraqi anti-cybercrime or information crime law, which has been re-proposed in several versions since 2011 and amended in 2019. The different versions of the draft were influenced by two factors: the need to defend national security against cyber threats, and observations by international human rights and professional organisations. A version of

the draft law contained Article 5, paragraph 3, which punishes access to a website or use of a computer to access data or information that harms national security or the national economy with up to ten years in prison and a fine. This is a generic description that is based on the type of information and its relation to security or the economy, without providing clear delineations on the notion of harm or a threshold for actual harm. Such text alarmed international organisations that deal with freedom of speech and online privacy about the potential to criminalise investigative journalism, whistleblowing to the public in the interest of the public, or even civil society or opposition dissident activities on the internet whenever they are vaguely connected to the concept of national security.

The general description of the draft's articles, which number more than 20 articles and include 63 crimes, particularly those related to the attack on state systems or the publication of information considered a threat to the interests of the government, society or religion, indicates that it has received multiple observations and criticism in reports by international human rights and professional bodies. These organizations believed that the density of punitive texts, the multiplicity of forms of criminalization, and their broadness make it difficult to reconcile the requirements of protecting national security with guarantees of freedom of expression and the circulation of information. These observations focused on the absence of precise definitions for some pivotal terms such as public order, morals, and harm to the supreme interests of the state, and on the lack of explicit provisions for the standards of necessity, proportionality, and effective judicial oversight in the application of rulings, which could open the door to strict interpretations that expand the scope of criminal liability in the digital realm. This criticism contributed to pushing the legislator to reconsider a number of proposed formulations and to consider introducing clearer guarantees for rights and freedoms within the texts of the law [9].

This interaction between the national legislator and international organizations reflects the reality that the latter's role in combating cybercrimes is not limited to advocating for harsher penalties or expanding the scope of criminalization, but is fundamentally based on attempting to draw a precise balance between the requirements of national security and the imperatives of respecting human rights in the digital sphere. International and regional organizations rely on multiple tools in this regard, including issuing periodic reports on the state of digital freedoms, providing technical comments on draft laws, organizing dialogues with governments and parliaments, in addition to offering technical support for developing the capacities of law enforcement bodies in investigating cybercrimes and collecting digital evidence. This ultimately leads to the national legislator adopting a legislative strategy that separates serious cybercrimes that impact on national security, which should be firmly criminalized and require specific derogations, from legitimate or protected uses of the digital environment for freedom of expression, communication and participation, thus contributing to building a more balanced and effective legal framework in the fight against cyber threats.

International bodies specializing in communications and technical standards play a role in the development of the normative framework for the prevention and combat of cybercrimes, by establishing protocols in cybersecurity, risk management and data protection, and by promoting their implementation in national laws and policies. These bodies publish technical manuals on network security, encryption and software integrity standards, and suggest tools for vulnerability detection and proactive mitigation, which in turn impacts the drafting of laws that regulate the responsibilities of service providers and operators of critical infrastructure. The national legislator frequently draws on these technical manuals to establish the minimum technical standards that must be met in order to prevent cyber risks, and judicial decisions are based on them when evaluating the conduct of enterprises and public authorities in liability lawsuits against breaches and attacks resulting from negligent measures. In this way, international technical organizations become indirect actors in shaping the substance of the legal obligations imposed on digital space actors within each state [10].

The role of international organizations also stands out in the field of coordination and network-based cooperation among judicial and police bodies through the establishment of platforms for the immediate exchange of information related to cybercrimes affecting national security, and the organization of joint databases on the patterns of attacks and the tools used in them. These

organizations encourage the appointment of national contact points operating around the clock to receive urgent requests and preserve data threatened with rapid disappearance, then refer them through official judicial channels. This quasi-operational form of cooperation reduces the gap between the speed at which cyber actors move and the slowness of traditional mutual legal assistance procedures, and it provides a basis for building mutual trust among the different national bodies through adherence to unified rules for protecting the confidentiality of information and ensuring its use solely for investigation and prosecution purposes. This interactive model helps to make the battle against cybercrimes an interactive process that cuts across political jurisdictions of states without compromising the judicial sovereignty of each state.

