SCIENTIFIC CULTURE

www.sci-cult.com

SCIENTIFIC CULTURE, Vol. 12, No. 4, (2026), pp. 2175-2185
Open Access. Online & Print

DOI: 10.5281/zenodo.12426298

STATE RESPONSIBILITY AND ATTRIBUTION IN CYBERSPACE: LEGAL CHALLENGES FOR THE GCC

Khalifa Ahmad Alkuwari*

Assistant Professor of International Law, Qatar Police College.
Email: ka4090@pa.edu.qa, ORCID iD: https://orcid.org/0009-0008-9762-3605

Received: 27/10/2025
Accepted: 01/03/2026

Corresponding Author: Khalifa Ahmad Alkuwari (ka4090@pa.edu.qa)

ABSTRACT

This study looks at cyber attribution and governmental accountability in the GCC. It examines theoretical underpinnings, draws attention to difficulties in demonstrating state participation, and examines significant events such as the Shamoon assaults and the hack of the Qatar News Agency. Unlike nations like France, Germany, Canada, and Japan that apply international law to cyberspace, the GCC lacks definite legal stances. The report suggests addressing accountability gaps through collaborative declarations, international cyber law debates, and harmonizing GCC legal systems.

KEYWORDS: State Responsibility; Cyber Attribution; ARSIWA; International Law in Cyberspace; GCC Cybersecurity Policy; Due Diligence; Legal Attribution.

1. INTRODUCTION

States are becoming more and more concerned with how international law regulates malevolent cyber activity, as cyber operations become more complex and large in scope. Cyberspace is governed by "international law, and in particular the Charter of the United Nations," according to the United Nations Group of Governmental Experts (GGE) and Open-Ended Working Group.[1]

According to the ILC's ARSIWA, cyber activities are subject to general state responsibility regulations. Nations such as Canada, Japan, and Germany agree that cyberspace is completely subject to current international law, including the UN Charter.[2]

The GCC states have not taken firm stances on cyber activities under international law, despite global trends. They prioritize technical defences and domestic criminal legislation, even if they have formed national cybersecurity authorities and policies. Although significant assaults like Shamoon and the 2017 breach of the Qatar News Agency bring attention to issues of attribution and responsibility, victims have few international options due to inward-looking GCC regulations. [3]

This study looks at cyber attribution and governmental accountability in the GCC. It contrasts the legal systems of France, Germany, Canada, and Japan, examines important case examples and GCC cyber legislation, and evaluates theoretical norms (ARSIWA). In order to bridge the responsibility gap for victims of cyber activities, the report suggests that GCC states harmonize their legislative stances on cyber attribution and cooperate globally.

Even though the main emphasis of this research is attribution, the law of State responsibility and attribution are inextricably linked. It serves as the legal cutoff point at which a State is held accountable for a globally unlawful act and is therefore subject to international law.

Research Question

The following main research topic is addressed in this paper:

How well can the current international legal framework − ARSIWA in particular −govern the attribution of cyber operations to States?

2. METHODOLOGY

This study employs a qualitative doctrinal legal research methodology, combining comparative legal analysis and case study examination. It starts by examining the theoretical underpinnings of state accountability under the Articles on State accountability for Internationally Wrongful Acts (ARSIWA) of the International Law Commission, namely Articles 1–8 on attribution. The study then looks at the official position papers and public declarations of a few chosen states, such as France, Germany, Canada, and Japan and how they interpret and apply ARSIWA to cyber operations.

France, Germany, Canada, and Japan were chosen on purpose. These states have published official position papers outlining their interpretations of the principles governing attribution in cyberspace, making them models of state practice. They also highlight different legal philosophies: Japan has a formal doctrinal approach, Germany concentrates on factual certainty, Canada emphasizes sovereignty, and France demands strong proof. While states like Estonia and the Netherlands have not created comparably thorough attribution-specific policies, the United States was left out since its positions have changed across administrations without a single comprehensive document. A variety of models are available for comparison with the GCC environment in this selection.

The report examines state cybersecurity plans and reactions to significant cyber events, such as the 2017 hack of the Qatar News Agency and the Shamoon assaults on Saudi Arabia, in order to put the Gulf Cooperation Council (GCC) strategy into perspective. These incidents highlight the GCC's present dependence on political and internal solutions as opposed to international legal frameworks.

Finally, the research draws on recommendations from international legal instruments, authoritative compilations of state practice such as the CCDCOE Cyber Law Toolkit, scholarly commentary (e.g., Tallinn Manual 2.0), and policy documents to propose actionable steps for the GCC to harmonize its legal stance on cyber attribution and strengthen regional and global accountability frameworks.

