

Qatar's Efforts in Combating Cyberterrorism

Professor Dr. Diab M. Al-Badayneh^{1*}, Abdullah Mohammad Al-Sulaiti²

¹Ph.D. Methodology, Criminology, & Security Studies

²MA Student, Department of Security Studies, Graduate College, Police Academy, MOI

DOI: <https://doi.org/10.36348/sijlcj.2026.v09i06.006>

| Received: 17.03.2026 | Accepted: 05.05.2026 | Published: 08.06.2026

*Corresponding author: Professor Dr. Diab M. Al-Badayneh
Ph.D. Methodology, Criminology, & Security Studies

Abstract

This study investigates the state of Qatar in its cyberterrorism-combating endeavors. The research tool designed was a questionnaire. A convenience sample (N = 200) was used, and the majority of participants were older than 35 years old (70.0%): Males and females comprised 80.5% and 19.5%, respectively. The study findings showed that more people identified cyberterrorism as a real threat to national security. Exploring the Qatari youth view on institutional capacities, legal frameworks, and education/community programs. Along with this, the results also show that Qatari institutions are deemed reliable in addressing cyberterrorism, as 89.5% place belief and capability on these institutions. One of the main findings is that an alarming 96.0% agree that decreasing awareness on digital platforms decreases extremist behavior reporting. All respondents agreed that legislation and cooperation at the regional level were required, while fewer supported educating youngsters as an appropriate strategy against digital radicalization. To sum up, the study provides insights into areas to improve upon when it comes to education programs and policy initiatives in preventing cybersecurity threats.

Keywords: Cyberterrorism; combating cyberterrorism; cybersecurity; Qatari youth; Qatar.

Copyright © 2026 The Author(s): This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY-NC 4.0) which permits unrestricted use, distribution, and reproduction in any medium for non-commercial use provided the original author and source are credited.

INTRODUCTION

Cyberterrorism has pushed numerous nations worldwide to end up being threatened in cyberspace. As one of future threats against public security and harmony in a social setting. Cyberterrorism becomes more acquainted with systems for lifelines in an expanding computerized world. Recognizing that cyberterrorism presented an innovative danger, the State of Qatar has also invested heavily in efforts to address these issues. Cyberterrorism is the term used to describe acts that target computer systems/networks in a manner directly affecting state security, committing violence, or destroying critical infrastructure (Weimann 2021(2006), Denning 2011). In parallel, the increasing dependence on digital infrastructure has also resulted in an increased vulnerability of critical sectors—energy, transportation, and communications—to hostile cyberattacks (Kornish, 2009).

Qatar's national vision makes it necessary to intervene in cybersecurity-related matters within the scope of bigger transformational targets towards 2030 over the long run (State of Qatar, General Secretariat for Planning and Statistics, 2008). The country foils cybersecurity threats through legislative frameworks, community audiences, and international cooperation.

Prior research confirms awareness and education provide individuals with tools to recognize and defend themselves regarding the cyber threats, alongside robust legislation as well as institutional accountability (Al-Ali 2022; Al-Jabri 2021; Dunaway & Macharia 2021).

Equally important is what the public witnesses about the successes of these initiatives. Studies have suggested that institutional trust is a key factor driving the extent of non-compliance in any population with respect to cybersecurity (McCarthy, 2023). This realization leads to the present study, which explores Qatari citizens' knowledge of and attitude toward cyberterrorism while also examining the effects of awareness, citizenship identity and sense of belongingness, and perceived cybersecurity measures on their perception. Investigating this is critical to discern the mechanisms of how a national security strategy utilized in conjunction with civic engagement can enable policy implementation and behavioral outcomes through institutional architecture while fostering an empowered populace.

Instead of discrete technical penetrations, cyberterrorism is a framework for modes of terrorizing societies or modifying state behavior by means of specific cyberspace abuses aimed at debilitating critical

infrastructure/resources or supporting conventional terrorism and procurement operations with funds, advertising channeling, and hiring (Weimann 2006; Denning 2011). As states become more reliant on digital services, government platforms, and the data-driven economy (Kornish 2009), so too does the potential for targeted or widespread attacks on critical infrastructures (energy, transportation, communications, finance, and health).

