Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Legislative Measures to Confront Cyber Terrorism in Iraq: An Overview Universiti Kebangsaan Malaysia (UKM)

Ibrahim Abduljaleel Kaky, Dr. Muhamad Helmi Bin Md Said

ARTICLE INFO

Received: 22 Dec 2024

Revised: 14 Feb 2025

Accepted: 26 Feb 2025

ABSTRACT

The proliferation of access to information, led to technological development that has both positive and negative impact on society. Terrorism exploited this technology and utilized it to spread ideology, develop terrorist mechanisms while expanding terrorist influence through cyberspace around the world. Iraq has been a major breeding ground for terrorist activities and cyber terrorism has become widespread in the country and across the globe. Yet, there is the absence of specific legal text to confront the menace. This research aims to assess the Iraqi legal measures in confronting cyber terrorism. Analysis of the existing legal framework in Iraq was done. Using a qualitative empirical research, 11 informants 7 of which are Iraqi Judges were interviewed through face-to-face semi-structured interview to ascertain how the Iraqi courts confront cyber terrorism. It was discovered that there is no provision on cyber terrorism in any of the Iraqi region's legislations and the provisions in the Kurdistan Region's cyber-Terror la are not sufficient to confront cyber terrorism crime. Therefore, the Iraqi courts rely solely on the general principles of criminal legitimacy to confront cyber terrorism. Doing so prejudices the principle of criminal legitimacy and granting judgments that are not commensurate with the crime. Therefore, this research suggest the development of robust legislation on cyber terrorism to minimize cyber terrorism crime in Iraq.

Keywords- Cyber Terrorism, Legal Measures, Courts, Legislation, Iraq

INTRODUCTION

Cyber terrorism is the convergence of cyberspace and terrorism while utilizing the computer as the weapon and the target. Cyber terrorism transient national borders and is perpetuated across jurisdictions with little or no restriction. This has been majorly due to the activities of violent extremist. Even though research have shown that socio-economic inequality, political instability and foreign invasion and ideologies are some of the causes of terrorism and in particular cyber terrorism across the globe (Al-Shamari, 2021; Albahar, 2019; Khater, 2023; Marsili, 2018; Muhammad Nadeem Mirza & Muhammad Shahzad Akram, 2022). Many countries like Iraq (Al-Shamari, 2021; Al-Tae et al., 2020; Baeewe, 2021; Rudner, 2016; Sedeeq & Ghareb, 2018; Shakarian et al., 2013; Tulga, 2022), Pakistan (Anjum, 2022; Geo, 2016; Muhammad Nadeem Mirza & Muhammad Shahzad Akram, 2022), India (Ambika & Senthilvel, 2020; Shakarian et al., 2013), Saudi Arabia (Abu-Taieh et al., 2018; Aissani, 2022; Alghamdi, 2020), China (Shakarian et al., 2013; Zheng & Di, 2022), the United States (Couzigou, 2022; Ofusori & Hendradi, 2023; Trautman, 2016) and others are among the most countries affected by cyber terrorism. The menace had led many countries have worked to globalize cyber security, expanded and engaged in initiatives through bilateral and multilateral cooperation (Alghamdi, 2020; Durac, 2018; Khater, 2023; Sedeeq & Ghareb, 2018) with local and international agencies to enhance

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

cyber security strategies in their countries. Countries have enacted laws against terrorism and cyber terrorism to confront the menace.

To confront terrorism legislatively, it is necessary to keep pace with the development taking place in the field of cybercrime. Especially through adequate legislative confrontation (Brière, 2021; Dhirani et al., 2023; Djenna et al., 2023; Sedeeq & Ghareb, 2018) and the necessary response to deal with these crimes. Through finding sufficient and necessary non-traditional legal rules to deal with cybercrimes. Iraq is one country that has been ravaged by cyber terrorism committed within its borders and outside its borders. It made efforts towards combating the menace by enacting the Anti-Terrorism law No. 13 of 2005 and another Anti-Terror law No. 3 of 2006 applicable to the Kurdistan Region. Despite the provisions of these legislations, cyber terrorism remained prevalent in the country. Cases of cyber terrorism are being handled in the Iraqi courts on daily basis, yet the problem persist. This led to the assessment of the legal measures utilized by Iraq to confront cyber terrorism. The research is very germane because, it is the first of its kind to qualitatively examine the measures used by the Iraqi courts in confronting cyber terrorism and the challenges they encounter that has made it difficult to adequately address cyber terrorist crime in the country. Beside a clear analysis of the existing legislation, this research is an eye-opener to the ways Iraqi courts confront cyber terrorism. The study was able to highlight the inadequacies of the existing legislations used by Iraqi courts to confront cyber terrorism crimes while proposing a more extensive and robust legislation to address the problem.

LITERATURE REVIEW

Research on cyber terrorism is widespread. Cyber terrorism is among the most dangerous crimes of the age, targets electronic systems, infrastructure and information, for individuals, institutions and countries to harm them through terrorist groups and organizations (Abdulqadir, 2021; Adamov et al., 2019; BasuMallick, 2022; Ofusori & Hendradi, 2023). In Iraq, researchers have raised several issues regarding the inadequacy of the Iraqi legislations to cover cyber terrorism crimes in the country. For instance, **Nehme** (2020), highlighted the impasse of cyber terrorism laws with specific reference to Iraq. **Al-Tae and friends** (2020) also argued that Iraq is lagging behind in the global index of cybersecurity. Due to the lack of synergy between the Iraqi ministry of communications and its other ministries. Indicating the need to adopt a more realistic solution to achieve cybersecurity. **Klenka** (2021) describes cyber-attacks and the nature of its threat to civil aviation. Highlighting the dangers of cyber terrorism to the aviation industry. **Al-Shamari** (2021) blames the insecurity and poverty in Iraq on cyber terrorism which became possible due to the openness of Iraq to the outside world in 2003 and the advancement in information technology. **Baeewe** (2021) argues that the current Iraqi legal text fails to apply to modern forms of crimes like cyber terrorism. This has resulted in the exercise of wide powers by the Iraqi judiciary which violates the principle of legality. Calling for a legislative protection for citizens against cyber terrorist crimes. Additionally, **Alkhagafy and friends** (2023) used a qualitative and secondary data, utilized as evidence to highlight the need for legislative intervention in Iraq to address cyber terrorism.

METHODOLOGY

This research adopted a qualitative analysis methodology in assessing the legal measures to confront cyber Terrorism in Iraq. The research adopted qualitative research methodology (Correia, 2022; Warburton et al., 2018; Yalley & Olutayo, 2020). Existing legislations were analyzed qualitatively and a face-to-face semi-structured interview (Carroll & Windle, 2018; Onugha, 2018; Tanriverdi et al., 2018) was carried out with Judges in Iraq and the Kurdistan Region in Iraq to determine the ways in which the courts confront cyber terrorism. The research was conducted from September 2023 to January 2024. 11 informants were interviewed in the course of the research and 7 of the informants are judges of the Iraqi courts. The essence is to examine from first high sources how cyber terrorism is being

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

addressed in the courts in Iraq in the absence of adequate legislative provisions in that regard. The interview session took between 30minutes to 45minutes for each of the informants and ethical consideration was made through the interview session.

The interview was recorded by traditional means as such there was no need for any transcription. However, for the purpose of verification, the handwritten interview was sent to the informants to confirm and correct the statements made if any. The result of the interview were analyzed into themes using content analysis (Bakhrudin et al., 2023; Lessard et al., 2020) and the findings were summarized into two key issues. They are ways the Iraqi courts confront cyber terrorism and the challenges faced by the courts in confronting cyber terrorism. Due to the sensitive nature of the issue of cyber terrorism, the researchers used snow-ball technique (Shaffril et al., 2018) of referral to source the informants that were later interviewed. As such, the analysis did not carry the names of the informants but only extracts from the statements of some of the informants and summary of issues discussed by the informants.

