SOCILEXIA
Journal of Social Sciences and Humanities

SOCILEXIA: Journal of Social Sciences and Humanities
Vol. 1, No. 1, 2026
E-ISSN: XXXX-XXXX
punggawajournal.com/socilexia

Cyberterrorism across Digital Borders and the Changing Limits of International Security Cooperation

Nadiah Khaeriah Kadir[1]
[1] Fakultas Hukum, Universitas Hasanuddin, Indonesia
Correspondence: nadiahkhaeriah@unhas.ac.id

Article Info

Article History:
Received June 15th, 2026
Revised June 25th, 2026
Accepted June 29th, 2026

Keyword:
Cyberterrorism; Cyber cooperation; International security; Sovereignty; Transnational threats.

ABSTRACT

A suspected cyberterrorist attack can damage infrastructure in one state while leaving the most useful evidence in another. Governments may face demands for retaliation before investigators know whether the actor is a terrorist group, an individual, or a state-backed proxy. This study examined how that uncertainty was changing the practical limits of international security cooperation. This research use normative legal research was used to analyze treaty rules, United Nations counter-terrorism measures, the law of state responsibility, and cyber norm documents. The analysis showed that sovereignty continued to determine coercive authority, while territorial jurisdiction no longer guaranteed timely access to evidence. Cooperation increasingly relied on faster preservation procedures, direct engagement with service providers, and emergency channels that could operate before final attribution. Those developments remained uneven because newer treaty frameworks were not yet fully operational in 2026. Cyberterrorism therefore exposed a shift in the problem rather than the disappearance of state authority: current limits increasingly concern speed, access, trust, private control of infrastructure, and disagreement over attribution.

© 2026 The Authors. Published by Punggawa Legacy Center. This is an open access article under the CC BY license (https://creativecommons.org/licenses/by/4.0/)

INTRODUCTION

A cyber operation directed at a hospital or electricity network can be felt in one country while the accounts, routing data, and service providers needed by investigators are located elsewhere. The affected state may have a clear basis to criminalize the conduct and protect its population, yet its police cannot simply enter a foreign network and seize evidence. That gap between legal authority and practical access becomes more difficult when the operation appears political or ideological. Counter-terrorism agencies may become involved before investigators can establish who acted, where they acted from, or whether another state supported them.

Cyberterrorism has never acquired a stable international definition. Broeders, Cristiano, and Weggemans (2023) show large differences between national policy and international diplomacy, while Iftikhar (2024) uses a broader threat-based understanding that includes several forms of hostile digital activity. Terrorist use of the internet is not the same as a cyberterrorist attack. Recruitment or propaganda can support terrorism without making the digital activity itself the coercive act. Research on critical infrastructure usually works with a narrower object. Backhaus et al. (2020) found strong emotional reactions to lethal cyberterrorism, Shandler et al. (2022) observed increased support for retaliation, and Snider et al. (2026) found greater support for surveillance after attacks on critical infrastructure. Governments therefore confront a political pressure that can arise before legal characterization is settled. The public may read delay as institutional failure even when delay reflects an unresolved evidentiary problem. That gap matters for international cooperation because an ally asked to endorse an attribution may not share the same level of confidence or the same domestic pressure to act.

The analysis uses cyberterrorism in a restricted sense. The term refers to politically or ideologically motivated cyber conduct that is itself used to intimidate or coerce through serious

disruption or harm. Ordinary ransomware does not become terrorism because it crosses a border, and routine online activity by a terrorist organization is not treated as a cyberterrorist attack merely because a terrorist actor is involved. A narrow working definition is necessary because the terrorism label can change the institutions and powers brought into a case.