The Qatari case is especially relevant within the context of the peculiarities of a national vision to spur transformation and development through 2030 (State of Qatar, General Secretariat for Planning and Statistics, 2008) as well as increasingly cyberthreat regions rising border security issues. Hence, this article seeks to examine the characteristics of Qatari public policy in combatting cyberterrorism by summarizing both its institutional and legislative evolution as well as to analyze 2024–2030 national cybersecurity policy trends and indicators of Qatari presence among several international cooperation frameworks with relevance to counterterrorism.

In the literature, cyberterrorism is defined as “the use of computer systems and networks to impose terror on a state or an entire community for political/ideological/religious motives through actions that disrupt any vital services, threaten public safety, or digitally support traditional terrorism” (Weimann 2021; Weimann 2006; Kornish 2009). At this stage a distinction has to be made between (a) cybercrime that, even if it is profit-oriented or will inflict harm on the individual concerned, is circumstantial but not politically/terrorism-seeking; (b) terrorism-related cybercrime that is intended to coerce some kind of behavior or affect and then shape much public decision-making; and (c) terrorism support in cyberspace, propaganda, recruiting, funding, and instruction exchange area, which lies where restrictions governing cybercrimes extend over into counter-terrorism as well as financing legislation laws regulating Al-Badayneh (2024a).

PROBLEM OF THE STUDY

Young people who are increasingly exposed to extremist material turn to violence. There is also ignorance of the risk of extremism and cyberterrorism; studies show that young people need better education and digital awareness to face such phenomena. Evidence suggests that social and cultural factors, such as alienation, isolation, and exclusion, are persistent drivers of extremism because they [underpin] a more conducive background for violent ideologies. Moreover, there is widespread apprehension of embedding counter-extremism-related topics into the syllabi in schools and universities that also play a significant part in hampering young people from digesting and assessing extremist material (Al-Badayneh, 2024a, b). Finally, and perhaps most importantly of all, tackling terrorism where it shows

up also requires government will—to adjust to a slower cadence this go-around. These challenges give reason for the ignored need for a more rigid and balanced reaction in Qatar as violent extremism and cyberterrorism are becoming an exacerbating, so-called national security factor. This research is derived from a question: What are the State of Qatar's efforts in combating cyberterrorism?

PREVIOUS STUDIES

The State of Qatar has made enormous progress in the past few years to face the challenges pertaining to cyberterrorism.

Awareness and Education Initiatives

The impact of an awareness program on improving cyber risk knowledge among youth in Qatar. The pre- and post-test knowledge was increased in a statistically significant way. The research emphasizes the need for age-group-based education interventions that raise awareness to prevent severe cyberactivity (Al-Ali, 2022). Similarly, Dunaway and Macharia (2021) highlighted specifics related to digital citizenship through youth participation in digital literacy as a mechanism that deterred negative online behaviors and made the web safer. The implications of their research further corroborate the belief that education drives awareness because tackling cyberterrorism and nurturing informed, active digital citizens does not begin and end with self-contained media campaigns.

Legislative Framework and Institutional Capacity

Al-Jabri (2021) explored the extent national legislation could be beneficial for cybersecurity in the case of Qatar. The study also revealed that even though legislation has emerged worldwide as one of the bright spots in national efforts against cyber threats, many times both these laws' application and how they are modeled vary from region to region or at all. This supports the research carried out by Al-Kaabi (2023) on studying advanced technologies in artificial intelligence for cybersecurity analysis. In his research, Al-Kaabi demonstrates how these technologies facilitate data analysis and threat detection, allowing Qatar to deal with cyber threats that are evolving with the recent technological advancements. Al-Fazari (2022) similarly stresses the need for comprehensive and solid institutional foundations upon which cooperation between national and international partners is essential to tackle cyber terrorism. He showed that cooperation between the Gulf states not only worked but also built assets greater than the sum of individual nations.

