E-ISSN : 2790-2404
P- ISSN 2070-9250
Qadaya siyasiyyat

Ministry of Higher Education
& Scientific Research
Al-Nahrain University
College of Political Science

وزارة التعليم العالي والبحث العلمي
جامعة النهرين
كلية العلوم السياسية

قضايا سياسية

Political Issues

مجلة فصلية محكمة

العدد ٨٤
Issue 84

كانون الثاني - شباط - اذار / ٢٠٢٦
Jan. - Feb. - Mar. / 2026

قضايا سياسية
العدد ٨٤
٢٠٢٦

جامعة النهرين
كلية العلوم السياسية

E-ISSN 2790-2404
P- ISSN 2070-9250
DOI prefix: 10.58298

قضايا سياسية
Political Issues

مجلة فصلية محكمة تعنى بنشر الأبحاث والدراسات السياسية العراقية والعربية والدولية
http://pissue.iq

مجلة قضايا سياسية

pissue.iq

قواعد النشر

- لغة المجلة هي اللغة العربية والانكليزية على أن يراعى الوضوح وسلامة النص.
- ترحب المجلة بنشر البحوث والدراسات السياسية النظرية والتطبيقية ولا سيما التي تجعل من قضايا المنطقة والعالم محط اهتمامها، ماضياً وحاضراً ومستقبلاً، وعلى وفق الآتي:

1. أن لا يزيد عدد صفحات البحث أو الدراسة عن (15) صفحة مطبوعة بحجم خط (14) والتباعد (1,15) ونوع الخط Simplified Arabic تقدم عبر المنصة الاليكترونية للمجلة على الرابط :
https://pissue.iq/index.php/pissue/about/submissions
2. أن تتصف البحوث والدراسات بالموضوعية والدقة العلمية.
3. أن تعتمد الترقيم العشري للعناوين الأساسية والفرعية او التنصيف المعياري العام.
4. يرفق مع كل بحث او دراسة ملخصين (احدهما باللغة العربية والآخر باللغة الانكليزية/ يتضمن اهداف البحث ، المنهج والمعالجة ، ابرز النتائج واهم الاستنتاجات والمقترحات) مع ضرورة مراعاة ان الملخص مختلف اختلافا جذريا عن المقدمة وليس تكرارا لها .
5. تخضع جميع البحوث المقبولة للنشر الى نظام الاستلال الالكتروني في كلية العلوم السياسية –جامعة النهرين.
6. يرفق مع كل بحث ودراسة سيرة ذاتية مختصرة للباحث وتعهد .

- تقوم المجلة بإخطار الباحثين بإجازة بحوثهم أو دراساتهم من عدمها بعد عرضها على محكمين تختارهم على نحو سري من بين أصحاب الاختصاص.

مجلة قضايا سياسية

pissue.iq

- يجوز للمجلة أن تطلب إجراء تعديلات شكلية أو شاملة على البحث أو الدراسة قبل إجازتها للنشر بما يتماشى مع أهدافها.
- البحوث المنشورة تعبر عن آراء أصحابها ، ولاتعبر عن راي المجلة .
- ترحب المجلة بالمناقشات الموضوعية لما ينشر فيها أو في غيرها من الدوريات وبأية ردود فكرية أو تصويب، وكذلك ترحب بنشر التقارير عن المؤتمرات والندوات ذات العلاقة ومراجعات الكتب وملخصات الرسائل الجامعية التي تتم إجازتها على أن تكون من إعداد أصحابها.

توجه جميع المراسلات إلى هيأة التحرير على العنوان الآتي
مجلة قضايا سياسية، كلية العلوم السياسية، جامعة النهرين-بغداد – الجادرية.
E.mail: pirj@nahrainuniv.edu.iq

الموقع الاليكتروني
https://pissue.iq/index.php/pissue

E-ISSN 2790-2404
P- ISSN 2070-9250
DOI prefix: 10.58298

Table of Contents

Ways to Combat Cyber Terrorism at the International Level: Iraq as a Case Study[▽]