However, the success of the role of international organizations in the fight against cybercrimes is still dependent on the degree to which states are prepared to take part in the mechanisms they offer and to go beyond mere statements that are not followed by action. While some states engage constructively with the reports and recommendations and proactively review their laws and institutional capacities, other states engage with this process more cautiously due to fear of encroachment on their discretion in matters of national security or the exposure of vulnerabilities in their cyber infrastructure. This poses a challenge to the efforts of international organizations to harmonise standards and raise the standard of legal and practical cyberprotection, which leads them to develop incentive mechanisms such as technical assistance programs, conditional funding and free consultancy services to interested states. The effectiveness of these efforts depends on their ability to persuade states that enhancing cooperation and transparency in the area of cybercrimes is, ultimately, an investment in their national security, rather than a loss of sovereignty [11].

The Third Section: Judicial Cooperation Between States in Combating Cybercrimes

Multilateral judicial cooperation in the fight against cybercrimes is a crucial component in the national security protection system, due to the transnational nature of such crimes and their ability to travel across networks and information systems from one country to another in a relatively short time, making national mechanisms insufficient to pursue perpetrators or secure digital evidence without the support of other countries. The international regime in this area is based on a number of mechanisms such as mutual legal assistance, extradition of the accused, exchange of information and evidence, and the establishment of joint investigation teams, which cannot be effectively triggered unless they are based on legislative and procedural rules that are reasonably consistent between different legal systems. This section will briefly describe the forms of such judicial cooperation and the instruments it relies on, and will examine the legal and technical obstacles to its implementation in cases of cybercrimes impacting national security, focusing on the role of the national judiciary in the network of interstate judicial relations, and on the balance between the principles of sovereignty and the needs of effective cooperation with other states in the fight against organised cyberattacks.

The First Requirement: Forms of International Judicial Cooperation in Cybercrime Cases

The forms of judicial cooperation in cybercrime cases are based on a fundamental principle: transboundary procedures cannot be isolated from the national rules of criminal procedure; rather, they are established on top of them and at the same time extend outside the national territory in line with the mechanisms defined jointly by domestic law and international treaties. Cybercrimes that affect national security are transboundary in nature, as the perpetrators may reside in one state, the servers in another state, and the impacts of the crime in a third state, which makes it difficult to prosecute such crimes relying on the unilateral efforts of each state. In this context, various forms of judicial cooperation have evolved, such as requests for mutual legal assistance, extradition of accused persons, transfer of proceedings or judgements, and exchange of information and digital evidence, along with the creation of joint investigation teams in some complicated cases. In all of them, the reference remains the domestic laws on search, seizure, and evidence admissibility, adapting them in a way that enables the fulfilment of the needs of international cyber investigation.

The amended Code of Criminal Procedure No. 23 of 1971 is a significant referential framework for delineating the boundaries of such cooperation in Iraq, at least as far as search and seizure of electronic devices - the usual vessel of digital evidence in cybercrimes - is concerned. Article 72 states "no

person, house or place shall be searched except in the cases enumerated by law and by an investigative judge or his deputy". In contemporary applications, this includes the search of mobile phones, computers, and local servers whenever they are subject to suspicion in a case with a cyber dimension. When requests for mutual legal assistance are received from another state to obtain the contents of an electronic device or account, national authorities must execute such requests within the limits drawn by this article, so that international judicial cooperation does not become a pretext for bypassing the guarantees afforded to individuals against search and seizure, even if the crime forming the subject of the request is of a serious nature and affects national security or public security.

Article 73 adds another dimension to the forms of judicial cooperation, represented in the requirement that an order be issued by a legally competent authority before conducting the search, while allowing, in cases of necessity, for the bypassing of certain formal conditions, which is useful in adapting urgent responses to cyberattacks. In practical reality, some cybercrimes may require immediate measures to prevent the erasure of digital evidence or the continuation of attacks on vital systems, such as attacks targeting electricity networks, banks, or telecommunications. The provision thus enables immediate action within a country in accordance with the minimum guarantees, followed by the issuing of the necessary authorisations. This approach also helps to facilitate the possibility that national authorities respond to urgent judicial requests (letters rogatory) of other states to identify the origin of a cyberattack or to block digital accounts related to a crime that affects national security, as long as it is done in the context of a legal framework that balances the need for speed with the need for respect for procedural legality [12].