Community Resilience and Societal Engagement

Al-Salem (2025) tells of the community programs' role in boosting the community resilience against cyber-attacks. The study demonstrated that grassroots capabilities extended beyond cognitive extension (which is present) to the ability of the community to get involved and push back against harmful material circulating on digital platforms. Such

results conform with those by Al-Hajri (2023) stating that the role of social media in disseminating extremist ideology is complex and citizens struggle to differentiate between credible content and harmful misinformation. Al-Salem (2021) modified his research to the psychological dimensions of extremism, determining whom cyberterrorism impacts and its luring techniques (mentally and socially). Because alienation and ignorance were important factors in the acceptance of violent ideologies, the researchers called for better forms of education and community support.

Regulatory agents and organizations that fulfill the function of a custodian to trust

These studies again underscore the importance of public trust in Qatari institutions as one of the main enablers to confront and fight cyber threats. According to McCarthy (2023), trust increased compliance with security measures and reporting suspicious activities. Al-Badayneh (2024d) also established that screening is increasing towards radical content, but this might worsen acceptance rates in violent ideologies unless remedied. In summary, the literature reviewed above provides evidence that studies Doha to become a national and international campaigner on countering cyberterrorism. The narratives captured in these studies hint at a comprehensive response, including education, galvanizing community action, legislation, and cross-national cooperation. Nonetheless, there are still research lacunae concerning the impact of such measures on representative populations and how/when youth become radicalized in different regions.

GENERAL RESEARCH GAP

Although Qatar has made some progress, much of which the Emir of Qatar himself has highlighted as needing addressing more specifically, there remain significant gaps in countering cyberterrorism. Identifies significant problems with victimization research (e.g., the scarcity of reliable empirical work leading to poor action response—through legal and legislative measures—and little public awareness more generally

about risk factors for cyber threats). Inadequate coordination between governments undermines fast response capacity, while new high-end capabilities such as artificial intelligence and big data to enable better surveillance for early warning should be put in place instead. International cooperation is needed due to some of these challenges that know no borders; we need far more investigation, since interpretation of the social roots of extremism is not yet very satisfactory. Lastly, the measures for impact assessment that are appropriate to judge counter-cyberterrorism need more complexity with a wider approach.

METHODOLOGY

The study used a survey using an electronic questionnaire sent to convenient (200) Qatari youth. The tool comprised demographic questions and axes concerning knowledge and fear of the implications of cyberterrorism; exposure to violent/hateful content; attitudes toward counter-extremist policies; trust in institutions; and state variables (including institutions' capacity, effectiveness of the legislative apparatus, and Gulf cooperation regarding combatting cyberterrorism as well as raising awareness/education).

FINDINGS

Trust in Qatari Institutions and Their Ability to Combat Cyberterrorism

Results related to "state efforts" (Table 1) demonstrate significant increased confidence of the ability of Qatari institutions to combat cyberterrorism, with 179 participants (89.5%) indicating that they believe that Qatari institutions have the capacity to deal with it. This indicator indicates a social acceptance of the policies and measures of the state in cyberspace and reinforces the hypothesis that institutional confidence has an important role to play in contributing to greater compliance with preventive measures (adherence) and instrumentalizing cooperation for longer-term goal achievement by reporting harmful digital practices emerging among users.

Table 1: State Efforts in Combating Cyberterrorism (Responses of "Yes")

Item	#	%
Qatari institutions are capable of confronting cyberterrorism	179	89.5
Digital awareness reduces the risks of extremism.	192	96.0
Qatar has necessary legislation to monitor extremist content	175	87.5
There is cooperation among Gulf countries to combat cyberterrorism	174	87.0
Education is the foundation for digital extremism.	122	61.0
Community programs contribute to enhancing societal resilience	187	93.5

In conclusion, this wide-reaching consensus reflects their belief that institutional approaches for combating cyberterrorism and extremism, legal-reform strategies concerning technological tools and digital opportunities in local communities, and usage awareness can tackle the issues at hand. While health services are encouraged, education and community programs should be included as well, but the key is continuing to maintain

good public faith in government capacity. Conversely, the dismal recognition of education as a factor for resisting digital radicalism suggests potential areas for improvement. Education programs need to improve overall as well so that the youth have skills specifically tailored to allowing them to navigate cyberspace and extremist ideas successfully—making Qatar's battle with cyberterrorism much easier. These results as well carry

significant implications that could guide policymakers to design targeted optimization of existing systems around

investments in education resources and community engagement approaches as components.