Asst. Lecturer. Shahad Qasim Mohammed*

Abstract

The study points towards the growing problems like threat from cyber-terrorism and growing dependence on technology and how the new frontiers of interstate and terrorist group conflict are cyber-terrorism. The study attributes these trends to the rising threats to the global order, as the economic losses from cybercrime are likely to surpass $10 trillion by 2025. The report above is testimony to the dangers of terrorists abusing technology. The analysis identifies three main (but still limited) avenues through which international cooperation may play a role in addressing cyber-terrorism: the Budapest Convention (2001); the United Nations Comprehensive Convention on Cybercrime (2024); and the Interpol-European Union cooperation on information and security and technical support to that European Union. The study notes Iraq's activism within the international context and the establishment of international cyber security meetings and building international capacity. The author of this study argues that international cooperation needed to overcome the challenges of cyber-terrorism, such as a response of legislation with the level of legislation corresponding to the pace of technological development and the amount of control needed between the right to digital privacy and the right to secure cyberspace is the answer.

Keywords: Cyber-terrorism, Cyber-security, Global cooperation, Budapest Convention, Iraq.

Significance of the Research:

Anecdotal research found, however, that cyberterrorism is on its way to being one of the most menacing possible threats to a country's security, not least because of how rapidly these threats are appearing, how quickly that world is shifting to digital and how heavily countries are relying on digital systems. This research attempts to establish the relevance and significance of the various cross-national collaborative frameworks that serve countries through global organizations for the prevention of this type of terrorism, which continues to represent the largest global issue in transnational threat vectors. Furthermore, by examining Iraq's involvement in the international initiatives on cyberterrorism, this study

▽ تاريخ التقديم : 2026/ 2/3 تاريخ القبول: 21 /3/ 2026 تاريخ النشر: 31/3/ 2026

* كلية العلوم السياسية – جامعة النهرين shahadqasim@nahrainuniv.edu.iq
Al-Nahrain University – College of Political Science

highlights the need for theoretical and practical integration. This research supports policymakers and academics in developing end-to-end policies and frameworks related to digital security that advance national security and preserve civil liberties.

Research Objective:

The research examines cyberterrorism as an emerging problem, the focus of which is on international cooperation and Iraq's role - to be investigated. It also analyses the global legal, technical, and institutional structures that have been exploited as a framework for this challenge to address them at a global scale.

Research Problem.

The research problem: the lack of developed international legal and cooperative systems to meet the changing threat posed by cyberterrorism. The challenges that these frameworks face are legal, technical and related to coordination. Besides, this calls for a role of Iraq in such objectives.

Research Hypothesis:

The study explains that improving international cooperation and aligning legal as well as technical foundations will have a positive effect on efforts to combat cyber terrorism. Furthermore, international mechanisms would improve Iraq's capacity to respond to cyberterrorism, the research concludes.

Research Methodological Framework:

1. Descriptive Method: This method analyzes and defines the domain at face value the characteristic features, extent, and aspects, its significance for international security of the phenomenon of cyber terrorism.

2. The Analytical Method: This method is about to analyse legal basis from international perspective, international cooperation mechanisms and international organizational roles on the face of cyberterrorism.

3. The Comparative Method: This is used to compare some international experiences and policy approaches when tackling cyberterrorism, focusing on similarities, disparities, and lessons learned.

4. Case Study Method: This approach looks at Iraq's experience as it relates to an array of global initiatives to combat cyberterrorism, evaluating the principal complexities encountered and the scope for improvement in effective solutions.

Introduction

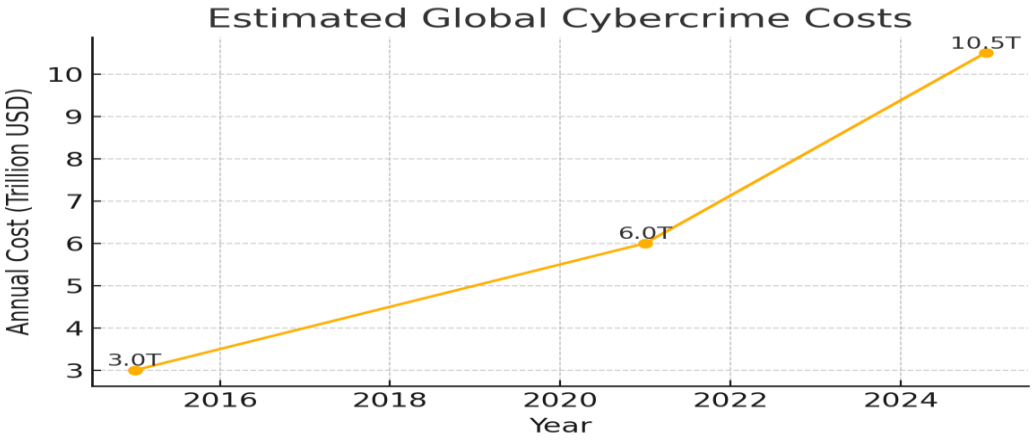
Cyberterrorism threat has been on the rise in the past 10 years, and terrorist organizations have a greater desire to conduct their operations in cyberspace to promote their interests and disseminate their message. The proliferation of digital