FINDINGS AND DISCUSSION

1. Existing legislation on Cyber Terrorism in Iraq

In Iraq, terrorism has been mentioned and criminalize in several legislations like the Iraqi Penal Code, the Iraqi 2005 Constitution, and the two Iraqi anti-terrorism laws applicable to the Iraqi and Kurdistan Regions. The provisions of the laws relating to terrorism and cyber terrorism have been highlighted in Table 1 below, while the analysis of the provisions is addressed under this sub-heading.

i) The Iraqi Penal Code

The Iraqi Penal Code No. (111) of 1969 is considered a general rule of law that provides for criminalization and punishment. The law is applicable to the whole of Iraq including the Kurdistan region. The law confirms the principle of criminal legality in its first article when it provides that: *"there is only punishment of an act or omission based on a law which stipulates that it is a criminal offence at the time it is committed. No penalty or precautionary measure that is not prescribed by law may be imposed."* In addition, The Iraqi constitution also affirmed the principle of criminal legality in Article (19-2) (*The Iraqi Penal Code No. (111) of 1969*, n.d.).

In the context of terrorism, the law did not mention the penalties for terrorism as an independent law. Rather, the Iraqi legislator dealt with terrorism in such a way that it constitutes an element of some punishable crimes, such as the crime of conspiring to change the fundamental principles of the constitution, assaulting the basic systems of the state, or assaulting employees and citizens as provided in Article 200(2), 365 and 366 of Penal Code in Table 1. The expression "terrorist crimes" were mentioned in Article 21(a) (5) of the Iraqi Penal Code in the context of enumerating terrorist crimes that are not considered political, even if they were committed for a political motive, but the law did not define these crimes and did not bring similar ones. This reveals the fact that the Iraqi Penal Code still lacks provisions to criminalize cyber terrorism.

Furthermore, Article 361 of the Penal code, considers offenses of assaulting using wired and wireless communications to mean, crimes of public danger or crimes against the public interest. While in relation to creating a website or publishing information that violates public morals via technical means. The legislator did not deal with this type of scenario in a special law. As such, offences relating to cybercrimes in general, including the fact of setting up a website or publishing information contrary to public morals that occur through technical means have not been addressed in any of the Iraqi legislations. Therefore, when such cases are brought before the court, the courts usually refer to the

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

general rules in the amended Penal Code No. 111 of 1969 in order to address those cases legally. The courts finds support in Article 403 as captured in Table 1.

Under the criminal justice system in Iraq, no expansion is permitted in the interpretation of legal texts, and any doubt or ambiguity is always interpreted in favor of the accused (Alkhafagy et al., 2023; Baeewe, 2021). This has made judges to be constrained by the legality principle in the area of criminalization and punishment, which rests on the pillars of avoiding broad interpretation and not imposing more criminal liability than the legislature intended. Despite these constrains, a cursory look at the other provisions of the Iraqi Penal Code, revealed a couple of articles that define terrorism in general. The first of these provisions is Article 21(A)(5) (*The Iraqi Penal Code No. (111) of 1969*, n.d.), which defines terrorist crimes as crimes regardless of whether they were committed for political reasons or not. Furthermore, from the provision of Article 190 of the Iraqi Penal Code, the criminal offence is general, and it does not specify whether the intention of the legislators is in relation to terrorist acts, terrorism or not. However, considering the wordings of the Article, it is no doubt that acts of terrorism and terrorism can be interpreted within this provision. Additionally, Article 191 emphasized Article 190 by reiterating a general crime without specifying the motives or reasons behind these acts, whether they are for terrorist reasons, rebellion, or political motives. However, from the wordings of the provisions discussed above, terrorism and acts of terrorism including recruitment of juveniles into the acts of terrorism can be read and interpreted within the provisions.

Article 192 of the Iraqi Penal Code is similar to other articles highlighted in Table 1, it provides for a general offence without specification regarding the motives. Also, Article 194, relate to a general offence and they lack specification regarding the motives behind these actions. This pattern is also repeated in Articles 195, 196, 197, and 204 of the Iraqi Penal Code, Law No. 111 of 1969 not highlighted in Table 1. Therefore, from the analysis of the highlighted provisions of the Iraqi Penal Code, it is evident that these articles criminalize various unlawful and criminal acts characterized by violence. However, the legislators did not explicitly classify them as terrorist crimes. Hence, it would be difficult for the courts to interpreted terrorism or terrorist crimes, as well as cyber terrorism within these provisions, without a separate legislation to that effect. Based on the legality principle in the Iraqi criminal justice system and the rule of interpretation of statute. It would be more justifiable and effective to amend these provisions of the penal code and specify the particular crime or label these crimes to encompass all acts that aim to destabilize the country, jeopardize its security, and undermine its unity, as terrorism or acts of terrorism of any kind.

ii) The Iraqi constitution of 2005

The Iraqi constitution, is the supreme law in Iraq and the federal law by which Iraq is currently governed. The law like the Penal Code applies to all parts of Iraq including the Kurdistan region. The constitution was approved in a referendum on October 15, 2005, and entered into force in 2006. Terrorism has mentioned in several articles of the Iraqi constitution. The Iraqi constitution is one of the constitutions that expressly stipulates the danger of terrorism. The preamble to the Iraqi constitution is firm in its resolve against terrorism see Table 1. Furthermore, the impact of terrorism on the situation of individuals and Iraqi society, made the constitution to address the issue of terrorism sequentially in several provisions of the constitution. Such as Article 7, 21(3), 73 and 156. While the other provisions mention terrorism and its acts, Article 156 of the Iraqi Constitution provides punishment for an unnamed act, the interpretation of which can include terrorism. Although, the constitution did not explicitly mention terrorist acts in these provisions, but it can be argued that acts of terrorism could be included under these articles since the language used is general and not specific or exclusive. This shows that terrorism is not only recognized but regarded as a serious crime to humanity that warrants disbarring a convict of such vicious crime from benefiting from the society or fitting into the society. As

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

a means of purging the society of such individuals and such acts in general. However, the offence of terrorism from the Iraqi constitution has not been expanded to include cyber terrorism, as such cyber terrorism is not recognized under the law since it was not covered in any portion of the Iraqi 2005 constitution as highlighted in Table 1.

iii) The Iraqi Anti-terrorism Law No. (13) of 2005

The increase in terrorist operations and the threat to the lives of citizens in Iraq, led to the development of a special and independent law to combat terrorism. Therefore, the Iraqi National Assembly approved Law No. 13 of 2005, which is the Iraqi Anti-Terrorism Law and applicable to the Iraqi central region alone excluding the Kurdistan Region. The law consists of only 6 articles dealing with various issues related to terrorism. Article 1 defined terrorism and in Article 2, the law clarified the acts that are considered terrorist acts, but it did not include in its provisions, cyber terrorism through the use of the information system or the information network or any means of publication or information or the establishment of a website to facilitate the conduct of terrorist acts. Article 3 addressed the crimes that affect the security of the state (Article 3 *Iraqi Anti-Terrorism Act No 13 of 2005*, n.d.), and in Article 4, the law provides the penalties that apply to the perpetrators of these crimes (Article 4 *Iraqi Anti-Terrorism Act No 13 of 2005*, n.d.). Article 5 of the law makes provisions for exemption, legal excuses, and mitigating judicial circumstances (Article 5 *Iraqi Anti-Terrorism Act No 13 of 2005*, n.d.) and the final provisions of the Act relating to miscellaneous provisions are contained in Article 6 (*Iraqi Anti-Terrorism Act No 13 of 2005*, n.d.).

An analysis of the Iraqi Anti-Terrorism law, reveals that the law did not refer to or make provisions for the offense of cyber terrorism, its effects on society or criminalize cyber terrorism. Revealing the fact that cyber terrorism is not recognized as an offense under the Iraqi Anti-Terrorism Law. Hence, where cyber terrorism is committed and brought before the Iraqi court, it would be difficult for the judges to determine such a case, because there is no legal justification to hold the perpetrator liable for the alleged offense.

iv) Kurdistan Region Anti-Terror Law No. (3) of 2006

The Kurdistan Region is a region in Iraq, governed by the autonomous Kurdistan Regional Government (KRG) as provided under the Iraqi Constitution. The Kurdistan Region is the only constitutionally recognized autonomous region and permitted by the Iraqi Constitution to have its own executive, legislative and judicial powers, aside from those exclusive to the federal government. The Kurdistan Region has enacted its own counter terrorism law known as the "Kurdistan Region Anti-Terror Law No. 3 of 2006." The law consists of 18 articles. The first article like the Iraqi Anti-Terrorism Law No. 13 of 2005, defines terrorism or a terrorist act. As well as a definition of the acts that constitutes the concept of terrorism which seems broader than the Iraqi anti-terrorism law. The fourth paragraph of Article 4, provides for the criminalization of cyber terrorism crimes.