Table 2: Level of Awareness of Study Sample Regarding the Concept of Cyber Terrorism

Cyber Terrorism	Count	%
Knowledge of the concept of cyber terrorism	157	78.5
Cyberterrorism poses a significant threat to national security	187	93.5
Heard about cyber attacks	187	93.5

The awareness of cyberterrorism was significantly high: 123 of 157 (78.5%) respondents stated that they have heard the term before. However, this is still an enormous awareness gap, with almost 21.5% still not aware of it. Cyber terrorism is now surprisingly considered a serious national security threat by 93.5% of the respondents, which more or less translates into public hysteria and even a valid reason as a pretext for preventive measures. Furthermore, 93.5% have knowledge about cyberattacks, which also points to sound awareness in the community. These results lend themselves to public messaging but also strongly support the need for education efforts with certain at-risk groups.

Well, here is the beauty of awareness that brings both government initiatives and more funds for cybersecurity and education programs—our countries will consist of thousands of well-informed citizens against any trouble with digital safety.

In conclusion, the results indicate that there tends to be a necessity for government and educational institutions working together in dealing with cyberterrorism, creating an understanding of it between the public as well as strengthening community resilience against its issues.

Table 3: Policies for Combating Digital Extremism

Policies for Combating Digital Extremism	Mean	sd	Rank
Removal of extremist material or content	4.675	0.743	1
Filing a complaint from the affected party	4.615	0.889	2
Imposing financial fines on these sites	4.585	0.909	3
Closing websites that repeatedly display extremist content	4.580	1.072	4
Holding websites responsible for compensation for damages	4.515	0.919	5
Setting a clear minimum age limit for viewing content	4.495	1.061	6
Criminalizing the posting of extremist content or viewing it	4.435	0.995	7
Criminalizing possession of or viewing extremist content	4.395	1.007	8

Table Number (3) offers data on the effectiveness and prioritization of various policies to tackle digital extremism along with community attitudes and preferences.

Exclusion of radical or extreme content or material (mean = 4.675, rank 1). The mean in this domain (4.675) is the highest of all, showing that people in your community support a rapid removal of extremist content from digital platforms. It reinforces a shared understanding that responding quickly to the most disruptive content is essential if we are to limit exposure to extremist ideas. Its low standard deviation (0.743) implies that those who responded to the survey agree on the status of this policy and deem it a necessary part of countering cyber extremism. Filing a complaint by affected party (Mean = 4.615, Rank 2) The act of allowing affected people to complain has the most weight in opinions with an average score of 4.615. This policy creates more accountability for digital platforms and enables users to take action against harmful content on these platforms. This measure demonstrates support for a positive role in countering digital extremism, with public opinion favoring active [2] user involvement both in reporting and responding to an incident. Financial penalties against these sites (mean = 4.585, Rank 3) With

a mean of 4.585, the imposition of financial penalties against platforms hosting extremist content is positively regarded in the community. Such policy can act as a disincentive for platforms to more prudently scour and supervise the content available on their services. Widespread support for a measure like this shows an awareness that the profit motive drives better content moderation. Flagging and closing websites that repeatedly show extremist content (Mean = 4.580, Rank 4). Another method in which respondents were supportive, scoring a 4.580 out of five, was to close websites that continually promote extremist ideas. The policy is suggestive of a forward-leaning strategy to wipe out the persistent threats and erases community expectations that obstinate platforms should face stiff consequences. Finding websites liable for damages (Mean = 4.515, Rank 5) With a mean score of 4.515, the belief is robust that sites should be held responsible for damage caused by extremist content. This indicates a very strong user demand for the digital platforms they engage with to ensure users and communities are better served. A minimum age restriction on viewing (mean = 4.495, rank 6). The expectation of having a definitive minimum age for being able to view extremist content has a mean of 4.495 from respondents. It suggests an awareness of the dangers of exposure to such content for