States have not become marginal in digital security. Mainwaring (2020) shows how sovereign authority continues to organize conduct in cyberspace, and Foulon and Meibauer (2024) argue that digital conditions modify international interaction rather than create a separate international system. The harder change concerns the location of security capacity. Private companies may see malicious traffic before public authorities do. They also control cloud services and communication systems from which evidence has to be obtained. Broeders (2021) and Pattison (2020) explain why private defensive capacity can support state security while creating legal and political problems when private action moves beyond the provider's own systems. The result is not a transfer of sovereignty to companies. Public authority remains with states, but states increasingly depend on actors that are not organized around national borders and that may answer to more than one legal system at the same time.

Domestic pressure can narrow the time available for careful judgment. Public attribution may be demanded while forensic work is incomplete, especially after visible disruption to essential services. A government that waits can be accused of weakness. A government that attributes too quickly can create an interstate dispute on evidence that would not survive criminal proceedings. Cyberterrorism makes the tension sharper because the language of terrorism carries expectations of prevention and punishment that are stronger than the language normally used for cybercrime.

International cooperation has also changed during the same period. The Budapest Convention created a durable basis for cybercrime cooperation, but newer instruments increasingly address the speed and location of electronic evidence. The Second Additional Protocol seeks more direct and faster cooperation across jurisdictions. A separate United Nations cybercrime convention was adopted in 2024, although it had not entered into force by 2026. The central question is no longer whether sovereignty survives digital borders. The more useful question is how states can exercise sovereign authority when evidence and operational knowledge are distributed beyond their immediate control. The argument developed here is that the limits of cooperation have shifted from a mainly territorial problem toward a combined problem of speed, attribution, trust, and access.

RESEARCH METHODS

This study uses normative legal research to examine the legal framework governing international cooperation in responding to cyberterrorism across national borders. The research focuses on legal norms, principles, and rules relevant to cross-border investigation, international cooperation, sovereignty, attribution, and state responsibility. The study does not seek to measure the frequency or technical characteristics of cyberterrorist attacks. Instead, it examines how international law regulates the authority of states and the legal mechanisms available when cyberterrorist activities involve more than one jurisdiction.

The research applies a statutory approach and a conceptual approach. The statutory approach is used to examine international legal instruments relevant to cyberterrorism and cross-border cooperation, including the United Nations Charter, United Nations Security Council Resolutions 1373 and 2341, the Convention on Cybercrime, its Second Additional Protocol, the Articles on Responsibility of States for Internationally Wrongful Acts, and the United Nations Convention against Cybercrime. The conceptual approach is used to examine legal concepts concerning sovereignty, jurisdiction, attribution, state responsibility, international cooperation, and the legal position of non-state actors in cyberspace. These approaches are used together to assess how existing legal rules apply when evidence, perpetrators, infrastructure, and affected states are located in different jurisdictions.

The study relies on primary and secondary legal materials. Primary legal materials consist of international conventions, United Nations resolutions, instruments concerning state responsibility, and other relevant international legal documents. Secondary legal materials include peer-reviewed journal articles and scholarly publications discussing cyberterrorism, international security, cyber sovereignty, attribution, electronic evidence, and international cooperation. Institutional documents and official reports are also used where necessary to clarify the development and legal status of international cyber cooperation frameworks.

The legal materials are analyzed qualitatively through legal interpretation and systematic analysis. Relevant rules and principles are examined in relation to one another to identify their scope, legal implications, and limitations in addressing cross-border cyberterrorism. The analysis distinguishes territorial jurisdiction from the authority to obtain evidence located abroad and also separates technical or public attribution from legal attribution to a state. The results are then assessed prescriptively to determine the legal limits and possibilities of international security cooperation when the legal characterization of a cyber incident develops as additional evidence becomes available.

RESULTS AND DISCUSSION

1. Territorial Authority and the Problem of Evidence Access

A state may have a strong territorial connection to an attack and still be unable to obtain the evidence needed to investigate it. Harm to a domestic hospital gives the affected state an obvious regulatory and protective interest. Account records held by a provider abroad are different. The state can prescribe offences that protect its territory without gaining a general right to exercise police powers inside another jurisdiction. The distinction matters because many practical disputes described as problems of jurisdiction are more precisely problems of enforcement authority and access to foreign-held evidence.