Similarly, the fourth paragraph of Article 3, provides for disrupting by means of communication and computer systems as part of terrorism which reveals that the Kurdish legislator are aware of the dangers of cyber terrorism and decided to deal with it in the terrorism law. Furthermore, the Kurdistan Region in 2008, enacted a Law to Prevent the Misuse of Telecommunications Equipment in the Kurdistan Region (No. 6/2008). Where in Article 2 and 3 of the law (*Kurdistan Region of Iraq Anti-Terror Law No (3)*, 2006), it provides for the punishment and offence of cyber terrorism as shown in Table 1. In summary, it is argued that, despite the efforts made by the Kurdistan legislators to confront cyber terrorism, there remains a lack of comprehensive definition and regulation to counter cyber terrorism in its legal framework in comparison with cyber terrorism in developed countries. As such,

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

there is much that needs to be done by the Iraqi government to confront this crime and strengthen the court's efforts in addressing cases of cyber terrorism.

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table 1: Existing legislations and provisions for confronting cyber terrorism in Iraq

Law	Provisions	Application
Penal Code No. 111 of 1969	**Article 200(2)** *"Any person who promotes or acclaims any movement that seeks to change the fundamental principles of the constitution or the basic laws of society or in order to raise one section of society over another or to oppress a particular section of society or to overthrow the basic social and economic laws of the State or the fundamental laws of society and the use of force, terror or any other illegal method is perceived in such action is punishable by a term of imprisonment not exceeding 7 years or by detention. The same penalty applies to any person who incites the overthrow of the appointed regime in Iraq or hatred of or scorn for such regime or acclaims or promotes anything that stirs up factional or sectarian chauvinism or encourages conflict between factions and classes or stirs up feelings of hatred and contempt among the population."* **Article 361** *"Any person who willfully causes damage to any means of cable or wireless communication set up for the public benefit or who disconnects or destroys any cable or equipment or willfully impedes the repair of such equipment is punishable by a term of imprisonment not exceeding 7 years or by detention. The penalty will be imprisonment if the offence is committed with the use of explosives or in time of war, civil strife or riot."* **Article 365** *"Any person who infringes or attempts to infringe with the use of force, violence, intimidation or menaces or by any other illegal means the right of a public official or agent to carry out his employment is punishable by detention plus a fine or by one of those penalties."* **Article 366** *"In circumstances other than those described in the preceding Paragraph, any person who uses force, violence, intimidation, menaces or other illegal method against the right of another to carry out his employment or the right to employ or refrain from employing a person is punishable by a period of detention not exceeding 1 year or by a fine not exceeding 100 dinars."* **Article 403** *"Any person who produces, imports, publishes, possesses, obtains or translates a book, printed or other written material, drawing, picture, film, symbol or other thing that violates the public integrity or decency with intent to exploit or distribute such material is punishable by a period of detention not exceeding 2 years plus a fine not exceeding 200 dinars or by one of those penalties."* **Article 191**	Applies to all parts of Iraq

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

	"Shall be punished by death or life imprisonment, anyone who assumes the leadership of a military unit, a military checkpoint, a port, or a city for criminal purposes without authorization from the government. The same penalty shall apply to anyone who continues to lead a military unit, regardless of the government's orders, as well as any commander who retains his armed forces or militias assembled after the government's order to discharge or disperse them." **Article 192** *"1. Anyone who initiates armed rebellion against the authorities established by the constitution or participates in a conspiracy or gang formed for this purpose shall be punished by temporary imprisonment.* *2. If the rebellion actually occurs, the penalty shall be life imprisonment.* *3. If the rebellion leads to armed clashes with state forces, results in the death of a person, or the perpetrator commands an armed force or fortification, the penalty shall be death."* **Article 194** *"Anyone who organizes, leads, or assumes leadership within an armed gang that attacks a group of residents, seeks to obstruct the implementation of laws, seizes state-owned or communal property by force, or resists public authorities with arms shall be executed. Those who join such a gang without taking part in its construction or assuming leadership will be sentenced to life in prison or a term of imprisonment."*	
Iraqi 2005 Constitution	**Preamble** *"We were not deterred by extremism and terrorism from moving forward to build a state of law. We, the resilient people of Iraq, emerged from our hardships and look confidently towards our future through a republican, federal, democratic, and pluralistic system. We have pledged, with our men, women, elders, and youth, to respect the rule of law, achieve justice and equality, reject aggression, and prioritize women's rights and concerns, as well as the concerns of our elders and the well-being of our children. We strive to promote a culture of diversity and extinguish the flames of terrorism."* **Article 7** *"Any entity or program that adopts, incites, facilitates, glorifies, promotes, or justifies racism or terrorism or accusations of being an infidel (takfir) or ethnic cleansing, especially the Saddamist Ba'ath in Iraq and its symbols, under any name whatsoever, shall be prohibited. Such entities may not be part of political pluralism in Iraq. This shall be regulated by law."* *"The State shall undertake to combat terrorism in all its forms, and shall work to protect its territories from being a base, pathway, or field for terrorist activities."* **Article 21(3)** *"Political asylum shall not be granted to a person accused of committing international or terrorist crimes or to any person who inflicted damage on Iraq."* **Article 73**	Applies to all parts of Iraq

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

	"The President of the Republic shall assume the powers to issue pardons on the recommendation of the Prime Minister, except for anything concerning a private claim and for those who have been convicted of committing international crimes, terrorism, or financial and administrative corruption" **Article 156** *"Shall be punished by death anyone who intentionally commits an act with the aim of undermining the independence, unity, or territorial integrity of the country, and any complete act that has the potential to lead to such consequences."*	
Iraqi Anti-terrorism Law No. 13 of 2005	**Article 1** *"Every criminal act committed by an individual or an organized group that targeted an individual or a group of individuals or groups or official or unofficial institutions and caused damage to public or private properties, with the aim to disturb the peace, stability, and national unity or to bring about horror and fear among people and to create chaos to achieve terrorist goals."*	Applies to central Iraq regions
Kurdistan Anti-Terrorism Law No. 3 of 2006	**Article 1** *": '[o]rganized use of violence, or threatening to use violence, or encouraging or glorifying the use of violence to achieve a criminal act either by an individual or groups randomly for the purpose of spreading terror, fear, chaos among the people to sabotage the general system or jeopardize security and safety in the region or the lives of individuals or their freedoms or security or sanctity, and causing damage to the environment or natural resources or public utilities or public or private properties to achieve political, intellectual religious, racist or ethnic aims or goals."* **Article 3(4)** *"Disrupting means of communication and computer systems, penetrating their networks, jamming them, or entering information or data in them with the aim of facilitating the commission of terrorist crimes."* **Article 4** *"Deliberately broadcasting news or data or broadcasting propaganda inciting terrorism or exploiting and using the visual, audio, print or electronic media, or publishing data on the Internet that amount to encouragement in direct ways for terrorist crimes that lead to undermining public security and spreading panic among people and threatening the political entity of the region."*	Applies only to the Kurdistan Region
Law to Prevent the Misuse of Telecom	**Article 2** *"He/she is punished by imprisonment for a period of no less than six months and not more than five years and a fine of no less than one million dinars and no more than five million dinars, or one of these two penalties, anyone who misuses a cell phone or any other wired or wireless communication devices, the Internet, or e-mail, by threatening, slandering, insulting, or publishing false news."*	Applies only to the Kurdistan Region

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

munications Equipment in the Kurdistan Region No. 6 of 2008	**Article 3** *"He shall be punished by imprisonment for a period of no less than three months and not more than a year, and a fine of no less than seven hundred and fifty thousand dinars and not more than three million dinars, or one of these two penalties, whoever intentionally causes the use and exploitation of a cell phone or any communication equipment. Wired or wireless, the Internet or e-mail, in order to disturb others, except for the cases mentioned in Article 2 of this law."*	

Source: Primary Analysis 2024

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

2. Ways through which Iraqi Courts Confront Cuber Terrorism

According to most of the judges in the Iraqi judges and Kurdistan region judges, despite the absence of special legislative texts to deal with cyber terrorism, they confront cyber terrorism through the existing legal frameworks. During the interview with the Iraqi judges both within the Iraqi region and the Kurdistan regions, they revealed that the Iraqi legal system does not include any provisions about the cyber terrorism, despite the high prevalence of diverse terrorist crimes in the country.