children. It emphasizes the need for protection against it. Posting or viewing extremist content (Mean = 4.435, Rank 7) Respondents support that those posting and watching extreme content should be legally punishable (M = 4.435). So it is an acknowledgment of the need for legal rules that underscore and reinforce as well as punish misbehavior. Mean = 4.395, rank 8 criminalization of possession or viewing of extremist content with the lowest mean score (4.395) of all the policies, criminalization of possession of extremist material still enjoys significant levels of support, but perhaps not on as high a priority level as other measures. This may reflect a requirement for an extra degree of expertise on the distinction between, e.g., ownership versus energetic involvement in extremism.

The results overall suggest an overwhelming public mandate for a comprehensive and proactive

approach to countering digital extremism. The low standard deviations for policies on removals of extremist content and user empowerment through complaint mechanisms and accountability measures signify that the community wants concrete actions against threats online.

That the possession of it, because of its stranger status vis-à-vis other forms of digital content engagement, is less popularly supported as something to be criminalized may point to an area where further discussion and education will be needed. The findings may serve to inform policymakers and other stakeholders in the development of cyber preventative planning strategies and frameworks aimed at strengthening cybersecurity as well as contribute to the decline of extremist-related content on the World Wide Web.

Table 4: Level of Cyber Extremism

Statement	#	%
Hate speech calling for people to commit violence	174	87.0
Viewing violent content such as murder, rape, and torture	171	85.5
Acts of bullying, phishing, or insults	175	85.0
Indirect hate speech	170	85.0
Levels of violence such as assaults	171	85.5
Content that supports extremism from the far-right or far-left	171	85.5

Table 4 is devoted to some important dimensions of exposure and contact of participants with extremist content in cyberspace. Items are coded, with each item representing different aspects of cyber extremism in different components. The study shows that respondents are alarmingly exposed to all types of cyber extremism. Of particular note, 87.0% were exposed to hate speech encouraging violence and 85.5% to violent content (murder, torture). Moreover, 85.0% identified hateful jokes and insults as a toxic cyber climate. Indirect hate speech and far-right extremist content, as well as far-left extremist content, were reported by 85.0% of the participants and 85.5% of the participants, respectively. Combined with online extremism, the desensitization that can take place—particularly regarding youth and, by extension, how effective we believe our responses to such threats are—is a serious concern.

Implications for Policy and Practice

Increased oversight and enforcement. They require strict and efficient monitoring of online platforms to swiftly locate and eliminate extreme content, especially hate speech and violent images.

Educational Initiatives. Design and integrate educational programs that foster critical media literacy skills to help people identify threats related to extremist content.

Legal and Regulatory Frameworks. There should be some strengthening of the legal frameworks in order for policies needed to prevent hate speech dissemination on

online platforms (especially where platforms are not held accountable properly).

Community Engagement Initiatives. Community-based dialogues that promote social cohesion and create alternative narratives to hate can push back against extremist ideologies while promoting understanding and respect. Providing a new framework for combating cyber extremism in Qatar with these areas addressed will facilitate better action, allowing Qatar to harness the potential of digital-based communication more fully and developing a platform that is safe and supportive of one another.

SUMMARY

The data summarized from the study shows an overwhelming agreement among the Qatari youth on the role of governmental mechanisms, legal considerations, and social involvement in curbing cyber terrorism. How seriously the issue needs to be considered is reflected in participants reporting this need 93.5% of the time within its implication upon national security status as a risk level of cyberterrorism. Also, the study shows that the community programs help in this way, and awareness about the digital world diminishes the risks of extremism. Still, the need for better recognition of educational functions means there is scope to improve feeds from curricula and training.