Sovereignty remains relevant because cross-border investigation still depends on permission, treaty procedure, or another accepted legal basis. Mainwaring (2020) describes states as continuing to assert control in cyberspace, while Shokri (2026) reaches a similar conclusion from international law despite disagreement about the exact legal consequences of sovereignty online. Cloud computing makes that authority harder to use quickly. Data can move across several jurisdictions without any decision by the offender, so server location may say little about where the harmful conduct was planned or directed. The affected state can possess jurisdiction over the offence while lacking practical access at the moment when logs or account information are most useful. That difference is easy to miss when jurisdiction is discussed as a single concept. Prescriptive authority over the offence may be clear, while investigative action against a foreign server still depends on consent or an accepted cooperation mechanism. Cyberterrorism does not create the distinction, but it makes the cost of ignoring it more visible because delay can affect both security response and criminal proof.

Delay is not a minor procedural inconvenience in a cyber investigation. Volatile data can disappear, accounts can be abandoned, and infrastructure can be reconfigured while a formal request moves between authorities. The legal question consequently changes from whether a state has jurisdiction to whether that jurisdiction can be exercised through cooperation at a speed that preserves the case. A valid legal request that arrives after the relevant data have disappeared offers little practical protection to the affected state. Speed therefore affects whether jurisdiction can produce an effective investigation in practice today.

Remote digital conduct can also affect sovereignty without resembling a conventional territorial intrusion. Michaelsen and Thumfart (2023), writing about digital transnational repression, show how conduct organized outside a host state can still interfere with persons and political activity inside it. Cyberterrorism raises a different legal problem, yet the jurisdictional lesson is useful. Physical distance no longer keeps the source of coercion outside domestic security concerns. States still have to respect foreign territorial authority while protecting people and systems at home, which makes cooperation part of the exercise of sovereignty rather than evidence that sovereignty has disappeared.

The Budapest Convention addressed international assistance through preservation duties, mutual assistance, and a 24/7 contact network. Its later Second Additional Protocol reflects a different level of dependence on foreign-held evidence. The Protocol provides for direct cooperation with service providers in other jurisdictions for subscriber information, faster government-to-government routes for certain data, and expeditious cooperation in emergencies. Those mechanisms respond to a practical weakness that became more visible as cloud services and globally distributed platforms expanded. The Protocol had four ratifications by April 2026 and had not yet entered into force, so its significance in this study lies in the direction of legal development rather than in a claim that it already governs cross-border practice for all parties.

Private providers are central to that change because evidence is often produced and retained outside government systems. Egloff and Dunn Cavelty (2021) show that knowledge about cyber incidents is assembled through public and private actors. Providers may preserve records or disclose

information through lawful processes, yet their operational role does not give them the same authority as states. Pattison (2020) and Broeders (2021) warn about the move from private defence into cross-border offensive conduct. Faster cooperation with providers can therefore improve evidence access without treating a company as an independent international security actor with coercive powers.

Different political projects of digital sovereignty make access harder to standardize. Farrand and Carrapico (2022) connect European digital sovereignty with regulatory autonomy, while Farrand, Carrapico, and Turobov (2024) place cybersecurity within a wider EU concern about geopolitical dependence. Gao (2022) describes a more state-centred Chinese approach to cyber governance. Flonk (2021) also identifies Russian and Chinese support for stronger state control over information. These positions do not prevent every form of cooperation, but they affect how governments view foreign requests and platform duties.

Territorial authority has therefore not weakened in a simple sense. The more important change is that authority is increasingly separated from the data and technical capacity needed to use it. Earlier cooperation could be organized mainly around one state asking another state for assistance. Current practice places service providers and emergency evidence preservation much closer to the centre of the response. The legal boundary remains territorial, while the practical limit increasingly turns on whether lawful access can occur before evidence is lost.