When the judges were asked how they confront cyber terrorism in the absence of legal provisions? The judges in Iraq and Kurdistan region claimed various views about this point. For instance a judges of the central investigator court of Iraq who specializes in terrorism cases said:

> *"The Iraqi Anti-Terrorism Law, No. 13 of 2005 provide us with wide definition that allow us to apply it with the cyber terrorism as well. Since there is a crime that threatens Iraqi security and peace and raises fear in the hearts of people, we must deal with it, whether it is ordinary or via the Internet. And cyber terrorism is a means and not a crime alone, because I believe that what was differed is not related to the origin of criminalization and punishment and it does not link to the legal formation of the crime, but it is only development into the means used to commit the crime."*
>
> He added that, *"Iraq does not have an electronic infrastructure and does not have the legislative capabilities to deal with these new crimes also. We and the legislators rely on the general rules in these new crimes. If a criminal act is found, the judiciary usually resorts to its authority to adapt and harmonize it with the general rules according to the applicable terrorism law."*

Two other judges within the Iraqi region say, in the absence of special legislation, they are forced to resort to the provisions of the Anti-terrorism law and consider cyber terrorism to be criminal assistance. Relying on the broad definition of terrorism in the Terrorist Act alongside the provisions of the Iraqi Penal Code and consider cyber terrorism to be means of assistance or at best part of a terrorists operation. Hence, they include all terrorist acts, including cyber terrorism as terrorism. This reveals the fact that the courts in Iraq consider cyber terrorism as criminal assistance and not an independent crime.

While in the Kurdistan region the situation is different, they have their own Anti-Terrorism Law No (3) of 2006 to deal with terrorism crimes including cyber terrorism in addition to 'misuse of communication devices' law to deal with cyber-crimes. When asked how the courts confront cyber terrorism, the judges opine that the Courts in the region deal with cyber terrorism under Articles 2, 3, 4, 5 & 7. For instance Articles 2(1) deals with establishing and joining a gang or organization like ISIS. Articles 3(1) deals with using communication to disrupt public institutions, 3(2) seizure of civilian aircraft or hijacking, 3(4) provides for an offence of disrupting computer system, and 3(5) provides against transfer of money within or outside Iraq by electronic means like Bitcoin. Article 4 (4) addresses intentional broadcasting using the internet or electronic means to propagate terrorism and Article 5 (c) provides for punishment for an attempt to commit the activities through electronic means which is a lesser punishment compared to the offence in Article 4. While Article 7(2) deals with cooperating with foreign country, body or organization to commit terrorism.

Despite these provisions, the judges are of the opinion that the provisions are inadequate to address specific aspect of cyber terrorism. For instance, one of the Kurdistan Judge of the national security investigation court said that:

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

> *"It is true that the Kurdistan anti-terrorism law mentions cyber terrorism acts in some ways, but we noticed deficiency in various aspects in the process of confronting the modern crimes… For instance, if you collect the statistics of cybercrime, you will see that most of them have been convicted according to Article 4, paragraph 4, but in the reality, they are different acts of cyber terrorism so they are also different in terms of criminal severity. But due to lack of the sufficient legal texts, we are forced to impose this legal provision on most acts of cyber terrorism."*

Another judge added that yearly they handle approximately 400 cases of terrorism, 250 cases on affiliation to terrorist groups and another 100 on terrorist activities which include acts of cyber terrorism but there are no adequate legal txt to address the crime. This indicates that there are crimes of cyber terrorism, but the Kurdistan courts tackle cyber terrorism under few provisions of the law due to lack of robust legislation to confront cyber terrorism effectively in the region like in the other parts of Iraq. Hence, the judges argue that they need a more comprehensive and clear law on cyber terrorism to keep pace with technological developments. Since all they do basically is interpreting the existing terrorism provisions to include cyber terrorism that has not be adequately addressed in any of the terrorism laws of both regions and the Iraqi Penal Code.

Judges generally do not have extensive power in criminal matters but are bound by the principle of criminal justice. In the absence of an appropriate or adequate legal text, they must resort to the provisions of the penal code. This means there is a possibility to determining the same case differently and imposing different punishments. For instance the same crime may receive a sentence of 5years in the Kurdistan Region while it receives 15yeras jail term in Iraq. Affecting the integrity of the whole Iraqi judicial system.

From the various responses of judges in the two regions of Iraq, the courts rely on interpreting existing laws to confront cyber terrorism's acts. Doing so, is likely to affect the principle of criminal legality. Interpretation is a judicial activity that seeks to determine the law applicable to the facts of a contested case by assigning meaning to a provision of the law and applying such law to the disputed facts. But on the condition that it does not expand the interpretation so as to prejudice the principle of criminal legitimacy (Assefa, 2017).

Criminal legality is one of the basic principles stipulated in most modern criminal legislation. What is meant by this is that the legislator alone has the power to determine the punishable acts, called (crimes), and determine the penalties to be imposed on their perpetrators, called punishments. Here, it is the legislative powers to make laws and determine crimes and punishments while it is the judicial duty to interpret the law and not otherwise. The purpose is to maintain the doctrine of separation of powers between the various arms of government (Babaeva et al., 2022; Lakin, 2017). Judges do not have the powers to make laws as doing so would amount to abuse of powers. Hence, in the absence of a provision criminalizing an act as a crime, the judges cannot consider the act as crime. Even if the act contradicts morality and public interest, it must have been so defined as a crime for the judge to adjudge it as such (Babaeva et al., 2022; Lakin, 2017).

Additionally, criminal legality is a fundamental principle on criminalization and punishments under the Iraqi Penal Code as mentioned earlier. Article 19(2) of the penal code provides that: "there is only punishment of an act or omission based on a law which stipulates that it is a criminal offence at the time it is committed. No penalty or precautionary measure that is not prescribed by law may be imposed." It means that to impose a penalty, first there must be a legal provision. The principle of legality states that no act can be punished unless the strength of the criminal rules in the legislation before the crime was committed (Puspitosari, 2020). Therefore, since the Iraqi judges rely on the broad definition of the anti-terrorism law in interpreting acts of cyber terrorism as terrorism to punish the perpetrators, it can be argued that cyber terrorism is yet to be acknowledge as an independent crime in Iraq. As such, the crime is not being adequately addressed as expected and there is a likelihood that the punishments are not commensurate to the crime committed and charged to court.

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

3. Difficulties faced by the Iraqi Courts in confronting cyber Terrorism

i) Lack of a Legal Text (Legislation)

Technological development have brought with it both benefit and causes. While it has ease man's activities, it has also create avenues for crime commission like cyber terrorism. Therefore, law must be developed to keep pace with advancement in technology. In this regard, any countries around the whole have developed their laws to include laws against cyber terrorism. Criminalizing acts such as creating a website to a terrorist purpose, or to promote its ideas, or to disseminate how to manufacture incendiary or explosive materials or any tools used in terrorist acts, or to disseminate the ideas and principles of a terrorist organization and call for them, or to finance and train terrorist operations, or to facilitate communications between terrorist organizations and their members and leaders. This is because, only by criminalizing a crime can the state have powers to punish perpetrators. In Iraq, as highlighted from the extract from existing legislations in Table 1 and the interview with the Iraqi judges, it is evident that there is the absence of a legal text to adequately address the crime of cyber terrorism in the country.

The lack of a legal text has hindered effective investigations into the activities of cyber terrorists. So as to apprehend them and reduce the crime in the country. Although the interview with the respondents reveal that the security operatives use tactics like eavesdropping, hacking and inserting devices into cyber terrorist systems to track them. These measures are used without existing legislation to back the procedures. Hence, it amounts to invasion of online privacy (Shakarian et al., 2013; Tran, 2016) which can have dare consequences on a nation (Huang, 2020; O'Flaherty, 2023; Zhou & Liu, 2023). As well as the issuance of arbitral judgments because the procedure resulting to the judgment was done without the due process of law. This was confirm by a judge of the Erbil Criminal Court who pointed out that the lack of provisions specifically for cyber terrorism and the large number of its actions often lead to arbitrariness in issuing the ruling

i) Punishment not commesurate to the Crime (Individualization of Punishment)

There is also the problem of proportionality and appropriateness between the punishment and the committed crime, known as 'individualization of punishment'. The concept of the individualization and suitability of punishment includes several characteristics that distinguish criminal punishment from others, and the need to guarantee justice in achieving criminal justice. This relates to the equality of punishment to the committed crime in general. Equality means the prescribed punishment that is commensurate to the crime is applicable to all perpetrators irrespective of status or position. Depending on the degree of involvement as prescribed by law (Vorapatr et al., 2023). The intended equality, then, is that equality before the law, which is relative, not absolute (Farmer, 2020).