platforms and the access of critical infrastructure to information networks has spawned a new space for states to meet and struggle against terrorist organizations. Terrorism is becoming a threat that is becoming increasingly complicated; it has moved beyond military and security measures only to encompass cyber-attacks against critical infrastructure or sensitive information in an attempt to sow panic and accomplish political or ideological objectives across a variety of activities, both within the military and security sectors. These new developments have led states and international institutions to make concerted efforts to create new legal, technical and political frameworks to tackle this emerging trend. They refer to arrangements like international conventions and cross-border security collaboration. The research works towards international approaches to counter cyber terrorism. It emphasizes on the most significant legal, technical and political tools applied in the fight against cyber terrorism. So, it comes down to collective international cooperation, the Budapest Convention, the United Nations Security Council and Counter-Terrorism Office, Interpol and the European Union. Furthermore, it would cover the Republic of Iraq's role in combatting cybercrime within the perspective of international cooperation.

The First Axis:
The Magnitude of Cyberterrorism

In the last ten years, cyber threats have skyrocketed globally in terms of number of attackers, severity and economic impact. Recent international sources suggest that there have been unprecedented quantum leaps in cybercrime and attacks worldwide. This led to the alarm of groups seeking to exploit this fact in order to wage vicious remote strikes. Studies and reports from the World Economic Forum suggest the total annual cost of cybercrime has risen from about $3 trillion in 2015 to approximately $6 trillion in 2021 and, Studies projected that the annual global cost of cybercrime would reach approximately USD 10.5 trillion by 2025, reflecting the rapid escalation of digital threats worldwide. For malicious digital activity, the increase represents what has been called and officially the "largest transfer of economic wealth in history", not to mention the massive "transfer of assets in human history." These huge economic losses illustrate the global scope of attacks and the deepening dependence of societies on digitalization worldwide and the inability to fully prevent these kinds of breaches until there is less and less control over them.

Figure 1 shows the estimated increase in the annual global cost of cybercrime from 2015 to 2025 in trillions of US dollars.



Such growing scale of the global cyber threat gives rise to increasing economic losses associated with cyberattacks, and the above curve displays this situation. The deteriorating cyber threat was acknowledged by the World Economic Forum (WEF) in its report, "Global Cybersecurity Outlook 2023." World leaders on business and cybersecurity expect a severe cross-border cyber incident to hit within the next two years owing to geopolitical tensions, 91% of them told Reuters. The Forum's Global Risks Report 2023 shows that cybercrime and cybersecurity insecurity is one of the top 10 global risks according to the severity anticipated. Such fears are confirmed by the Forum's statistical data. On average, the world faces more than 2,200 cyberattacks of different kinds daily (over 800,000 attacks in 2023). The information they offer reveals a context ripe for terror organizations to exploit as such a gap between what states technically know and what attackers can do gets ever-deeper as already on the dark web, a number of ready-to-eat hacking tools simply can be found and sold. Intelligence reports show that the use of advanced hacking by terrorist organizations is somewhat limited notwithstanding the general rise of cyber threats. However, there are still significant international worries regarding the potential for terrorist groups to find technical support from rogue states or sophisticated hacking groups, which may help them to do more destructive attacks. In fact, under Security Council discussions, the United Nations warned that terrorists could be increasingly tech-savvy and a co-ordinated global response to counter "technologically savvy terrorists" would be needed. This calls for international cooperation mechanisms capable of addressing any qualitative advancements in cyberterrorism capabilities in the early response, which we will cover in the next section.