Article 212 acquires a crucial significance to the forms of judicial cooperation in cybercrime proceedings when it sets forth that a court shall not base its decision on evidence that has not been discussed in the hearing, or on a document that has not been discussed by the litigants. This rule institutionalises the principle of transparency in the collection of digital evidence shared between countries. Evidence obtained from an electronic search, or from the data of a foreign service provider, or from the content of external servers, does not have probative value simply because it has been received in the context of judicial cooperation; rather, it must be produced in a public hearing in order for litigants to discuss it and to question the validity of the processes of collection and preservation, the chain of custody, and the veracity of the procedures used to confirm its authenticity. This requires national judicial authorities to agree in advance with those of other states to ensure that the procedures for seizure, preservation and translation of evidence are recorded in a way that allows the court to evaluate such evidence in the context of fair-trial guarantees. This turns judicial cooperation into a legal partnership between courts that guarantees the rights of the defence and strengthens trust between judicial authorities in the area of fighting cybercrimes that undermine national security.

The forms of international judicial cooperation in cybercrime cases take multiple practical shapes, foremost among them requests for mutual legal assistance, which are usually handled by a central authority in each state, such as the Ministry of Justice or the Office of the Public Prosecutor. This authority receives requests from abroad and verifies that they satisfy the formal and substantive requirements before referring them to the competent investigative bodies. These requests include conducting a search of devices or servers, seizing and preserving digital data, hearing witnesses and experts, obtaining communication records and electronic account activity, and may also include a request to provide the requesting state with copies of relevant judgments or legislative texts. The urgent nature of digital evidence necessitates the adoption of fast and direct communication channels between central authorities, relying on secure means for exchanging information and maintaining its confidentiality, so that the factor of time does not become an obstacle preventing the tracing of offenders or the establishment of facts before the judiciary [13].

Another form of judicial cooperation in cybercrime cases appears in the field of extradition and transfer of proceedings, where a state receives requests to extradite individuals accused or convicted of cybercrimes that affect the security of another state. Its judiciary is thus responsible for verifying the availability of the conditions of dual criminality and the guarantees of a fair trial before approving extradition. When extradition of nationals is not permitted by domestic law or there are other legal

obstacles, the state may choose to proceed with the transfer of the proceedings or enforcement of the foreign judgment in its territory as a substitute form of cooperation that allows the punishment to be carried out without violating national sovereignty. In complex cases, where criminal networks operate in more than one state, the notion of joint investigation teams has developed, which allows judges, prosecutors and technical specialists from multiple states to collaborate on the same case, according to an agreed plan, thus minimising jurisdictional problems and overlapping efforts and procedures.

These traditional forms of judicial cooperation are complemented by non-traditional forms of operational and technical cooperation, such as the exchange of experts in the field of computer forensic science, the joint organisation of training courses for judges, judicial assistants and law-enforcement officers, and the creation of digital forensic laboratories whose procedures converge in a way that makes the results of their work acceptable before various courts. Many jurisdictions have developed standardised formats for the requests for assistance in cybercrime cases and practical guidelines that explain the procedures to be followed for the preservation of data and the maintenance of the chain of custody from seizure to court from the moment of seizure to its presentation in the trial, thus encouraging confidence in the quality of the evidence shared. This technical and institutional cooperation, which parallels formal judicial cooperation, contributes to building a broader protective network for national security in the face of cyberattacks, as it creates an environment of procedural and normative harmony that renders the pursuit of cybercrime perpetrators a practically feasible process despite the complexities inherent in the cross-border nature of such crimes [14].

Methodology

The Second Requirement: Challenges Facing Judicial Cooperation in Matters of Cybercrimes

Cybercrimes affecting national security pose a set of structural challenges to international judicial cooperation, foremost among them the nature of national penal provisions and the manner in which they are drafted compared to the standards prevailing in international legal practice. Many of these provisions were enacted at a time when cyberspace had not yet gained its current importance, making their application to contemporary electronic facts a complex interpretative exercise in which judicial authorities may differ from one state to another. This leads to inconsistencies in the definition and ambit of cybercrime, and in determining the material and moral elements of the crime, which in turn impacts the dual criminality conditions that constitute the basis of any judicial cooperation in areas such as extradition, letters rogatory and mutual legal assistance. The more abstract, general or outdated the provisions, the more challenging it becomes to persuade other states of the compatibility of the crime description with the facts presented, which affects the efficiency of judicial cooperation mechanisms in tracking down cyber criminals, who are often based in more than one jurisdiction.