Researchers have argued that in terms of suitability, the punishment must be divisible and flexible to allow the judge issue the appropriate punishment for a crime depending on the degree of criminality. Hence, the judge must be allowed to estimate the appropriate punishment within the appropriate limits of the punishment, and can be achieved through the implementation of mitigating circumstances as provided under Article 132 of the Iraqi Penal code (Khalaf Naser, 2020; Shamsuldin, 2021). The concept of individualization of punishment was first coined by Rymond Sailes jurist (Donovan, 2021). By way of emphasis, Beccaria wrote, saying: "...Crimes of every kind should be less frequent, in proportion to the evil they produce to society ... If an equal punishment be ordained for two crimes that injure society in different degrees, there is nothing to deter men from committing the greater as often as it is attended with greater advantage..." (Mooney, 2019).

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Therefore, the punishment must be proportionate to the condition of the offender and the circumstances of his crime due to the purpose of punishment (Ranasinghe, 2023). The Iraqi Court of Cassation claimed that the punishment should not be so severe that it is not taken into account, nor should it be unjustifiably harsh, as there is no benefit from a non-deterrent punishment (Shamsuldin, 2021). This confirms that the severity of punishment must be proportionate to the personal circumstances of the offender and the objective circumstances of his crime in order for the punishment to bear fruit and achieve its functions. As it is, the minimum punishment under the cyber terrorist law in Iraq is 15years. The judges during interview also confirmed that they cannot issue less than 15years imprisonment for any terrorists' crime. This means that, in the absence of a specific legal text addressing cyber terrorism, any acts of cyber terrorism which the Iraqi judges handle, usually rely on the anti-terrorism Act in deciding the case and granting not less than 15years punishments. It is argued that the punishment is not commensurate with the crime committed. Since most cyber offences do not require capital punishment of 15years to death penalty.

However, in the Kurdistan region the situation is different, the Kurdish Ant-terrorism law has provided more flexible provisions for the judges, there are more than one options for judges to choose in imposing punishment depending on the type of crime committed and the circumstances of the crime, as it extends from a prison sentence to life imprisonment and death penalty. Therefore, it is argued that although the Kurdish judges claim inadequacy in their anti-terrorism law regarding cyber terrorism, yet with the flexibility of punishment options, they can issue punishments that are commensurate with the crime. Though, it will be difficult for them to effectively address cyber terrorism in the absence of robust provisions on cyber terrorism.

ii) Determining Jurisdiction of Cyber Terrorism crimes

The issue of cross-border or extraterritorial or trans-jurisdictional crime is common to terrorism and cyber terrorism in particular because most cybercrime are committed outside the mother country. This creates the problem of jurisdiction, the court that has jurisdiction to determine the crime, the applicable law and the issue of enforceability of the judgment of the court that determines the case. The majority of Iraqi penal laws do not provide for extraterritorial application but predicated almost exclusively on the locus delicti territorial doctrine. This doctrine asserted that the authority to prescribe laws to criminalize is restricted to crimes committed within the Iraqi borders.

Generally, the state's right to punish, and therefore its right to issue penal laws, is considered one of the main manifestations of its sovereignty over its territory. Since the state's sovereignty in principle must not extend beyond its territory, it behooves that its powers to criminalize and punish is restricted to its territory. As acting outside its territory infringes on the sovereignty of another country under the principle of territorial jurisdiction (Farmer, 2013; Kenneth, 2022; Payer, 2023). Though some exceptions exist in the application of this principle. This principle of territorial criminal jurisdiction is incorporated in a state's criminal law. In Iraq for instance, the principle of territorial jurisdiction in criminal matters is provided in Article 6 of the Iraqi Penal Code. It provides that, "The provisions of this law apply to all crimes committed in Iraq…" Highlighting the fact that crimes committed in Iraqi are subject to Iraqi law, regardless of the perpetrator's nationality. As what is important is the presence of the perpetrator in Iraq.

The general principle of territorial jurisdiction as provided under Article 6 of the Iraqi Penal Code is difficult to apply to cyber terrorism. Given its nature and the characteristics that distinguish it from traditional crime, especially the difficulty of accurately determining the place and time of its commission. Besides, the borderless nature of cyber terrorism and the unconventional technologies

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

used by cyber terrorists make it difficult, if not impossible to apply the traditional doctrine of territoriality to cyber terrorism.

One of the exceptions to the principle of territorial jurisdiction include the doctrine of in rem jurisdiction which means applying state's criminal law to every crime that affects its basic interest regardless of the place of the commission of the offence and the nationality of the perpetrator. Article 9(1) of t Iraqi Penal Code stipulates that the criminal law applies to anyone who commits any crime that affects both the external and internal security of Iraq. Therefore the in rem jurisdiction applies to cyber terrorism perpetrators whether local or foreigners, irrespective of the applicable law, jurisdiction or location of the perpetrator. Provided the crime was committed against Iraq. However, its application would encounter difficulties because the measure used are unclear due its nature and the perpetrators are mostly unknown to enable prosecution.

Secondly, is in terms of the doctrine of personal jurisdiction. Personal jurisdiction means applying the state's criminal law to every person who holds its nationality, even if he commits his crime outside its territory. The perpetrator is deemed subject to his/her national legislation. This is because the citizen enjoys his/her country's protection while abroad, hence bound to obey his country's legislation. Likewise, the possibility of punishing the national for crimes committed abroad indirectly strengthens the national law and the values it protects. In addition, this principle complements the rule that a state may not extradite its citizens to the foreign state in whose territory they committed the crime, as it guarantees that they will not escape punishment (Farmer, 2013; Kenneth, 2022). Personal jurisdiction in Iraq is contained in Article 10 & 11 of the Iraqi Penal Code. It covers offences committed by an Iraqi, an employee or person in public service and Iraqi diplomats who commits a felony or misdemeanor outside Iraq. But in cyber terrorism crime, using personal jurisdiction would jeopardize the main purpose of curbing the menace because of the nature of the crime and complexity involved in identifying the perpetrators.

Thirdly, the doctrine of universal jurisdiction which seems for appropriate in handling cases of cyber terrorism crimes. The principle of universality is based on the idea of solidarity between countries in combating crime and emphasizing the universality of punishment so that the perpetrator of the crime does not escape punishment for the humanitarian interest of the international community (Payer, 2023). Many countries have adopted this principle in their criminal legislation. In Iraq for instance, this principle was adopted in Articles 9, 10, 11 & 13 of the Penal Code and Article 3(6) of the Iraqi Anti-Terrorism Law of 2005. The provisions apply to anyone found in Iraq after committing a crime abroad either as a perpetrator or an accomplice of any of the following crimes: sabotaging or disrupting communications means and international transportation, and trafficking in women, children, slaves, or drugs.

In terms of cyber terrorism, research have shown that universal jurisdiction is the best measure to be adopted in addressing the crime (Payer, 2023). This is because it ensure accountability, and promote international peace and justice (Michielin, 2020). However, the doctrine of universality has not been extended to cyber terrorism because of legal and political reasons. More so that the doctrine is not available to prosecutors because it will exacerbate interstate conflict while at the same time prove ineffective in preventing and prosecuting cyber terrorist crimes (Stockton & Michele Golabek-Goldman, 2014).

Currently, customary international law have restricted the scope of universal crimes to those offenses deemed to be "heinous" in nature such as: piracy, genocide, torture, war crimes, and crimes against humanity. Therefore, for cyber terrorism to invoke universal jurisdiction, it must be proved to fall within heinous crimes (Abdelkarim, 2023).

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

iii) Lack of International Judicial Cooperation

To effectively investigate and prosecute electronic and internet-related crimes, there is a need to trace the crime through diverse internet service providers or companies providing those services (Broeders et al., 2020). These ivestigations must follow computer communication channels to succeed. Law enforcement agencies often have to rely on historical records that reveal when those connections were made, the location and presense of perpetators (Horan & Hossein, 2021) during investigations. But often very difficult to achieve without assistance and collaboration of other countries. Since cyber terrorism is a global crime that cuts across jurisdiction, therefore, international judicial assistance is required. This assistance is defined as every judicial procedure undertaken by a country that facilitates the task of trial in another country in connection with A crime (Corsei, 2023), and judicial assistance in the criminal field takes several forms including information sharing (Efrat & Newman, 2018). Such as Article 1, paragraphs 2(f) & (g) of the United Nations Model Treaty on Mutual Assistance in Criminal Matters, Article 4 clause (f) of the Organization of the Islamic Conference on combating International Terrorism, Article 1 of the Riyadh Arab Agreement on Judicial Cooperation, and Article 8 (3) & (4) of the United Nations Convention against Transnational Organized Crime of 2000.