Second Axis:
Cyberterrorism-related International Cooperatives

Acknowledging that countering the threat of cyberterrorism demands a holistic, multilateral response, states and the global community have formulated international legal frameworks, security and technical cooperation, as well as political and diplomatic initiatives. So, we have devised several initiatives and settlements that would augment the collective effort against cyberattacks, mostly as terrorist events. States and organizations are implementing the following prominent international cooperation mechanisms:

1st, global legal frameworks and legislation

The foundation for legal cooperation in combating cybercrime and cyberterrorism lies in the international treaties and agreements. Amongst them:

The Budapest Convention on Cybercrime (2001)

It is the most substantial international legal framework for cooperation in cyber investigation. It permits the alignment of definitions of cybercrime within national law and the exchange of information and electronic evidence between states that have ratified it. While the deal was launched by the Council of Europe; it is available to countries other than Europe. The number of parties to the convention, through the end of 2023, had climbed slowly to around 69 countries (with the United States, Japan, and Latin American countries among the others). The Budapest Convention provides important tools for tracking cybercriminals and terrorists, such as urgent mutual legal assistance mechanisms to preserve communications data and track the origin of international attacks. Several international organizations have urged countries which have not yet joined to quickly adopt the convention, or at minimum reconcile their own laws with it, to ensure that legal loopholes exploited by cross-border attackers are blocked. (Kralik, 2023, p. 3).

The United Nations has developed a worldwide legal framework in parallel with the Budapest Convention. In conclusion and summary of the discussion, the General Assembly adopted the Comprehensive International Convention on Cybercrime by unanimous vote on December 14, 2024, which was the first global treaty. The agreement seeks to bolster international collaboration in the fight against cybercrimes, from cyberterrorist attacks to the sharing of electronic evidence in criminal trials. In 2025, the high-level conference will open the agreement for signatures at Hanoi, Vietnam. It will then come into force once 40 countries have ratified it. The Budapest Convention — which some major countries did not sign: Russia and China — will serve to fill the void after major

nations largely chose not to participate in the talks that were held at the UN, and the agreement. At the same time some Western countries expressed concern over the text of The Convention in question — most notably over internet freedom and human rights. For all the difference this is for another party, still, adoption represents a significant step to provide a unified global legal structure for handling the problem of cybercrime. (Kralik, 2023, p. 5).

Alongside international agreements, many countries have adopted national laws that explicitly criminalize cyberterrorism or broaden the scope of traditional anti-terrorism legislation to encompass computer-related crimes. Several countries have also passed legislation to protect critical information infrastructure, imposing strict security standards on digital service providers to prevent or detect breaches early on.

Table 1: National Legislation of Countries

Country	Legislation/Policy	Notes
United States	**Patriot Act 2001** **Law to strengthen the fight against terrorism in the United States** **Cybersecurity Act 2015** **Cybersecurity law**	Expanded the definition of terrorism to include cyberattacks and imposed an obligation on companies to report breaches.
Germany	**IT-Sicherheitsgesetz Information Technology Security Act**	Critical infrastructure (such as hospitals and energy) is required to adhere strictly to cybersecurity.
France	**Loi de Programmation Militaire Military Programming Law**	It strengthens Internet surveillance and gives the state powers to block websites with terrorist content.
China	**(Cybersecurity Law – 2017)**	It requires local and foreign companies to store data locally and ensure its security, and criminalizes terrorist activities online.
Russia	**Yarovaya Law (2016)**	It obliges telecommunications service providers to store data and make it available to national security agencies and

		strengthens the fight against "cyber extremism."
Iraq	**Under development – but there are draft cybercrime laws (2021 and 2023)**	It includes provisions against the use of the internet for terrorism, recruitment, and incitement to violence, and there is ongoing debate about human rights safeguards.

Second: International Security and Technical Cooperation

Countries realized that legal measures alone were insufficient, so they created platforms and tools for field security cooperation and the near-instantaneous exchange of information on cyber threats. INTERPOL (the International Criminal Police Organization) plays a vital role in this regard by coordinating law enforcement agencies in 195 countries. In recent years, INTERPOL has enhanced its ability to combat cybercrime by establishing a Cybercrime Center. This center includes digital forensic laboratories, rapid response teams for major cyber incidents, and a platform for sharing intelligence between member states.