2. Attribution and the Politics of Uneven Cooperation

Attribution becomes more difficult when the political demand for an answer develops faster than the evidence. Technical investigation may identify infrastructure or malware without establishing who controlled the operation. Public attribution by a government adds a political judgment about responsibility. Legal attribution to a state asks a different question again. Article 8 of the Articles on State Responsibility requires conduct by a person or group to be carried out on the instructions of, or under the direction or control of, the state before that conduct is treated as an act of the state under that rule. Mere presence of an attacker or server within state territory does not satisfy that test. Legal attribution also differs from a claim that another state failed to prevent harmful activity originating from its territory. Those questions may overlap politically, but they rest on different legal reasoning. A careful analysis must therefore resist the common move from technical indicators to state responsibility without showing the required connection between the conduct and the state.

Cybersecurity practice often produces a level of confidence that is useful for diplomacy but not identical to proof required for prosecution or legal responsibility. Egloff (2020) treats public attribution as a political practice. Egloff and Smeets (2023) show how evidence, timing, audience, and strategic purpose affect decisions to attribute publicly. Brown and Fazal (2021) add that governments accused of cyber operations may benefit from refusing to confirm or deny responsibility. A victim state can therefore face a real security threat while the legal status of the actor remains unsettled.

Cyberterrorism makes the distinction harder to ignore. A non-state group may trigger criminal and counter-terrorism cooperation without any basis for attributing the conduct to a state. Evidence of state support can matter without proving that the operation is legally attributable to that state. Hosting infrastructure, tolerating a group, financing related actors, and directing a specific operation raise different legal questions. Collapsing them into one accusation may produce a strong political message, but it weakens the analytical basis for deciding what response is lawful.

Terrorist purpose does not by itself convert a cyber operation into an armed attack. Scale and effects matter under the Charter framework, and many serious cyber incidents remain below that level. Kello (2021) argues that conventional legal categories do not always capture competition in cyberspace well, while Lonergan and Schneider (2023) show how deterrence and escalation beliefs have evolved in cyber strategy. Those criticisms do not remove legal thresholds. They show why a government can regard an incident as strategically serious even when the available facts do not support self-defence or another coercive interstate response. The gap can be politically uncomfortable. A cabinet may believe that a weak response invites further attacks while its lawyers conclude that the facts support criminal cooperation rather than force. International security policy has to manage that gap rather than erase it by stretching legal categories.

Differences among states also shape which attribution claims they trust. Chen and Gao (2024) describe China as an active participant in cyber norm development rather than a passive recipient of Western rules. Fung (2022) shows how shared cyber language can be adapted to fit different political

positions. Foulon and Meibauer (2024) caution against treating cyberspace as detached from the structure of international relations. Attribution therefore takes place inside existing rivalry and institutional distrust. A technically plausible claim can still fail to produce collective action when other states do not accept the evidence or the political framing attached to it.

Domestic reactions can increase the cost of that disagreement. The survey experiments by Backhaus et al. (2020), Shandler et al. (2022), and Snider et al. (2026) suggest that severe cyberterrorist incidents can affect fear, support for retaliation, and support for surveillance. Those findings do not determine international law, but they help explain why governments may prefer a quick public position. Another state asked to cooperate may face no equivalent pressure. Different political clocks can therefore operate around the same incident, making evidence sharing easier than a joint declaration of responsibility.

States with limited forensic capacity can slow evidence collection for an attack that harmed another country. Better-resourced governments can draw on national cyber agencies and large private firms during an investigation. Others depend more heavily on external assistance. Katagiri (2021) notes the difficulty international law faces in preventing non-state cyberattacks, especially when enforcement capacity is uneven. A weak investigative system in one jurisdiction can slow evidence collection in another. Capacity-building is consequently part of international security cooperation rather than a separate development issue.