Secondly, cyber terrorism also require transfer of criminal proceedings from one authorized entity of a state to another with the request to investigate and prosecute perpetrators based on certain verified conditions (de Jonge, 2020). Such as in cases of dual criminality, existance of legitimacy of proceedings available in both jurisdictions and the measures required can reveal the commission of the crime (de Jonge, 2020). Transfer of criminal proceedings has been adopted in some international treaties and conventions like the United Nations Model Treaty on the Transfer of Procedures in Criminal Matters, Article 21 of the United Nations Convention against Transnational Organized Crime 2000 and Article 9 of the Organization of the Islamic Conference Treaty to Combat International Terrorism 1999.

Thirdly, it require international judicial regatory, a judicial assistance that a state's judicial authority grants permission to a different state's authority, responsible for carrying out specific judicial actions linked to a particular criminal procedure, to investigate and prosecute on behalf of the first state (Corsei, 2023). This method aims to facilitate criminal procedures between countries in order to ensure that the necessary investigations are conducted to bring the accused to trial and to overcome the obstacle of territorial sovereignty that prevents the foreign state from exercising some judicial actions within the territories of other countries, such as hearing witnesses or conducting inspections, etc. Usually, as is usual, the request for a judicial rogatory letter is sent through diplomatic channels (Corsei, 2023).

Fourthly is extradiction, a form of international cooperation in combating crime and criminals and protecting societies from those who disturb their security and stability, so that those who violate their security do not remain immune from punishment (Edmonds-Poli & David A. Shirk, 2018). This is because cyber terrorism like telecommunication and other informaton techology-related crimes are borderless, perpetrators are not restricted to a specific region but have access to countless regions within the speed of light. Therefore the crime has an international character, and the criminal himself has become an international criminal requiring international intervervention (Edmonds-Poli & David A. Shirk, 2018).

Extradition is a procedure of international judicial cooperation in which one state (the requested state) extradites a person present on its territory to another state, or to an international judicial body (the requesting state or entity, either for the purpose of trying him for a crime he was accused of committing, either for the purpose of implementing the conviction issued against him by the

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

courts of this country (Corsei, 2023). It is also 'the delivery of an accused or a convicted individual to the state where he is accused of or has been convicted of, a crime, by the state on whose territory he happens to be for the time to be.'(Sekati, 2022). However, the sources of extradiction differ according to a country's legal system, treaties and agreements and circumstance (Sekati, 2022). For extradiction to be executed, there must be dual criminality (Sekati, 2022), the crime must constitute one of the crimes that permits extradiction because political, military or crime of low importance are excluded (Klaassen, 2017; UNODC, 2012). As well as risk of persecution in the requesting state due to gender, race, religion, ethnic origin, nationality, or political opinion(UNODC, 2012) and risk of unfair trial in requesting state (UNODC, 2012). Except in cases of inadmissibility of extradicting nationals, double jeopady and persons granted assylum (Klaassen, 2017; UNODC, 2012). These measures assist in combating cyber terrorism and internet-related crimes that cuts across borders.

In Iraq, terrorist groups like Al-Qaeda, al-Naqshabandia, and ISIS, have ravaged the country with a third of its population affected by ISIS in 2014. ISIS is one group koown for its acts of cyber terrorism but the Iraqi judges complained that many of their letters for international assistance was turned down initially, but much later, the international assistance they got helped to reduce ISI menace i the country. But much of international cooperation is still needed in this regard in Iraq to help combat terrorism and cyber terrorism in particular in Iraq.

iv) The Authenticity and Strength of digital Evidence

Investigating officers in cyber crimes or electronic crimes seek evidence that may help them to prove the facts and attribute it to the accused. However, they encounter difficulties due to lack of a legal text that provides for the procedure for investigation and prove in cyber terrorist crimes cases in Iraq. This cases usually require electronic evidence that is characterized by objectivity, impartiality, and efficiency. Usually a digital evidence. However, whether digital evidence lgal and admissible depends on the provision of ttthe Iraqi legislation on procedural rules. Article 213 (a) of the Criminal Procedure Code (CPC) provides that the verdict of the court in a case is based on the extent to which it is satisfied by the evidence presented during any stage of the inquiry or the hearing.in this context, evidence includes admission reports, witness statements, written records of an investigation, other official discoveries, reports of experts and technicians (background information), and other evidence by saying "and other legally established evidence." For cyber terrorist crime to be determined bfore the court, there must be prove of evidence and the evidence must be in the form that it is acceptable in accrodance with the provision of the CPC. To detrmine the strength of digital evidence in Iraq, the evidence must be determined within any of the doctrine of proof as obtainable in most jurisdictions. Such as by a) free proof regime which allows parties to proof their claim by all possible means, b) evidence-sorting where parties are bound to rely on specific rules and methods of proof and c) mixed proof where both methods are used in proof of a case (Ashour & Hayder Ars Afan, 2023; Choo, 2015). In cyber terrorism crimes, digital evidence is more appropriate than traditional evidence and both dffer from each other. Including the decoding and conversion of magnetic and electrical impulses into data and information related to the crime. In the absence of existing legislation on procedure in cyber terrorism cries in Iraq, judges who were interviewed said that when electronic evidence are presented before them, they consider it as presumptious evidence or indirect-evidence. Hence, they cannot convict an accused on the basis of one presumption, but the presumptious evidence must be supported by another evidence to grant conviction. This means, where the only available evidence is a digital evidence, then the perpetrators would escape liability for their criminal acts which is dangerous to the Iraqi society.

CONCLUSION

This reaserch assessed the Iraqi legal measures available to confront cyber terrorism in Iraq. The various legal text on terrorism such as the Iraqi Penal Code, 2005 Iraqi Constitution, the Iraqi Anti-Terrorism Law No. 13 of 2005 and the Kurdistan Region's Anti-Terror Law No. 3 of 2006 were analyzed. The analysis revealed that there are provisions on terrorism as a crime in the Penal Code, Constitution

and Anti-Terrorism laws. While only the Kurdistan Region's anti-terror law that mentined cyber terrorism. However, the provisions are narrow and did not adequately address all aspects of cyber terroorism. Yet, cyber terrorism continue to ravage the country.

When the judges were interviewed to asertain how they confront cyber terrorism in the courts. The judges in Iraq argue that they treat cyber terrorism as a means of assistance and as an aspect of terrorism but not as an independent crime because there is no specific provision to address it. Hence, they rely solely on the general principles of criminal legality as provided in Article 19(2) of the Iraqi Penal Code in handling cases of cyber terrorism. On the other hand, the judges in the Kurdistan Region argue that Articles 2, 3, 4, 5, and 7 of the Kurdistan Region Anti-Terrow Law makes provision for cyber terrorism. Yet the provisions have not adequately dealth with all aspects of cyber terrorism so they rely on genral principle of criminal legality just as it is obtainable with the Iraqi judges. This means that, both the courts in Iraq and the Kurdish region rely on the general principles of criminal legality to confront cyber terrorism in the absence of specific and adequate provisions to deal with the crime.

Challenges to confronting cyber terrorism in the Iraqi courts were identified by the judges. Including lack of legal text to address the crime of cyber terrorism, administering punishment that is not commurate with the offense, jurisdictional issue due to the cross-border and trans-jurisdictional nature of the crime, procedural difficulties, strength of evidence and lack of international cooperation. Similarly, reliance on genral principles of criminal legitimacy has resulted in interpreting existing legal text to address criminal activities that have not been considered as crime but interpreted to constitute crime which prejudices the principle of criminal legitimacy. Therfore, this research suggest the development of a seperate legislation that ir clear and robust to address all aspect of cyber terrorism and the procedure for investigation and appreending perpetrators. While this rresearch have not adequately delve into procedural difficulties and specific issues that should be included in the propose legislation, there is need for more research in these areas.