This issue is clear in the Iraqi case in relation to some provisions of the amended Iraqi Penal Code No. 111 of 1969 that could be used to criminalise cyber acts that affect the state's economic security. Article 304 prohibits the dissemination of information or rumours that may impact on the value of the Iraqi currency or market trust in the country, while Article 305 prohibits acts that disrupt financial markets and banks. But the application of these two provisions in the cyber context raises practical challenges in identifying the source of the digital information harmful to the currency or markets; proving a link between the digital information and the perpetrator's intention and place of residence; and determining the scope of the state's power to prosecute in the case of a perpetrator residing outside the state's territory. The question also arises as to whether these provisions are adequate to criminalise coordinated disinformation campaigns or information attacks through cross-border platforms and primarily targeting the confidence in the currency or the financial system through the spread of false information or partial leaks, as some states might argue that such acts are protected under freedom of speech or legitimate business practices unless they cause direct material damage [15].

Another challenge emerges through the provisions that protect state secrets and the confidentiality of correspondence, such as Article 327, which criminalizes the disclosure of official

secrets by a public employee who, by virtue of his position, has access to confidential information, and Article 328, which criminalizes the interception or obstruction of private correspondence by a public employee. In the context of international cooperation in cybercrime matters, these rules interact with the need of judicial authorities to share information and evidence with regard to national security with their counterparts in other countries. This brings up the question of finding the balance between the obligation to preserve the confidentiality of information and communications and digital documents of strategic importance, and the need to combat organized crime networks that cannot be broken without a coordinated exchange of technical and analytical information. If the law does not provide for any explicit exceptions that allow for the exchange of certain information under judicial control and in the scope of bilateral agreements, the public servant is at risk of facing liability in case he responds to international cooperation requests, and the authorities may refuse to cooperate in the fear of violating the duty of secrecy. This undermines the effectiveness of international investigations in the area of cybercrimes.

Other technical and procedural issues also relate to the challenges of judicial cooperation in cybercrime cases, including the difficulty of finding consensus on the standards for preservation of digital evidence and its chain of custody, the differences in terms of the states' capacities in the area of digital forensics, and the different rules on personal data protection, as well as the slowness of some traditional mutual legal assistance procedures versus the speed of data disappearance or transformation in cyberspace. The success of cooperation requires mutual trust between judicial systems, and this trust is shaken when one state doubts another's respect for fair trial guarantees, or for the protection of data being exchanged, or for its precise understanding of the nature and seriousness of cybercrimes. Added to this are political and strategic considerations that make some states reluctant to reveal details of cyberattacks they have suffered or vulnerabilities in their digital infrastructure, fearing the exploitation of such information or its impact on their international image, whereas combating cybercrimes affecting national security requires a high degree of transparency and coordination. Addressing these challenges therefore becomes a necessary condition for transforming judicial cooperation from the level of texts to the level of actual implementation in this complex and rapidly evolving field [16].

The issue of judicial jurisdiction in cybercrimes presents a qualitative challenge to international cooperation, because the intangible nature of these crimes allows their elements to occur across multiple territories, making it difficult to determine the state that holds the original jurisdiction or is most entitled to adjudicate the dispute. An attack may originate from a device located in one state, pass through servers in a second state, strike critical infrastructure in a third state, while the perpetrator holds the nationality of a fourth state. This creates a conflict between the principle of territoriality and the principle of the nationality of the offender or the victim, and scenarios of abstaining from exercising jurisdiction—or, conversely, jurisdictional competition in politically sensitive cases—are often repeated. The lack of international binding rules for the allocation of jurisdiction in this area leads each state to follow its own interpretation of the concepts of cross-border jurisdiction, with the risk of conflicting decisions or punitive gaps that favour the impunity of some cyber offenders. This also undermines states' cooperation with the risk that the implementation of an assistance request may support conflicting interpretations that do not correspond with their interests or legal system.