Unilateral action can create a new dispute before the original attack is understood. A private company may have the technical ability to disrupt infrastructure used by an attacker in another country, but domestic authorization does not remove the international consequences of crossing that boundary. Leventopoulos, Pipyros, and Gritzalis (2024) show how difficult retaliation decisions become when attribution and legal thresholds are uncertain. Broeders (2021) reaches a similar concern for private active defence. Restraint is especially important when the actor may be non-state and the foreign state may have no responsibility for the operation.

Cooperation does not have to wait for all of those questions to be answered. Foreign authorities can preserve data or respond to emergency requests while attribution remains provisional. Providers can retain relevant records without deciding whether the incident amounts to terrorism. Such measures have a lower political and legal cost than sanctions, countermeasures, or public claims against another state. The distinction is important for international relations because it allows states with different views of an incident to cooperate on evidence before they agree on responsibility.

3. The Shift toward Faster and More Conditional Cooperation

Cyberterrorism moves across several bodies of law because no single regime was designed for the entire problem. A suspected attack may require ordinary cybercrime procedures at the start (Kadir, 2025; Kadir & Kadir, 2024). Evidence of ideological purpose can bring counter-terrorism obligations into the same investigation. Credible state direction can later raise questions of international responsibility. Broeders et al. (2023) show how disagreement about the meaning of cyberterrorism already complicates national policy and diplomacy. The practical challenge is therefore not a complete absence of rules. Different rules become relevant at different points and do not always require the same evidence.

The Budapest Convention remains the most established treaty framework in this area, but recent legal development shows why traditional mutual assistance is no longer considered sufficient on its own. The Second Additional Protocol was opened for signature in 2022 after years of concern about electronic evidence held in foreign or shifting jurisdictions. Direct provider cooperation and emergency procedures are a response to the speed of digital investigations. The Protocol still had not entered into force by 2026. That limited legal reach is itself revealing. States increasingly recognize the need for faster cooperation, yet agreement on new procedures does not immediately produce wide operational coverage. Ratification also requires domestic changes and institutional preparation. A state may support the idea of faster access while remaining cautious about direct provider requests or data protection safeguards. The gap between treaty design and operational use is therefore part of the changing limit, not a technical detail outside the security analysis.

The United Nations Convention against Cybercrime points in the same direction at a global level but must be described according to its current legal status. The convention was adopted in December 2024 and remained open for signature through the end of 2026. On 2026 the United Nations

Treaty Collection recorded that it was not yet in force. Article 65 requires forty instruments of ratification, acceptance, approval, or accession before the entry-into-force process begins, while only three parties were recorded on that date. The convention can therefore be assessed as an emerging framework for future cooperation and electronic evidence, not as a source of operational treaty obligations that already binds a broad global membership.

Security Council Resolution 1373 requires states to suppress terrorist financing and cooperate against terrorism, while Resolution 2341 addresses terrorist threats to critical infrastructure. Neither instrument provides a settled definition of cyberterrorism. A state can therefore share evidence under criminal cooperation channels while another authority examines terrorist purpose. Keeping those functions separate at the early stage reduces the risk that a contested security label will determine whether evidence can be obtained.

The UN Group of Governmental Experts and related state positions recognize that international law applies in cyberspace and support norms of responsible state behaviour. Those processes have not removed disagreement over sovereignty or information control. Chen and Gao (2024), Flonk (2021), and Gao (2022) show that states continue to promote different models of cyber governance. Liebetrau and Monsees (2024) argue that international relations needs concepts that connect digital politics with wider world politics rather than isolating cyber issues as a separate field. Cooperation is therefore most durable when it does not depend on full agreement about the political order of the internet. Norms can reduce uncertainty, but they cannot remove competition over who should control information or how far sovereignty should reach. The practical value of a cooperation mechanism lies partly in whether states with different political models can use it without treating participation as endorsement of a rival model of internet governance.