REFERENCES

[1] Abdelkarim, Y. (2023). Employing The Responsibility to Protect to Impose Universal Jurisdiction Regarding Cyber-Terrorism: Eradicating Cyber-terrorists' Impunity in International Law. *Papers.Ssrn.Com*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4428168

[2] Abdulqadir, J. & Z. (2021). The evolution of terrorism and its reflection on the stability of societies. . . *Journal of Research and Studies in International Relations*, *13*(1). https://dspace.univ-ouargla.dz/jspui/handle/123456789/24891

[3] Abu-Taieh, E., Alfaries, A., Al-Otaibi, S., & Aldehim, G. (2018). Cyber security crime and punishment: comparative study of the laws of Jordan, Kuwait, Qatar, Oman, and Saudi Arabia. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, *8*(3), 46–59.

[4] Adamov, A., Carlsson, A., & Surmacz, T. (2019). An analysis of lockergoga ransomware. *2019 IEEE East-West Design and Test Symposium, EWDTS 2019*. https://doi.org/10.1109/EWDTS.2019.8884472

[5] Aissani, R. (2022). Anti-cyber and information technology crimes laws and legislation in the gcc countries: A comparative analysis study of the laws of the UAE, Saudi Arabia and Kuwait. *Journal of Legal, Ethical and Regulatory Issues*, *25*(1), 1–14.

[6] Al-Shamari, M. I. (2021). Cybersecurity and its impact on Iraqi national security (in Arabic). *Journal of Legal and Political Sciences*, *10*(1).

[7] Al-Tae, A. K. J., Al-Dhalimi, H. A.-H., & Al-Shaibani, K. J. (2020). Relationship of Cybersecurity and the National Security of the Country: Iraq Case Study. *Sys Rev Pharm*, *11*(12), 469–476.

[8] Albahar, M. (2019). Cyber attacks and terrorism: A twenty-first century conundrum. *Springer*, 993–1006.

[9] Alghamdi, M. I. (2020). A Strategic Vision to Reduce Cybercrime to Enhance Cyber Security. *Webology*,

17(2), 289–295. https://doi.org/10.14704/WEB/V17I2/WEB17031

[10] Alkhafagy, T., Nazem, S. N., Farhan, A. F., Salman, S. D., Khudadad, A. M., Nsaif, A. D., Gatafa, A. A., Sabti, A. A., & Abdelhassan, M. I. (2023). Cybercrime and Inheritance Legislation in Iraq: Extension of Perspectives on Inheritance Legislation within Iraq. *International Journal of Cyber Criminology*, *17*(2), 63–76. https://doi.org/10.5281/zenodo.4766705

[11] Ambika, T., & Senthilvel, K. (2020). Cyber Crimes against the State: A Study on Cyber Terrorism in India. *Webology*, *17*(2), 65–72. https://doi.org/10.14704/WEB/V17I2/WEB17016

[12] Anjum, A. (2022). *Adopting a strategy of urgency to achieve cyber resilience*. 26–37.

[13] Ashour, A. J., & Hayder Ars Afan. (2023). Legality of Electronic Evidence in Criminal Evidence. *Journal of Namibian Studies: History Politics Culture, 33*(1), 33–34. https://namibian-studies.com/index.php/JNS/article/view/431.

[14] Assefa, S. K. (2017). Methods and manners of interpretation of criminal norms. *Mizan Law Review*, *11*(1), 88–124.

[15] Babaeva, Y., Bauman, N., Grudtsina, L., Lazareva, M., & Mnatsakanyan, V. (2022). Legality in the Implementation of the Principle of Separation of Powers. *Lex Humana*, *14*(1), 420–429.

[16] Baeewe, S. S. (2021). Cybercrime under the New Iraqi Draft Cybercrime Law. *Journal of the College of Basic Education*, 123–141.

[17] Bakhrudin, B., Margolang, F. I., Sudarmanto, E., & Sugiono, S. (2023). Islamic Perspectives on Cybersecurity and Data Privacy: Legal and Ethical Implications. *West Science Law and Human Rights*, *1*(04), 166–172. https://doi.org/10.58812/wslhr.v1i04.323

[18] BasuMallick, C. (2022). *"What is hacktivism?" Meaning, workings, types, and examples*. Spiceworks. https://www.spiceworks.com/it-security/cyber-risk-management/articles/what-is-hacktivism/

[19] Brière, C. (2021). EU Criminal Procedural Law onto the Global Stage: The e-Evidence Proposals and Their Interaction with International Developments. *European Papers-A Journal on Law and Integration*, *6*(1), 493–512.

[20] Broeders, D., Els De Busser, & and Patryk Pawlak. (2020). Three tales of attribution in cyberspace: Criminal law, international law and policy debates. *The Hague Program for Cyber Norms Policy Brief*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3589139.

[21] Carroll, P., & Windle, J. (2018). Cyber as an enabler of terrorism financing, now and in the future. *Journal of Policing, Intelligence and Counter Terrorism*, *13*(3), 285–300. https://doi.org/10.1080/18335330.2018.1506149.

[22] Choo, A. L.-T. (2015). Evidence,(In) efficiency, and freedom of proof: a perspective from England and Wales. *Ala. L. Rev*, *66*(3), 493–505. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/bamalr66&section=27.

[23] Correia, V. J. (2022). An Explorative Study into the Importance of Defining and Classifying Cyber Terrorism in the United Kingdom. *SN Computer Science*, *3*(1).

[24] Corsei, A. (2023). International Judicial Cooperation in Criminal Matters. *European Integration Realities and Perspectives. Proceedings 2023 Proceedings*, *18*(1), 32–38. https://dp.univ-danubius.ro/index.php/EIRP/article/view/357..

[25] Couzigou, I. (2022). The Criminalization of Online Terrorism Preparatory Acts Under International Law. *Studies in Conflict and Terrorism*, *45*(5–6), 535–554.

[26] de Jonge, B. (2020). Transfer of criminal proceedings: from stumbling block to cornerstone of cooperation in criminal matters in the EU. *ERA Forum*, *21*(3), 449–464. https://doi.org/10.1007/S12027-020-00616-8

[27] Dhirani, L. L., Mukhtiar, N., Chowdhry, B. S., & Newe, T. (2023). Ethical Dilemmas and Privacy Issues in Emerging Technologies: A Review. *Sensors*, *23*(3). https://doi.org/10.3390/s23031151

[28] Djenna, A., Bouridane, A., Rubab, S., & Marou, I. M. (2023). Artificial Intelligence-Based Malware Detection, Analysis, and Mitigation. *Symmetry*, *15*(3), 1–24. https://doi.org/10.3390/sym15030677

[29] Donovan, J. M. (2021). The French judicial and political origins of Raymond Saleilles' individualization of punishment. *The Limits of Criminological Positivism: The Movement for Criminal Law Reform in*

the West, 1870-1940, 74–97. https://doi.org/10.4324/9780429323713-4/French-Judicial-Political-Origins-Raymond-Saleilles-Individualization-Punishment-James-Donovan.

[30] Durac, V. (2018). Counterterrorism and democracy: EU policy in the Middle East and North Africa after the uprisings. *Mediterranean Politics*, *23*(1), 103–121.

[31] Edmonds-Poli, E., & David A. Shirk. (2018). Extradition as a Tool for International Cooperation: Lessons from the US-Mexico Relationship. *Md. J. Int'l L*, 33–215

[32] Efrat, A., & Newman, A. L. (2018). Divulging data: Domestic determinants of international information sharing. *The Review of International Organizations*, *13*(3), 395–419. https://doi.org/10.1007/S11558-017-9284-1.

[33] Farmer, L. (2013). Territorial Jurisdiction and Criminalization. *The University of Toronto Law Journal*, *63*(2), 225–246. http://www.jstor.org/stable/24

[34] Geo. (2016, August 20). *US hacked NTC to spy on Pakistan military, political leadership: Snowden documents*. Geo News. https://www.geo.tv/latest/112040-US-hacked-NTC-to-spy-on-Pakistan-military-political-leadership-Snowden-documents

[35] Horan, C., & Hossein, S. (2021). Cyber crime investigation: Landscape, challenges, and future research directions. *Journal of Cybersecurity and Privacy*, *1*(4), 580–596. https://doi.org/10.3390/jcp1040029.

[36] Huang, J. (2020). Applicable law to transnational personal data: Trends and dynamics. *German Law Journal*, *21*(6), 1283–1308. https://doi.org/10.1017/glj.2020.73

[37] *Iraqi Anti-Terrorism Act No 13 of 2005*. (n.d.).