A further challenge is the great variation among legal systems in the standards for the admission of digital evidence and the conditions for its probative value, as some systems adopt sophisticated models for the chain of custody and technical documentation of electronic seizures and searches, while others rely on vague and general rules, which do not distinguish between evidence and evidence obtained from digital devices and online platforms. This poses a problem when a state requests the admission of digital evidence obtained according to its standards, which may not, in the opinion of the cooperating state, be sufficient in terms of documentation or data protection. This gives rise to disputes concerning the integrity of procedures and the possibility of excluding the evidence before the courts. Linguistic and technical barriers also impede the smooth flow of cooperation, because converting large volumes of digital data into formats understandable to judges and experts in different states requires time and advanced resources, and increases the likelihood of errors in analysis or

translation, thereby adding yet another layer of complexity to the process of judicial cooperation in this type of case.

One of the most dangerous challenges lies in the risks of politicizing judicial cooperation in cybercrimes affecting national security, as some states may tend to employ the classification of cybercrimes to include opposition, journalistic, or civil activities within the category of acts threatening national security, thereby requesting other states to pursue individuals or block platforms on the basis of broad and vague provisions. These practices raise serious doubts among the states from which cooperation is requested regarding the extent to which fair trial standards are respected and the non-arbitrary application of cybercrime laws to restrict fundamental freedoms. As a result, they may express reservations about executing such requests or reject them on the grounds of the potentially political nature of the crimes under investigation. This leads to a legal uncertainty that makes even legitimate requests for serious cybercrimes to be scrutinised or treated with suspicion because the lack of distinction between matters that fall within the ambit of national security protection and those which relate to legitimate political and media activities makes it difficult to have a relationship of trust between judicial authorities and international cooperation in this field is subject to the political and sovereign considerations that may prevail over the initial aim of fighting organised cybercrimes.

Results and Discussion

1. The study revealed that cybercrimes affecting national security are a digital manifestation of the traditional forms of crimes against the state and society, but they are distinguished by technical characteristics that allow them to have a greater impact, to occur more rapidly and to conceal themselves. It is evident that cyberspace is no longer just a means of communication, but has become a strategic space by which vital facilities can be disrupted, public opinion manipulated, and public confidence undermined. Therefore, any legal approach to these crimes must be grounded in an accurate understanding of the nature of these crimes as having a two-fold dimension: a criminal dimension on the one hand and a strategic security dimension on the other.
2. The study found that the Iraqi constitutional and legal framework offers an initial starting point that can be built upon to criminalise certain types of cybercrimes affecting national security through the provisions of the Constitution, the Anti-Terrorism Law, the Anti-Money Laundering and Counter-Terrorism Financing Law, the Penal Code, and the Code of Criminal Procedure. However, it is evident that these texts were enacted in a non-digital environment and were not originally designed to accommodate the particularities of cyberattacks, which makes their application to contemporary digital incidents dependent on judicial interpretations that may vary. This situation leads to gaps in protection and a lack of clarity regarding the limits of criminal liability for acts committed through digital space and affecting national security.
3. The study demonstrated that the international treaty framework— particularly in the areas of combating money laundering, terrorism financing, and transnational organized crime—plays a central role in surrounding cybercrimes affecting national security with a set of shared normative rules. The importance of these instruments lies in unifying or approximating the definitions of certain serious acts, such as transferring illicit proceeds through electronic channels and financing dangerous entities using digital systems. It is clear that implementing these conventions within national legislation contributes to expanding the scope of criminalization to include stages of preparation, financing, and logistical support for cyberattacks, in addition to strengthening financial and supervisory mechanisms aimed at drying up the sources of such crimes.
4. The study concluded that international and regional organizations are no longer merely external observers of national legislative processes in the field of cybercrimes, but have become influential actors in shaping these processes through technical reports, legislative models, training programs, and evaluative mechanisms. This was evident in the discussions surrounding the Iraqi draft Cybercrime Law, where the observations of human rights and

professional organizations contributed to exposing the risks of expanding criminalization and the absence of sufficient guarantees for digital rights and freedoms. It appears that this interaction between international discourse and national legislators forms a pressure factor directing the process toward building a more precise balance between the requirements of cybersecurity and the guarantees of human rights in the digital environment.