Carrapico and Farrand (2020) found continuity in EU cybersecurity policy during a period of major political disruption, which suggests that defined operational tasks can survive wider disagreement. Masyhar et al. (2023) show from the Indonesian context how NCB Interpol links domestic enforcement with international counterparts in cyberterrorism cases. The same logic applies more broadly. Evidence preservation or contact between designated authorities can proceed even when governments disagree about attribution. A narrow request is easier to assess than a demand that another state endorse the requesting state's entire security narrative.

Private control of evidence makes trust more complicated because cooperation can involve a state, a foreign authority, and a company at the same time. Egloff and Dunn Cavelty (2021) describe the mixed public and private production of cyber knowledge, while Katagiri (2021) points to the difficulty of restraining non-state cyber actors through international norms alone. A provider can respond quickly to an emergency request and still need a clear legal basis for disclosure. States also need confidence that expedited procedures will not become routine shortcuts around territorial safeguards. Faster cooperation therefore depends on institutional trust as much as technical speed.

Incident responders can contain harm and retain technical material before governments agree on the final legal and political meaning of an attack. Law-enforcement authorities can use treaty or other lawful channels to obtain evidence abroad. Counter-terrorism authorities can assess purpose and organizational links as the facts develop. Public attribution or a claim of state responsibility should come later when the evidence supports it. No universal order of steps will fit every attack, but the underlying distinction is useful. Reversible forms of cooperation can begin earlier than coercive responses that may create a new interstate dispute.

The meaning of changing limits follows from that development. Territorial sovereignty still limits foreign enforcement, and political rivalry can still block assistance. Newer cooperation mechanisms do not erase those constraints. They alter where failure is most likely to occur. The older problem was heavily associated with formal requests between territorial states. Current cooperation depends more on rapid preservation, direct or expedited access routes, provider participation, and trust in shared evidence. Cyberterrorism tests those arrangements because the legal character of an incident can change while the evidence is still being collected. International security cooperation becomes stronger when it can tolerate that uncertainty without treating every early suspicion as a final attribution.

CONCLUSION

Cyberterrorism does not make sovereignty obsolete. The affected state still depends on sovereign authority to investigate offences, request assistance, prosecute suspects, and decide whether

an incident has consequences for interstate responsibility. The difficulty is that much of the evidence needed to exercise those powers may be held outside its territory. Cross-border cooperation has responded by moving toward faster preservation and more direct access procedures, but the legal reach of those newer mechanisms remains incomplete. The Second Additional Protocol and the United Nations Convention against Cybercrime show the direction of change while also showing how slowly new treaty arrangements can acquire broad legal effect.

Attribution creates a different limit. Technical confidence, public attribution, and legal attribution to a state should not be treated as the same conclusion. Cyberterrorism can be investigated through criminal and counter-terrorism cooperation while state responsibility remains uncertain. Keeping those questions apart reduces the pressure to convert incomplete evidence into an interstate accusation. That separation also gives partner states more room to assist with an investigation without being asked to endorse a political conclusion that their own authorities are not yet prepared to accept. Cooperation can continue while political judgment remains unsettled.

More effective international security cooperation depends on what can lawfully be done before final characterization. Evidence preservation, emergency assistance, and provider cooperation can often proceed with less political risk than sanctions or coercive responses. Wider disagreement over cyber sovereignty will remain, and unequal investigative capacity will continue to matter. The practical shift is nonetheless clear. Cooperation is no longer limited mainly by territorial borders. Its effectiveness increasingly depends on speed, access to privately held evidence, confidence in attribution, and the willingness of states to cooperate without requiring immediate agreement on the final political meaning of an attack.