3. THEORETICAL FRAMEWORK

3.1. State Responsibility and ARSIWA

Under international law, attribution serves as the legal entry point for addressing state responsibility. ARSIWA states that an action cannot be considered globally unjust unless it can be traced back to a State. As a result, attribution is a requirement for claiming

[1] France, *International Law Applied to Operations in Cyberspace*, (14 July 202, citing UN GGE and OEWG Reports, A/76/135, 1

[2] Federal Government of Germany, *On the Application of International Law in Cyberspace*, (Position Paper March 2021), 2.

[3] William C Banks, 'Cyber Attribution and State Responsibility' (2021) 97 *International Law Studies* 1040.

State responsibility in cyberspace rather than a stand-alone idea.[4]

The implications of a state committing an internationally unlawful conduct are addressed under the law of state liability. These secondary principles are codified in ARSIWA, which was endorsed by the International Law Commission in 2001. "Every internationally wrongful act of a State entails the international responsibility of that State," according to Article (1). [5] What constitutes a "internationally wrongful act" is:

(a) a violation of a fundamental legal principle (an international commitment), and (b) actions attributed to the State.[6]

3.1.1. Attribution of State Organs

According to Article (4) of ARSIWA, "The conduct of any State organ shall be considered an act of that State under international law." This is the fundamental attribution norm.[7] Stated differently, the State is automatically bound worldwide by any action taken by a government department, agency, or person, whether it be legislative, executive, judicial, or otherwise. In a similar vein, a State is responsible for choices or actions that are acknowledged such as by its own legislation. Therefore, it is assumed that state responsibility is incurred by the actions of state organs, even if they are beyond their authority.[8]

3.1.2. Attribution of Non-State Actors

Non-state actors are covered by ARSIWA if they follow directives or are governed by a state. It is possible to link a state to hackers or terrorists operating through proxies, but the state's involvement must be significant and direct; ideological or indirect support is insufficient.[9]

3.1.3. The Relationship Between Attribution and Wrongfulness

According to Article 2 of ARSIWA, a state's behavior, whether action or omission, in violation of a binding international rule" constitutes a breach of an international responsibility. Therefore, a State bears responsibility in the context of cyberspace when it transgresses duties such as sovereignty, non-intervention, or the UN Charter's ban on using force. An "internationally wrongful act in the cyber context is a cyber-related action or omission that constitutes a breach of an international legal obligation … and is attributable to a State," according to Canada's position paper, supports this definition.[10]

In conclusion, cyber activities are subject to the same broad framework of the Articles on the Responsibility of States for Internationally Wrongful Acts (ARSIWA) such as any other type of behaviour. Finding an internationally broken obligation and proving a strong enough connection between the behaviour in issue and the State, whether via the activities of its organs or behaviour attributable to it due to control are necessary for the analysis.[11]

3.2. Attribution: Legal vs. Technical vs. Political

Three layers are often used to understand attribution in cyberspace. Technical attribution is the process of using forensic investigation to determine the origin of a cyber activity. When a State openly places blame on another State or person, this is known as political attribution. Legal attribution, on the other hand, is the process by which a State engages its duty under ARSIWA by determining that the action is traceable to it under international law.[12] Importantly, ARSIWA's requirements for legal attribution must be met; technical and political attributions do not always match these requirements. In order to attribute illegal behaviour in cyberspace, Canada "applies the customary international law on State responsibility to attribute," which entails identifying the accountable State legally.[13] According to the legislation, the victim State must nevertheless confirm that the attacker was operating such as a state organ or under State direction in order

[4] TALLINN MANUAL2.0 ONTHE INTERNATIONAL LAWAPPLICABLE TOCYBEROPERATIONS, 80-84

[5] International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*, (2001), Yearbook of the International Law Commission, Vol. II, Part 2, 40-41.

[6] Government of Canada, *International Law applicable in cyberspace*, (Global Affairs Canada, 10 April 2022), https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng, accessed 4 February 2026.

[7] Ibid, 40.

[8] Ibid, 41-45.

[9] International Law Commission (ILC), *Draft Articles*, above, 47-48.

International Law Commission (ILC), *Draft Articles*, above, 34-35.

[11] League of Nations, *Conference for the Codification of International Law, (The Hague, 1930)*, cited in Yearbook of the International Law Commission (1956) vol II, 225, UN Doc A/CN.4/96, annex 3, art 1.

[12] Government of Canada (n 5).