5. The study clarified that international judicial cooperation in confronting cybercrimes affecting national security has become an inevitable option imposed by the cross-border nature of these crimes; however, its practical implementation remains constrained by the national framework of criminal procedures and the degree to which it aligns with the requirements of investigation in cyberspace. It became evident that the provisions of the Iraqi Code of Criminal Procedure relating to searches, the seizure of devices, and the probative value of evidence provide a basis upon which requests for mutual assistance and judicial commissions involving digital evidence can be executed. Nevertheless, the absence of detailed rules specific to electronic evidence and its chains of custody continues to cause disputes regarding the integrity of procedures and the probative value of resulting data before national and foreign courts.
6. The study confirmed that the challenges facing judicial cooperation in matters of cybercrime are not limited to deficiencies in penal or procedural texts, but extend to technical, institutional, and political issues, including the difficulty of attributing attacks to specific actors, disparities in states' capabilities in the field of digital forensics, and differences in data protection and privacy rules. It appears that the ambiguous boundaries between cybercrimes of a security-related nature and certain forms of political or media activity conducted through digital space sometimes open the door to the politicization of requests for judicial cooperation, which affects the level of mutual trust between judicial systems. This is reflected in the reluctance of some states to execute requests or accept evidence, especially when there is a possibility that cybercrime laws may be used for purposes that exceed the narrow meaning of protecting national security.
7. The study ultimately concluded that building effective protection for national security against cybercrimes requires a comprehensive approach that goes beyond the logic of legislative reaction toward the logic of multi-level strategic planning. The review of criminal and procedural texts must be integrated with the development of specialized institutional structures and the enhancement of the capacities of the judiciary and investigative bodies in the field of digital evidence, in addition to strengthening formal and informal channels of international cooperation. It also appears that the preventive dimension is no less important than the punitive one, as the matter requires consolidating a culture of cybersecurity among individuals, public administrations, and the private sector, and adopting national policies for risk assessment and the protection of critical infrastructure, so that the legal system becomes part of an integrated environment capable of absorbing cyber threats and reducing their impact on national security.

Conclusion

1. It is advisable to enact national laws that specifically regulate cybercrimes that impact national security, which include a clear definition of the different types of serious cyber offences, with the crime classification based on the element of actual damage or serious risk of damage to infrastructure and public safety. This law should be drafted in accordance with the principles of legality and clarity, and should differentiate between criminal conduct and legitimate digital activities, such as freedom of opinion, the media and academic research. This helps overcome the gaps in the application of general provisions, while avoiding unwarranted criminalization in the digital environment.
2. It is advisable to review the criminal provisions on economic security, state secrets and communications in the Penal Code and other special laws in order to update them to the realities of the digital environment. It is also advisable to amend the provisions that criminalize the distribution of digital information that is harmful to the national currency or financial markets by clarifying the scope of application and providing standards and ways to

calculate this harm in the digital space. It is also recommended to add exceptions and safeguards that ensure freedom of reporting corruption and other serious misconduct in the public interest so that these provisions do not become a means of censorship or hinder public control over the activity of authorities.

3. It is advisable to elaborate on the rules of criminal procedure on the search and seizure of electronic devices and preservation of computer evidence by introducing detailed regulation in the Code of Criminal Procedure or in a special law on computer evidence. Conditions for issuing search warrants must be defined, along with rules governing access to stored or transmitted data across networks, specifying retention periods and the method for documenting chain of custody. Such regulation strengthens the admissibility of digital evidence before national and foreign courts and reduces disputes regarding procedural integrity when executing requests for judicial assistance in cross-border cases.
4. It is recommended to broaden the state's accession to international and regional conventions related to cybercrimes, money laundering, terrorism financing, and organized crime, and to work on implementing the obligations arising therefrom at the legislative and institutional levels. This helps unify or approximate applicable definitions and procedures and enhances the national authorities' capacity to benefit from the judicial and law-enforcement cooperation mechanisms offered by these instruments. Active participation in periodic monitoring and evaluation mechanisms organized by international organizations is also important, as these provide technical diagnoses of gaps and offer opportunities to obtain technical support and capacity-building in digital investigation and cyber risk analysis.
5. It is recommended to strengthen the institutional structure responsible for confronting cybercrimes affecting national security by establishing specialized units within public prosecution offices, judicial police, and regulatory authorities overseeing vital sectors such as finance, communications, and energy. These units require advanced technical equipment and personnel trained in digital forensics and the use of advanced data-analysis tools. Standing coordination mechanisms should also be set up between these institutions to facilitate information and expertise sharing, and ensure quick and coordinated response to sophisticated cyberattacks.
6. It is advisable to strengthen international judicial cooperation in cybercrime matters by reviewing bilateral and multilateral treaties and including more specific information regarding the exchange of digital evidence, as well as urgent measures for the preservation of evidence. It is advisable to designate an effective central authority to receive requests for mutual legal assistance and judicial commissions and handle them according to clear timelines, using secure and rapid communication channels. It is also essential to develop joint operational guidelines with partner states regulating the documentation and translation of evidence, and ensuring compliance with fair-trial standards and personal-data protection at all stages of cooperation.
7. It is recommended to adopt a comprehensive preventive approach to enhancing national cybersecurity, based on raising awareness among individuals and institutions about digital risks and strategies for mitigating them, along with encouraging the private sector to comply with strict information-security standards. This can be achieved through tiered educational and training programs, incentive-based policies, and linking operating licenses in vital sectors to the fulfillment of specific digital-security requirements. This approach helps reduce the likelihood of successful cyberattacks and ensures that the criminal and cooperative frameworks operate within an environment more capable of withstanding cyber threats to national security.