REFERENCES

Backhaus, S., Gross, M. L., Waismel-Manor, I., Cohen, H., & Canetti, D. (2020). A cyberterrorism effect? Emotional reactions to lethal attacks on critical infrastructure. *Cyberpsychology, Behavior, and Social Networking*, *23*(9), 595–603. https://doi.org/10.1089/cyber.2019.0692

Broeders, D. (2021). Private active cyber defense and (international) cyber security—pushing the line? *Journal of Cybersecurity*, *7*(1), tyab010. https://doi.org/10.1093/cybsec/tyab010

Broeders, D., Cristiano, F., & Weggemans, D. (2023). Too close for comfort: Cyber terrorism and information security across national policies and international diplomacy. *Studies in Conflict & Terrorism*, *46*(12), 2426–2453. https://doi.org/10.1080/1057610X.2021.1928887

Brown, J. M., & Fazal, T. M. (2021). #SorryNotSorry: Why states neither confirm nor deny responsibility for cyber operations. *European Journal of International Security*, *6*(4), 401–417. https://doi.org/10.1017/eis.2021.18

Carrapico, H., & Farrand, B. (2020). Discursive continuity and change in the time of COVID-19: The case of EU cybersecurity policy. *Journal of European Integration*, *42*(8), 1111–1126. https://doi.org/10.1080/07036337.2020.1853122

Chen, X., & Gao, X. (2024). Norm diffusion in cyber governance: China as an emerging norm entrepreneur? *International Affairs*, *100*(6), 2419–2440. https://doi.org/10.1093/ia/iiae237

Egloff, F. J. (2020). Public attribution of cyber intrusions. *Journal of Cybersecurity*, *6*(1), tyaa012. https://doi.org/10.1093/cybsec/tyaa012

Egloff, F. J., & Dunn Cavelty, M. (2021). Attribution and knowledge creation assemblages in cybersecurity politics. *Journal of Cybersecurity*, *7*(1), tyab002. https://doi.org/10.1093/cybsec/tyab002

Egloff, F. J., & Smeets, M. (2023). Publicly attributing cyber attacks: A framework. *Journal of Strategic Studies*, *46*(3), 502–533. https://doi.org/10.1080/01402390.2021.1895117

Farrand, B., & Carrapico, H. (2022). Digital sovereignty and taking back control: From regulatory capitalism to regulatory mercantilism in EU cybersecurity. *European Security*, *31*(3), 435–453. https://doi.org/10.1080/09662839.2022.2102896

Farrand, B., Carrapico, H., & Turobov, A. (2024). The new geopolitics of EU cybersecurity: Security, economy and sovereignty. *International Affairs*, *100*(6), 2379–2397. https://doi.org/10.1093/ia/iiae231

Flonk, D. (2021). Emerging illiberal norms: Russia and China as promoters of internet content control. *International Affairs*, *97*(6), 1925–1944. https://doi.org/10.1093/ia/iiab146

Foulon, M., & Meibauer, G. (2024). How cyberspace affects international relations: The promise of structural modifiers. *Contemporary Security Policy*, *45*(4). https://doi.org/10.1080/13523260.2024.2365062

Fung, C. J. (2022). China's use of rhetorical adaptation in development of a global cyber order: A case study of the norm of the protection of the public core of the internet. *Journal of Cyber Policy*, *7*(3), 256–274. https://doi.org/10.1080/23738871.2023.2178946

Gao, X. (2022). An attractive alternative? China's approach to cyber governance and its implications for the Western model. *The International Spectator*, *57*(3), 15–30. https://doi.org/10.1080/03932729.2022.2074710

Iftikhar, S. (2024). Cyberterrorism as a global threat: A review on repercussions and countermeasures. *PeerJ Computer Science*, *10*, e1772. https://doi.org/10.7717/peerj-cs.1772

Kadir, Z. K. (2025). Kejahatan Berbasis Identitas Digital: Menggagas Kebijakan Kriminal untuk Dunia Metaverse. *Jurnal Litigasi Amsir*, *12*(2), 124–137.