[13] International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts* (2001) UN Doc A/56/10, arts 17–18.

to hold that State globally liable, even if intelligence identifies the attacker.[14]

On the other hand, a State is not required to provide a public attribution only because it complies with ARSIWA's attribution requirements. According to the Canadian stance, states "bear no obligation to publicly provide the basis for their attribution, and public attribution of an internationally wrongful act engages various political considerations.[15] In reality, many states exchange intelligence with allies or carry out private investigations, although they are cautious about disclosing sensitive material. Currently, there is "little international law of cyber attribution, and what law there is exists largely by implication," according to one researcher.[16] To put it briefly, legal attribution is a high hurdle; many States will not use ARSIWA if the proof of State participation is somewhat circumstantial or unclear.

Politically, attribution is also very important. Even if a victim State decides not to make the supporting facts publicly available, it must be convinced that it has a strong legal foundation on which to react, whether through self-defence or countermeasures. According to Germany's position document, before responding, a state should try to make attribution and state responsibility more clear. In this regard, legitimate countermeasures require explicit attribution, at least internally.[17]

3.3. Challenges of Cyber Attribution

There are legal and technical obstacles to attribution in cyberspace. Attackers can deploy worldwide botnets, conceal their activities across jurisdictions, or take use of credentials that have been stolen. Due to private company logs or sensitive intelligence, forensic evidence may be incomplete and difficult to collect. States are forced to rely on alliance agreement or internal criteria because to the lack of clarity surrounding international evidentiary requirements. The situation is made more difficult by jurisdictional concerns, particularly when servers and attackers are located in different states. Remedial measures for state-to-state cyberattacks include ICJ proceedings, diplomacy, or penalties; however, ARSIWA requires reliable proof. Additionally, conventional notions of injury and sovereignty are blurred in cyberspace. However, Japan points out to invoke State responsibility... it is necessary to consider whether the act is attributable to a specific State." ARSIWA is still the framework.[18]

The level of proof necessary for attribution is one of the most important legal issues. Effective control or direction is required by international jurisprudence, especially under ARSIWA Article 8, which establishes a high standard of proof. However, because cyberspace operations are sophisticated, such proof is rarely available. Because of this, a lot of states rely on circumstantial evidence, which begs the question of whether current legal standards are sufficient in cyber situations.[19]

3.4. International Legal Debates on Cyber Attribution

There has been much discussion over the applicability of ARSIWA to internet. The standard of proof is one important concern. Cyber activities seldom produce the "clear and convincing evidence" that traditional international law demands (Nicaragua case). In 2021,[20] Germany demands "reliable factual grounds," whereas France demands "sufficient evidence." "There is no settled practice regarding the standard of proof," according to the Tallinn Manual 2.0.[21]

A second debate concerns the degree of State control required under article 8. The ICJ in Nicaragua required "effective control" over specific operations, while the ICTY in Tadić adopted "overall control" over the group.[22] Canada and France favour the stricter Nicaragua standard, but scholars argue the overall control test may be more suitable for cyberspace where States direct proxies without micromanaging operations.

Third, due diligence has emerged as an alternative basis for responsibility.[23] Germany notes that States may be responsible for operations emanating from their territory if they knowingly fail to act. This

[14] International Law Commission (n 4) art 8.
[15] Government of Canada (n 5).
[16] William C Banks (n 3), 1040, 1067.
[17] Federal Government of Germany, *On the Application of International Law in Cyberspace*, (Position Paper, March 2021), 13-14.
[18] Ministry of Foreign Affairs of Japan, *Basic Position of the Government of Japan on International Law Applicable to Cyber Operations*, (28 May 2021), p.4-6.
[19] Tallinn Manual 2.0 (n 1) rule 17, 95.
[20] Jeremy K. Davis, *Developing Applicable Standards of Proof for Peacetime Cyber Attribution*, Tallinn Paper No. 13 (2022), 16
[21] Tareq Al-Billeh, Jessica Al-Mudanat, Abdulaziz Almamari, Tawfiq Khashashneh and Odai Al-Hailat, The International Framework for Cyber-Attacks Under the Rules of International Humanitarian Law, (2025) 5(2) Journal of Human Rights, Culture and Legal System, 426.
[22] Collin S. Allan, *Attribution Issues in Cyberspace*, 13 Chi.-Kent J. Int'l & Comp. Law 55 (2013), 68.
[23] Jeremy K. Davis, *Developing Applicable Standards of Proof for Peacetime Cyber Attribution, (n20), 13.*

lowers the evidentiary burden, though its precise contours remain unsettled.[24]

4. BACKGROUND OF GCC CYBERSECURITY APPROACHES

Though they have not made clear international duty, GCC states have established cybersecurity agencies and policies that concentrate on infrastructure protection, cybercrime, and national defence. Regarding international law in cyberspace, none have released a formal stance.