1. INTERPOL efforts

A. Launching joint international operations targeting criminal piracy networks INTERPOL led Operation Synergia in 2023, in which security agencies from dozens of countries participated to counter growing cyber threats. The operation succeeded in dismantling the infrastructure and malicious software used by criminal and terrorist groups. (INTERPOL, 2024).

B. In August 2023, INTERPOL joined the international Combating Ransomware Initiative (CRI), a U.S.-led coalition of more than 30 countries and organizations (including the European Union), which aims to share expertise and best practices to disrupt ransomware gangs that may be exploited by terrorist groups to raise funds or cause chaos. (INTERPOL, 2023, p. 12).

C. INTERPOL's global network makes the I-24/7 secure communications system available to facilitate the exchange of alerts on current cyber threats between countries. When a country detects an attempted terrorist or international sabotage attack, it can use Interpol to circulate a warning bulletin (e.g., the Violet Alert bulletin on new criminal methods) to alert other members. (INTERPOL, 2023, p. 15).

D. INTERPOL experts regularly issue analytical reports on the latest tactics used by hacking and cyberterrorism groups. These reports help less experienced countries improve their preparedness.

E. INTERPOL plays a role in training police officers around the world on how to investigate cybercrimes related to terrorism through capacity-building programs in collaboration with organizations such as the United Nations and the European Union.

Crucially the UN Security Council has commended international security organization INTERPOL in its resolutions. For instance, Security Council Resolution 2341 (2017) on the protection of infrastructure against terrorism emphasizes the necessity of working together with INTERPOL to exchange information about cyberattack plans targeting critical infrastructure. Several jurisdictions, besides INTERPOL itself, have developed direct networks of cooperation on technical measures in security monitoring of cyberattacks and in malware analysis for terrorist groups or states that sponsor terrorism. Most notably:

(1) The European Union has activated a cross-border "Cyber Emergency Response Team" (CERT) mechanism whereby a response team in one country can request immediate assistance from its counterpart in another country when faced with a large-scale cyberattack; and (2) a meeting of experts within the framework of the CERT Network, sponsored by entities such as the International Telecommunication Union (ITU), to exchange early warnings about viruses or vulnerabilities that could be exploited by terrorists.

(2) Experts meet within the CERT Network framework, sponsored by entities such as the International Telecommunication Union (ITU), to exchange early warnings about viruses or vulnerabilities that could be exploited by terrorists. (International Telecommunication Union, 2023, p. 17).

Between 2015 and 2025, several international simulations of major cyberattacks were conducted, such as the Cyber Storm series led by the U.S. Department of Homeland Security and the Cyber Europe exercises led by the European Agency ENISA, to test countries' readiness and coordinate their responses to scenarios involving digital terrorist attacks. These exercises improved communication between countries during cyber crises and identified weaknesses that needed to be addressed.

Third: Political and Diplomatic Efforts at a Collective Level

Cyberterrorism has been designated a priority in international political decision-making on the global stage. The most notable example is:

1. United Nations Security Council

It includes prevention of terrorist use of the internet in the Security Council's counterterrorism efforts. Several resolutions recognize this approach. (United Nations Office of Counter-Terrorism, 2025).

A. Resolution 2354 (2017), which laid down an international framework to address terrorist rhetoric and extremist propaganda on the internet. This resolution highlights the need for states to work with technology companies to rapidly eliminate terrorist content.

B. Resolution 2396 (2017), which also calls on states to build their capabilities to monitor and prevent the use of technology to facilitate terrorist travel, which includes enhancing travel document and border information system security.

C. More broadly, the UN General Assembly adopted amendments to the Global Counter-Terrorism Strategy (notably in the 2016 and 2018 revisions) that refer to the importance of preventing terrorists from exploiting information and communications technology for their purposes.

D. In 2018, the UN Secretary-General established a Technology Task Force within the Office of Counterterrorism (UNOCT) to explore ways to counter emerging threats in the digital space. This resulted in cooperation programs with social media companies to monitor terrorist propaganda accounts and initiatives to educate young people about the dangers of online extremist recruitment.

2. European Union

Over the last 20 years, European cooperation in the battle against terrorism has made extraordinary advances. It bolstered the capability of the Member States to safeguard the security and safety of their citizens. The EU databases strengthen cooperation between police and judicial institutions of EU countries, linking border points, and ensuring that terrorists do not travel around the countries for terrorist reasons. In July 2020, these efforts culminated in the following: (United Nations Security Council Counter-Terrorism Committee Executive Directorate, 2023, p. 31).