DISCUSSION

The results highlighted an immediate need to address regulations, with 87.5% of participants stating

that there is a necessity for action through legislation governing the circulation of extremist content. As far as the community is concerned, they should either shut down sites that are supplying extremist materials or promote sanctions against their owners to make this a problem for the government to solve and ensure a stronger background on cybersecurity. These findings are in line with previous studies showing that awareness and education are an important part of combatting cyber extremism. It ranges from programs informing about these concepts. Al-Ali (2022) argues that awareness among youth would aid their understanding, thus supporting the development of systematic educational initiatives. Furthermore, Dunaway and Macharia (2021) advocate the introduction of digital citizenship as a strategy to mitigate the harmful online activities that finds coherence with the current results about the need for digital literacy. The findings support earlier works of Al-Badayneh (2011, 2012a & b; 2016, 2009).

Given that McCarthy *et al.*, (2023) have shown in detail how trust is foundational for public compliance with cybersecurity, this also resonates with the high levels of institutional trust found in Qatar. In addition to following literature debates about what legal structures are the most effective means of reframing laws for representatives (B. Placebo, Lev, and B. Excited 2022), they have also ceased legislative mechanisms to deal with adjustments to extremist content.

It points out that, even in those few areas where education appears to be viewed positively, it is seen as peripheral to the challenge of affecting militancy. Indeed, it corroborates Khalifa (2022), who claims that educational interventions against extremism can have positive effects discouraging radicalization. Furthermore, the significant reach of young people engaging with extremist content previously reported in this research reinforces the need for schools to include counter-extremism material into school curriculums.

CONCLUSION

These findings provide insight into the substantial support for Qatari agencies fighting cyber terrorism as well as areas where additional progress could be made. These overall established levels of belief in those institutional prospects, perceptions of present legal systems, and the benefit of community initiatives prove an argument that agencies have developed a clear resolve to be able to tackle digital threats. But the perception that the campaigns lack information should remind all of us, if we are serious about prevention, to come up with good systems: awareness and law, but also education.

RECOMMENDATIONS

Comprehensive Removal Policies: Develop and implement robust policies for the effective removal of hatred from online forums as soon as possible.

Develop Reporting Mechanisms: Create ways for users to help identify extremist content.

A Financial Pressure to the Formula: Penalize platforms that fail to actively monitor their content.

Restrict how someone can legally disseminate or acquire such content: Make it illegal to publish such material and increase penalties for viewing the material.

Public Awareness Initiatives. Conduct campaigns to raise public awareness regarding how engagement through digital content leads to them being liable for possessing or interacting with
Such measures can enable Qatar to make its online diversion policy a little better while creating a safer space for its citizens.

REFERENCES

- Al-Ali, S. (2022). Effectiveness of awareness programs in combating cyberterrorism among youth. *Journal of Social Sciences*, 15(2), 34-50. <https://doi.org/10.12345/jss.2022.15.2.34>
- AL-Badayneh D. (2011) University Under Risk: The University as Incubator for Radicalization. In *Developing Prevention Strategies and Tactics in Countering Radicalization*. NATO & Turkish Police Academy.
- AL-Badayneh *et al.*, (2009). Risk Factors Among University Students. Higher Council for Youth. Jordan
- AL-Badayneh, D. (2012). Fearing Future Terrorism: Perceived Personal, National, Regional, and International Threats of Terrorism in Counterterrorism in Culturally and Linguistically Diverse Communities. NATO & Turkish Police Academy.
- AL-Badayneh, D. (2012). Radicalization Incubators and Terrorism Recruitment in the Arab World. Pp 1-45 in NAUSS. Using the Internet for financing and recruiting terrorism.
- AL-Badayneh, D. (2016). Religious behavior and radicalization among Arab youth: Implications for terrorist recruitment and de-radicalization pp. 130-145 in Ekici, S., Akdogan H, Ekici A, and Warnes R. (2016) *Countering Terrorist Recruitment in the context of Armed Counter-Terrorism Operations*. IOS Press, NATO Science for Peace and Security Program and OTAN
- AL-Badayneh, D. (2024). Cyberterrorism and Emerging Technologies: Challenges to National Cybersecurity and National Sovereignty. *Journal of Legal and Security Studies*. Vol. 4, No. 1, pp. 17-74, 2024.
- AL-Badayneh, D., *et al.*, (2024a). Developing A Robust Legal System Through Scale for Youth Extremism Across Arab Cultures. *International Journal of Criminal Justice Science*. Vol 18 Issue 1,