[38] Kenneth, G. S. (2022). *The Territorial Principle', International Criminal Jurisdiction: Whose Law Must We Obey?* (Onine). Oxford Academic. https://doi.org/https://doi.org/10.1093/oso/9780199941476.003.0004

[39] Khater, M. H. (2023). International Perspective on Securing Cyberspace Against Terrorist Acts. *International Journal of Sociotechnology and Knowledge Development (IJSKD)*, *15*(1), 1–11. https://doi.org/10.4018/IJSKD.318706.

[40] Khalaf Naser, M. (2020). The Violation of the Principle of Equality in the Iraqi Penal Code. *International Journal of Innovation, Creativity and Change*, *13*(6).

[41] Klenka, M. (2021). Aviation cyber security: legal aspects of cyber threats. *Journal of Transportation Security*, *14*(3–4), 177–195.

[42] Klaassen, P. (2017). *The Threshold of Inhuman and Degrading Treatment or Punishment: under which circumstances should extradition, expulsion, or return be refused?* https://studenttheses.uu.nl/handle/20.500.12932/28836

[43] *Kurdistan Region of Iraq Anti-Terror Law No (3)*. (2006).

[44] Lakin, S. (2017). Legality as separation of powers. *Jurisprudence*, *8*(3), 653–659. https://doi.org/10.1080/20403313.2017.1385298.

[45] Lessard, G., Lévesque, S., Lavergne, C., Dumont, A., Alvarez-Lizotte, P., Meunier, V., & Bisson, S. M. (2020). How Adolescents, Mothers, and Fathers Qualitatively Describe Their Experiences of Co-Occurrent Problems: Intimate Partner Violence, Mental Health, and Substance Use. *Journal of Interpersonal Violence*, 1–24. https://doi.org/10.1177/0886260519900968

[46] Marsili, M. (2018). The war on cyberterrorism. *Democr Secur*, *15*(2), 172–199. https://doi.org/10.1080/17419166.2018.1496826.

[47] Michielin, S. (2020). *Cyberterrorism: A study of the issue in the framework of the Council of Europe*. http://dspace.unive.it/handle/10579/18331.

[48] Mooney, J. (2019). *The theoretical foundations of criminology: Place, time and context*. https://books.google.com/books?hl=en&lr=&id=uZ7BDwAAQBAJ&oi=fnd&pg=PT13&dq=++Cesare+Beccaria+If+an+equal+punishment+be+ordained+for+two+crimes+that+injure+society+in+different+degrees&ots=-TUlDlE5LM&sig=dpIS-_zj7Cmg-WwEjYX8lCopOXY.

[49] Muhammad Nadeem Mirza, & Muhammad Shahzad Akram. (2022). 3-Cs of Cyberspace and Pakistan: Cybercrime, Cyber-Terrorism, and Cyber Warfare. *Strategic Studies*, *42*(1), 62–80. https://doi.org/10.53532/ss.042.01.00134
[50] Nehme, T. (2020). Impasse of Cyber laws: Iraqi Case. *Defence Magazine*, 112. https://www.lebarmy.gov.lb/en/content/impasse-cyber-laws-iraqi-case
[51] O'Flaherty, V. K. (2023). Protecting Privacy Online. *Business Sportlight*, *3*.
[52] Ofusori, L. O., & Hendradi, R. (2023). Understanding the Impact of the Dark Web on Society: A Systematic Literature Review. *International Journal of Information Science and Management*, *21*(4), 1–21. https://doi.org/10.22034/ijism.2023.1978002.0
[53] Onugha, C. V. (2018). *Partners in national cyber security strategy?: An analysis of cyber security strategies of Ministry of Defence and police in UK*.
[54] Payer, A. (2023). The Territorial Principle as a Basis for State Criminal Jurisdiction: Particularly with Regard to Cross-Border Offences and Attempts, and to Multiple Parties to an Offence Acting in Different Countries. *International Criminal Law Review*, *23*(2), 175–238. https://doi.org/10.1163/15718123-bja10151.
[55] Puspitosari, S. H. (2020). *Cybercrime in The field of Decency: Information Technology and Morality*. https://books.google.com/books?hl=en&lr=&id=c6j7DwAAQBAJ&oi=fnd&pg=PR5&dq=Cybercrime+in+The+field+of+Decency:+Information+Technology+and+Morality&ots=r-DF8FIIkk&sig=JVObVIysJxsf96bze1qUoiKEGf4.
[56] Ranasinghe, P. (2023). Cesare Beccaria and the Aesthetic Knowledge of On Crimes and Punishments. *Law and Critique*, *34*(1), 127–144. https://doi.org/10.1007/S10978-022-09321-6.
[57] Rudner, M. (2016). "Electronic jihad": The internet as al-qaeda's catalyst for global terror. *Violent Extremism Online: New Perspectives on Terrorism and the Internet*, 8–24.
[58] Sedeeq, F. M., & Ghareb, M. I. (2018). Electronic Crimes And The International Community Legislation: Comparative Analytical Study. *International Journal of Scientific & Technology Research*, *7*(8).
[59] Sekati, P. (2022). Assessing the effectiveness of extradition and the enforcement of extra-territorial jurisdiction in addressing trans-national cybercrimes. *International Law Journal of Southern Africa*, *55*(1). https://journals.co.za/doi/pdf/10.25159/2522-3062/10476
[60] Shaffril, H. A. M., Krauss, S. E., & Samsuddin, S. F. (2018). A systematic review on Asian's farmers' adaptation practices towards climate change. *Science of the Total Environment*, *644*, 683–695. https://doi.org/10.1016/j.scitotenv.2018.06.349
[61] Shakarian, P., Shakarian, J., & Ruef, A. (2013). *Introduction to cyber-warfare : a multidisciplinary approach*. 318. https://books.google.com/books/about/Introduction_to_Cyber_Warfare.html?id=ziq8LPWfgkIC
[62] Shamsuldin, B. (2021). Legitimate Rooting of the Principle of Individualization of Punishment in Iraqi Law. *Anbar University Journal for Islamic Sciences*, *12*(4), 225–270
[63] Stockton, P. N. , & Michele Golabek-Goldman. (2014). Prosecuting cyberterrorists: Applying traditional jurisdictional frameworks to a modern threat. *Stan. L. & Pol'y Rev*, 25–211. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/stanlp25&section=15.
[64] Tanriverdi, G., Çapik, C., & Yalçin Gürsoy, M. (2018). Prevalence of domestic violence against married women in Turkey and associated risk factors. *Turkiye Klinikleri Journal of Medical Sciences*, *38*(3), 218–229. https://doi.org/10.5336/medsci.2017-58822
[65] *The Iraqi Penal Code No. (111) of 1969*. (n.d.).
[66] Tran, J. L. (2016). Navigating the cybersecurity act of 2015. *The Chapman Law Review*, *19*(2).
[67] Trautman, L. J. (2016). Congressional Cybersecurity Oversight: Who's Who and How It Works. *Journal of Law and Cyber Warfare*, *5*, 147.
[68] UNODC. (2012). *Handbook on Mutual Legal Assistance and Extradition, United Nation Office on Drugs and Crime*.
[69] Vorapatr, T., Jirawut Lipipun, & and Sonthon Khongwan. (2023). The rule of law and the individualization of punishment in Thailand. *Kasetsart Journal of Social Sciences*, *44*(2), 639–644.

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

[70] Tulga, A. Y. (2022). Hard and soft terrorism concepts: the case of ISIS. *Pakistan Journal of Terrorism Research*, *3*(2), 109–132.

[71] Warburton, W., Whittaker, E., & Papic, M. (2018). Homelessness Pathways for Australian Single Mothers and Their Children: An Exploratory Study. *Societies*, *8*(1), 16. https://doi.org/10.3390/soc8010016

[72] Yalley, A. A., & Olutayo, M. S. (2020). Gender, masculinity and policing: An analysis of the implications of police masculinised culture on policing domestic violence in southern Ghana and Lagos, Nigeria. *Social Sciences & Humanities Open*, *2*(1), 100077. https://doi.org/10.1016/j.ssaho.2020.100077

[73] Zheng, F., & Di, G. (2022). Global Cyber Governance in China: Towards Building a Community of Shared Future in Cyberspace. *Science, Technology and Society*, *27*(3), 456–475.

[74] Zhou, S., & Liu, Y. (2023). Effects of Perceived Privacy Risk and Disclosure Benefits on the Online Privacy Protection Behaviors among Chinese Teens. *Sustainability*, *15*(2), 1657. https://doi.org/10.3390/su15021657