A. The European Commission adopted a new strategy for the EU Security Union (2020-2025). This ensures that threats are mitigated and detected in time, critical infrastructure is strengthened, cybersecurity is improved, and research and innovation are put into practice. This strategy took effect in April 2021 after the European Parliament passed stricter rules that put a one-hour deadline

on online platforms to eliminate terrorist material. The goals of these regulations are to dissuade terrorists from taking advantage of the internet for radicalization, recruitment, and inciting terrorism.

B. The Commission urged the adoption of the EU Code of Conduct on Countering Online Hate Speech in 2016 and launched an initiative to broaden the EU-based crimes list to cover hate crimes.

C. The EU has instituted significant collective policies. The EU supported the Budapest Convention and participated actively in the negotiations of the UN Convention. Similarly, the EU adopted the EU Cybersecurity Strategy (2020) which intends to better prepare European cyberspace for attacks.

D. It also issued the European Counter-Terrorism Directive (2017), obliging member states to criminalize acts such as carrying out or inciting serious cyberattacks for terrorist purposes online.

E. The EU has established coordination platforms, such as Europol's European Cybercrime Center (EC3) in The Hague. The EC3 works with the European Counter Terrorism Center (ECTC) to exchange information on intersections between cyber investigations and terrorism cases.

F. One of the achievements of this joint European cooperation is that, during joint European operations such as Operation Eye of Horus, which targeted ISIS's media infrastructure on the dark web, Europol has dismantled several propaganda media platforms belonging to ISIS and Al-Qaeda terrorist groups online.

G. In 2021, the EU launched the "Online Terrorist Content Contact Center" to enhance cooperation with major technology companies and quickly remove terrorist content in accordance with the EU law preventing the dissemination of terrorist content online.

3. African Union

The African Union adopted the Convention on Cyberspace Security and Personal Data Protection in 2014. However, the convention has not yet gone into effect because the number of signatory states has not reached the required minimum. Ten additional states need to sign the convention, as only 19 of the 54 states have signed it so far. The lack of interest among African countries in signing this agreement may be due to a lack of awareness of cybercrime's severity, considering the low level of internet usage in Africa. Only 28% of Africans used the internet at the end of 2019. (Salama, 2022, p. 29).

4. International actors

Several international groups have formed forums dedicated to cybersecurity and combating cyberterrorism, the most important of which are:

A. The Global Counterterrorism Forum (GCTF), which discussed the issue of terrorists' exploitation of technology at its meetings and issued recommendations to strengthen the legal capabilities of states.

B. The Group of Seven (G7), which launched an initiative in 2017 to pressure technology companies to remove terrorist content within two hours of its publication.

C. The 2019 Christchurch Call, led by New Zealand and France, emerged as a collaboration between governments and technology companies to prevent terrorists from exploiting live streaming and social media during violent terrorist attacks (this came after the Christchurch terrorist attack was broadcast live online).

Although these initiatives focus more on terrorist content, they are complementary to efforts to counter cyberterrorism in general, because combating cyberattacks and digital extremism are two sides of the same coin in the overall strategy to combat modern terrorism.

The following table illustrates some of the most important international cooperative frameworks, legal and security—adopted by states to combat cyber terrorism and cybercrime during the period under review:

Table 2: Major international agreements and initiatives to combat cyberterrorism

International agreement/initiative	Year	Participating parties	Description and main objective
Budapest Convention on Cybercrime (Council of Europe)	**2001**	69 countries (European, Asian, American, and others) by 2023	The first international treaty to establish a unified legal framework for cybercrime and promote judicial cooperation and the exchange of electronic evidence between countries. It is also used to deal with cybercrimes related to terrorism.
Interpol Cybercrime Center	**2015–present**	195 countries (INTERPOL members combating cybercrime)	Provides a global platform for sharing alerts and information on cyber threats Supports joint cross-border operations and provides training and technical assistance to countries investigating terrorism