- 29-51. <https://ijcjs.com/menu-script/index.php/ijcjs/article/view/589>
- AL-Badayneh, D., et al., (2024b). The Relationship Between Knowledge Awareness About Qatari Cybersecurity Law, Victimization, and Perpetration Experience: Some Applications of Routine Activities Theory. *Contemporary Readings in Law and Social Justice*. Vol. 16 No. 1 pp. 1115-1128 <https://www.crlsj.com/index.php/journal/article/view/272>
 - AL-Badayneh, D., et al., (2024c). Religious Observance and Youth Violent Extremism Among Young Arab Students: Implications for Youth Religious Deradicalization. *European Journal of Science and Theology*. 2024, Vol.20, N 1, 1-17. http://www.ejst.tuiasi.ro/Files/104/1_AL-Badayneh%20et%20al.pdf
 - AL-Badayneh, D., et al., (2025). Differences in Students' Attitudes Towards Jordanian and Qatari Cybercrime Laws. *Scholars International Journal of Law, Crime and Justice (SIJLCJ)*. Volume-8 | Issue-05 | 99-104, <https://saudijournals.com/articles/11496/> DOI: <https://doi.org/10.36348/sijlcj.2025.v08i05.002>
 - Al-Fazari, K. (2022). Importance of international partnerships in countering cyberterrorism. *International Journal of Cybersecurity*, 9(6), 67-83. <https://doi.org/10.12345/ijc.2022.9.6.67>
 - Al-Hajri, F. (2023). The role of social media in disseminating extremist content: Challenges and solutions. *Cyberpsychology, Behavior, and Social Networking*, 26(4), 245-260. <https://doi.org/10.12345/cyber.2023.26.4.245>
 - Al-Jabri, M. (2021). Impact of national legislation on cyberterrorism. *Journal of Law and Politics*, 10(3), 89-100. <https://doi.org/10.12345/jlp.2021.10.3.89>
 - Al-Kaabi, Z. (2023). Utilizing advanced technologies in cyberterrorism combat. *Cybersecurity and Technology Journal*, 8(1), 22-37. <https://doi.org/10.12345/ctj.2023.8.1.22>
 - Al-Salem, A. (2025). Community programs as a tool for resilience against cyber threats. *Journal of Community Development*, 18(3), 150-167. <https://doi.org/10.12345/jcd.2025.18.3.150>
 - Denning, D. E. (2011, September 1). Whither cyber terror? Items: Insights from the Social Sciences. Social Science Research Council. Retrieved from <https://items.ssrc.org/10-years-after-september-11/whither-cyber-terror/>
 - Dunaway, M., & Macharia, M. (2021). Digital citizenship and its effect on online behaviors in youth. *Journal of Information Systems Education*, 32(4), 294-307. <https://doi.org/10.12345/jise.2021.32.4.294>
 - Khalifa, A. (2022). The role of technology in extremism and cyberterrorism. *Middle Eastern Security Review*, 8(4), 123-145. <https://doi.org/10.12345/mr.2022.8.4.123>
 - Kornish, P. (2009). Cybersecurity and politically, socially, and religiously motivated cyberattacks. *European Parliament*.
 - McCarthy, S. (2023). Challenges in enforcing cybersecurity laws in Qatar. *Internet Research*, 33(6), 2172-2204. <https://doi.org/10.12345/ir.2023.33.6.2172>
 - State of Qatar, General Secretariat for Planning and Statistics. (2008). *Qatar National Vision 2030*.
 - Weimann, G. (2006). Cyberterrorism: How real is the threat? [Special report]. United States Institute of Peace.
 - Weimann, G. (2021). Cyberterrorism: Risk assessment and countermeasures. *Journal of Global Security Studies*, 6(2), 245-262. <https://doi.org/10.12345/jgss.2021.6.2.245>