Kadir, Z. K., & Kadir, N. K. (2024). Examining of the Concept of Standard of Proof in the Indonesian Criminal Procedure Code. *International Journal of Global Community*, *1*(1), 13–25.

Katagiri, N. (2021). Why international law and norms do little in preventing non-state cyber attacks. *Journal of Cybersecurity*, *7*(1), tyab009. https://doi.org/10.1093/cybsec/tyab009

Kello, L. (2021). Cyber legalism: Why it fails and what to do about it. *Journal of Cybersecurity*, *7*(1), tyab014. https://doi.org/10.1093/cybsec/tyab014

Leventopoulos, S., Pipyros, K., & Gritzalis, D. (2024). Retaliating against cyber-attacks: A decision-taking framework for policy-makers and enforcers of international and cybersecurity law. *International Cybersecurity Law Review*, *5*, 237–262. https://doi.org/10.1365/s43439-024-00113-5

Liebetrau, T., & Monsees, L. (2024). Cybersecurity and international relations: Developing thinking tools for digital world politics. *International Affairs*, *100*(6), 2303–2315. https://doi.org/10.1093/ia/iiae232

Lonergan, E. D., & Schneider, J. (2023). The power of beliefs in US cyber strategy: The evolving role of deterrence, norms, and escalation. *Journal of Cybersecurity*, *9*(1), tyad006. https://doi.org/10.1093/cybsec/tyad006

Mainwaring, S. (2020). Always in control? Sovereign states in cyberspace. *European Journal of International Security*, *5*(2), 215–232. https://doi.org/10.1017/eis.2020.4

Masyhar, A., Utari, I. S., Usman, U., & Ahmad Sabri, A. Z. S. (2023). Legal challenges of combating international cyberterrorism: The NCB Interpol Indonesia and global cooperation. *Legality: Jurnal Ilmiah Hukum*, *31*(2), 344–366. https://doi.org/10.22219/ljih.v31i2.29668

Michaelsen, M., & Thumfart, J. (2023). Drawing a line: Digital transnational repression against political exiles and host state sovereignty. *European Journal of International Security*, *8*(2), 151–171. https://doi.org/10.1017/eis.2022.27

Pattison, J. (2020). From defence to offence: The ethics of private cybersecurity. *European Journal of International Security*, *5*(2), 233–254. https://doi.org/10.1017/eis.2020.6

Shandler, R., Gross, M. L., Backhaus, S., & Canetti, D. (2022). Cyber terrorism and public support for retaliation—A multi-country survey experiment. *British Journal of Political Science*, *52*(2), 850–868. https://doi.org/10.1017/S0007123420000812

Shokri, A. (2026). Sovereignty in cyberspace from the viewpoint of international law. *Asian Journal of International Law*, *16*(2), 326–356. https://doi.org/10.1017/S2044251325100556

Snider, K. L. G., Hefetz, A., Shandler, R., & Canetti, D. (2026). Experimenting with threat: How cyberterrorism targeting critical infrastructure influences support for surveillance policies. *Terrorism and Political Violence*, *38*(5), 511–524. https://doi.org/10.1080/09546553.2025.2457746

Council of Europe. (2001). Convention on Cybercrime, ETS No. 185.

Council of Europe. (2022). Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, CETS No. 224.

International Law Commission. (2001). Articles on Responsibility of States for Internationally Wrongful Acts.

United Nations. (1945). Charter of the United Nations.

United Nations General Assembly. (2021). Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, A/76/135.

United Nations General Assembly. (2021). Official compendium of voluntary national contributions on the application of international law in cyberspace, A/76/136.

United Nations General Assembly. (2024). United Nations Convention against Cybercrime, A/RES/79/243.

United Nations Security Council. (2001). Resolution 1373, S/RES/1373.

United Nations Security Council. (2017). Resolution 2341, S/RES/2341.

United Nations Treaty Collection. (2026). Status of the United Nations Convention against Cybercrime.