European Cybersecurity Strategy (European Union)	**2020**	27 Member States of the European Union	A comprehensive strategy to strengthen Europe's cyber immunity, including the development of cyber defense capabilities and infrastructure protection. The strategy also supports the EU's efforts to combat the exploitation of the internet by terrorists, through laws such as the regulation of terrorist content on digital platforms.
Counter Ransomware Initiative	**2021**	36 countries + European Union + Interpol accession (2023)	A multilateral coalition launched by the United States to coordinate international efforts against ransomware attacks, which cripple systems and are sometimes used for extortion to finance terrorism, members share intelligence and best defensive practices.
Bilateral cooperation (US-EU cyber dialogue)	**2021**	The United States and the European Union	As an example of bilateral/multilateral cooperation for cyber policy coordination, both sides launched a joint council to deepen information sharing on cyber threats and enhance joint response to attacks, including those carried out by terrorist actors.
International Convention on Cybercrime (United Nations)	**2024**	Adopted by the General Assembly (available to all Member States)	The first comprehensive global treaty to combat cybercrime and strengthen international cooperation in preventing and prosecuting online crimes facilitates the extradition of criminals and the exchange of digital evidence between countries, and is scheduled to open for signature in 2025.
Establishment of the new cyber defense center	**2024**	North Atlantic Treaty Organization (NATO)	The center aims to promote cooperation between military, civilian, and industrial experts to counter growing cyber threats, particularly those related to hybrid attacks.

The Third Axis:
Iraq's Role in Countering Cyber Terrorism

The Republic of Iraq is one of the countries that has directly suffered from terrorism over the past two decades, particularly at the hands of ISIS and other extremist organizations. While confronting these organizations militarily and security-wise, the Iraqi state realized the need to counter the cyber front terrorists exploited to spread propaganda and coordinate activities. Despite political and technical challenges, Iraq has taken significant steps to bolster its cybersecurity

capabilities and actively participates in international efforts to combat cyberterrorism.

Internationally, Iraq has engaged with cooperation structures to combat cyberterrorism and has benefited from them. The country has acceded to several relevant conventions and actively participated in discussions on drafting the new UN Convention on Cybercrime. Within the United Nations framework, Baghdad has supported the United Nations Office of Counter-Terrorism's (UNOCT) efforts to strengthen states' capabilities to counter terrorist use of the internet. The country has provided financial and logistical contributions to support United Nations training programs in this field and has hosted a high-level international conference on counterterrorism and cybersecurity.

1. International Conference on Cybersecurity and Counterterrorism

In September 2021, Baghdad hosted the first International Conference on Cybersecurity and Counterterrorism, with delegations from 55 Arab and foreign countries and more than 15 specialized companies participating. The conference aimed to exchange experiences with leading countries and companies in cybersecurity technologies and review best practices in protecting institutions from cyberterrorist attacks. This conference was a milestone in Iraq's quest to become an international platform for discussion on cybersecurity. Iraq benefited from its outcomes in developing bilateral relations with advanced countries in this field, most notably the signing of memoranda of understanding for cyber cooperation with European and Asian countries. (Ibrahim, 2021).

Iraq has also cooperated closely with INTERPOL and other international law enforcement agencies. The Iraqi police force uses the INTERPOL system to track individuals wanted for cyberterrorism and to notify them of cyberattacks targeting Iraqi infrastructure. Any international report of a planned cyberattack on the oil or banking sectors in the region is immediately circulated to INTERPOL and then to Iraq, allowing them to take precautions.

Iraq has also sought to benefit from international police training programs. With support from the United Nations and INTERPOL, Baghdad has sent security experts to advanced workshops on digital forensic investigation and tracking terrorist financing via the Internet.

Iraq is cooperating with NATO, which has a training mission in the country. Countering cyber threats is included in Iraqi capacity-building programs, and the Iraqi government has discussed ways to strengthen the security of Iraqi military and government networks against breaches with NATO mission leaders. During a meeting held in 2025 between the Iraqi prime minister and NATO officials, it

was confirmed that Iraq would continue to implement its national cybersecurity strategy and develop the necessary infrastructure while welcoming advisory and technical support from the alliance. On April 22, 2025, as part of the 13th edition of the Security, Defense, and Military Industries Exhibition (IQDEX 13), Baghdad hosted a cybersecurity conference under the supervision of the Iraq Computer Emergency Response Team (Iraq-CERT), in cooperation with the United Company for Exhibitions and Conferences. Attendees of the conference were more than 155 companies from 24 countries (including the United States, France, China, and Russia) and Iraqi companies focused on information technology. This shows Iraq's increasing national capabilities in cybersecurity. Iraqi universities such as Al-Mustaqbal University added to the academic aspect of the conference by supporting the integration of the scientific and technical sectors to enhance national cybersecurity. Such a conference represented as part of the establishment on the way to enhancing the cybersecurity of Iraq, and its findings will be able to shape a few effective plans to deal with the forthcoming digital risks. Its most important objectives are: (Asharq Al-Awsat, 2025).