References

[1] K. Bourhou, "The role of Arab legislation in combating cybercrime: A study of the most significant developments," Journal of Scientific Readings in Legal, Economic, Human and Sharia Research and Studies, no. 41, pp. 213–221, 2025.

[2] S. M. Abdulhamza, "Iraqi legislative policy for the protection of cyber national security: A

study in light of the provisions of public international law," Lark Journal for Philosophy, Linguistics and Social Sciences, no. 46, pp. 522–540, 2022.
[3] O. K. Al-Rumaihi, "International efforts to combat cybercrime," International Electronic Journal for Publishing Legal Research, vol. 6, no. 25, pp. 240–248, 2025.
[4] M. S. Q. Al-Hamadain, "Cyberattacks and their repercussions on the threat to digital security," Journal of Security Studies, no. 21, pp. 121–188, 2024.
[5]
[6] A. A. A.-M. M. Ahmed, "Combating cybercrimes: Arab and international agreements," Dhakhaer Journal for Human Sciences, no. 14, pp. 12–31, 2022.
[7] M. Al-Aidani, "Cyber threats and information crimes," Ijtihad Journal for Legal and Economic Studies, vol. 13, no. 1, pp. 15–30, 2024.
[8] A. Afoufo, "Security globalization: Its dimensions and its relationship with national security," Ijtihad Journal for Legal and Economic Studies, vol. 11, no. 2, pp. 781–809, 2022.
[9] H. S. M. Al-Zuyut, "Cybersecurity crimes as a global issue and their impact on international relations," Master's thesis, Al al-Bayt University, 2024.
[10] R. Y. M. Al-Bayati, "Cyber terrorism: Models of international efforts to curb it," Tikrit Journal for Political Science, no. 28, pp. 87–121, 2022.
[11] M. Shahmat, "Cybersecurity of states: A virtual dimension of a material reality," Al-Naqid Journal for Political Studies, vol. 7, no. 2, pp. 99–114, 2023.
[12] M. A.-S. Msika, "Cyberspace and the challenges of national security for states," Journal of Legal and Social Sciences, vol. 7, no. 4,
[13] pp. 447–462, 2022.
[14] M. I. S. Al-Shammari, "Cybersecurity and its impact on Iraqi national security," Journal of Legal and Political Sciences, vol. 10, no. 1,
[15] pp. 147–190, 2021.
[16] D. Al-Badaineh, "Cyber terrorism and emerging technologies: Challenges to cyber national security and national sovereignty," Journal of Legal and Security Studies, vol. 4, no. 1, pp. 7–72, 2024.
[17] R. Hamida, "Electronic crime through social media platforms: Toward activating the role of informational cybersecurity," Journal of Media and Society, vol. 5, no. 2, pp. 338–356, 2021.
[18] S. Kalaa, "Cybersecurity and the challenges of espionage and electronic intrusions against states through cyberspace," Journal of Law and Human Sciences, vol. 15, no. 1, pp. 292–314, 2022.
[19] M. G. H. Ibrahim, "The effectiveness of criminal policy in confronting cybercrimes: A comparative study in light of cybersecurity requirements," Journal of Sharia and Law, no. 45, pp. 2619–2709, 2025.