A. Boosting national cybersecurity: By addressing challenges and opportunities in cybersecurity and reviewing the latest solutions and technologies for safeguarding critical electronic infrastructure.

B. Sharing international experiences: The conference brought together a group of international speakers and experts from leading global institutions and companies in the field of cybersecurity, providing an opportunity to exchange knowledge and experiences.

Despite the progress made thus far, Iraq still faces a significant challenge in developing robust cybersecurity capabilities. Experts point out that Iraq is in the early stages and needs to invest more in technical infrastructure and regulatory frameworks to strengthen its cyber resilience. However, it is clear that the Iraqi government is taking this vital area seriously, as it has begun to address gaps in strategy, legislation, and international cooperation to become an active part of the global system for combating cyberterrorism. With continued international support, Iraq is expected to steadily progress in protecting its digital space from terrorist exploitation.

Conclusion

There has been considerable progress made in the international community in shaping unified action when it comes to cyber terrorism. With a real understanding of the magnitude of the dangers of lethal cyberattacks, countries have allied actions, signed agreements and created cooperation and sharing of know-how mechanisms. Most notably, changes in international law such as the Budapest Convention and its protocols, the UN Convention, as well as strengthening the capacity of organizations including Interpol, Europol and the United Nations to attack cybercrime related to terrorism. Awareness has also been spurred by technical advances and geopolitical shifts. The increase in ransomware attacks, attacks on digital supply chains and state-sponsored attacks have also stimulated an overall strengthening of cybersecurity efforts, which are also advantageous to the battle against cyberterrorism because common tools are at work. Still, the world has complicated obstacles to address in this regard. Among these challenges are the challenge of tracing perpetrators across borders, the considerable gap between countries' capabilities in cyberspace, and the tension at the intersection of security concerns with privacy rights and freedoms in cyberspace. However, the success of neutralizing a substantial number of terrorist propaganda structures online and preventing infrastructure hacking schemes shows that close international cooperation can indeed work. Hence vigilance, contingency planning, and periodic refresh of counter-measures will be vital. Because technology is developing rapidly and will continue changing to be a variable factor, the counter-cyberterrorism system needs to be dynamic and proactive. This is so we can make sure all those responsible for using it for terrorism and extremism don't misuse our digital space in doing so.

References

1. Asharq Al-Awsat. (2025). Iraq-NATO talks on fighting terrorism and cyber threat. April 14, 2025.
2. Ibrahim, W. (2021). Iraq hosts first international conference on cybersecurity and counter-terrorism. Al-Jazeera, September 15, 2021.
3. INTERPOL. (2023). INTERPOL annual report 2023. Lyon: INTERPOL.
4. INTERPOL. (2023). INTERPOL's submission to the 2023 High-Level Political Forum on Sustainable Development. Lyon: INTERPOL.
5. INTERPOL. (2024). INTERPOL-led operation targets growing cyber threats. February 1, 2024.

6. International Telecommunication Union. (2023). ITU contribution to the 2023 High-Level Political Forum on Sustainable Development. Geneva: ITU.
7. Kralik, J. (2023). Budapest Convention on Cybercrime: Content, impact, benefits, and process of accession. PGA Regional Caribbean Workshop, Port of Spain, Trinidad and Tobago, July 5–6, 2023. Council of Europe.
8. Salama, M. (2022). International and regional organizations in the fight against cyber terrorism. International Politics Magazine, 1(227), 29.
9. United Nations Office of Counter-Terrorism. (2025). Cybersecurity and new technologies. Retrieved May 3, 2025, from https://www.un.org/counterterrorism/ar/cybersecurity
10. United Nations Security Council Counter-Terrorism Committee Executive Directorate. (2023). CTED factsheet – April 2023. New York: United Nations.