Saudi Arabia's National Cybersecurity Authority and Strategy focus on national resilience, legal frameworks, and public–private cooperation, but do not address international law or holding other states accountable for cross-border cyber incidents.[25]

With an emphasis on domestic enforcement, the UAE has created national cybersecurity authorities and passed cybercrime legislation. The way the ARSIWA attribution standards apply to foreign cyberattacks is not made clear by UAE remarks in international forums, despite the fact that they urge responsible state action under international law.[26]

Qatar's 2014 National Cyber Security Strategy focuses on defending the country from large-scale cyberattacks and aims to establish a legal and regulatory framework for cyberspace. It emphasizes diplomacy, participation in forming international rules, and using military, intelligence, and security resources for cyber defence. However, the strategy does not specify how international law applies.[27] In practice, during the May 2017 Qatar News Agency hack, the government treated the incident such as a domestic cybercrime, investigating and condemning it without attributing legal responsibility to any other state, even though the attack had significant international implications.[28]

National cybersecurity organizations and regulations that safeguard networks and penalize hackers are also in place in Bahrain, Kuwait, and Oman. None of these governments have made public the ways in which international law restricts state behaviour in cyberspace, despite the fact that these frameworks concentrate on domestic protection and enforcement. Unlike nations like France and Canada, none of the GCC have released a written "cyber doctrine" that explains when a cyberattack would be considered an internationally unlawful conduct. To date, official GCC pronouncements on cyber responsibility have focused more on political context and particular occurrences than on legal requirements.[29]

Saudi Aramco and Sadara were the targets of the Shamoon malware assaults in 2012 and 2016, which caused significant disruption without causing physical harm and erased thousands of machines. Saudi Arabia concentrated on repairing networks, improving cybersecurity, and bringing inside collaborators to justice after the incident, which was widely ascribed to an Iranian outfit. At the UN, neither self-defence nor an official call for Iran to be held accountable under international law were made. Because reactions to these attacks have relied on internal measures rather than formal international legal action, they emphasize the region's cyber vulnerability and the lack of legal responsibility.[30] From the standpoint of attribution, the Shamoon assaults highlight how challenging it is to satisfy Article 8's "effective control" requirement. Technical attribution to Iranian actors would not meet legal attribution criteria without evidence of State direction, and the deployment of malware that could be obtained by different actors produced plausible deniability.

False comments were aired during the 2017, hack of the Qatar News Agency, sparking a global crisis. Without explicitly blaming any state, Qatar conducted a lawful investigation into the event, treating it such as a local cybercrime. Although no GCC government pursued the issue via international legal procedures, neighboring nations severed their links with Qatar, suggesting state-sponsored participation. The case demonstrates the region's inclination toward political and diplomatic solutions rather than relying on international cyber law or ARSIWA.[31] The difficulty of identifying information

[24] Federal Government of Germany, *On the Application of International Law in Cyberspace, (n2), 3.*
[25] National Cybersecurity Authority, *National Cybersecurity Strategy*, https://nca.gov.sa/en/national-cybersecurity-strategy/ , accessed 8 February 2026.
[26] Permanent Mission of the United Arab Emirates to the United Nations, 'Peace and Security: Addressing Evolving Threats in Cyberspace' (20 June 2024) https://uaeun.org/statement/unsc-uae-threats-in-cyberspace-20june/ accessed 4 February 2026.
[27] Ministry of Foreign Affairs of Qatar, 'Foreign Minister: Qatar Will Address the Media Campaign Targeting It' (25 May 2017) https://mofa.gov.qa/en/qatar/latest-articles/latest-news/details/2017/05/25/foreign-minister-%27qatar-will-address-the-media-campaign-targeting-it%27 accessed 4 February 2026.
[28] Qatar National Cyber Security Strategy, (MAY 2014), 6-10
[29] Ibid.
[30] Zakariya. D, Norah. A, Saudi Arabia's Response to Cyber Conflict: A case study of the Shamoon malware incident, (Information School University of Washington Seattle, 2013), 73-74.
[31] Ministry of Foreign Affairs of Qatar (n 20).

operations under ARSIWA is brought to light by the breach of the Qatar News Agency. Legal attribution necessitates proof of State direction or control, even in cases where political context points to State involvement. Content-based assaults may find it difficult to fulfill this standard. Victim States are left without clear legal redress due to the GCC's lack of stated stances on such activities.

Every GCC state has national plans and cybercrime legislation that prioritize domestic defence and enforcement, acknowledging the dangers posed by cyberspace. None have formally adopted shared rules outside of UN procedures or provided guidelines on how ARSIWA relates to cyber operations. Because of this, GCC states frequently resort to diplomatic or local remedies instead of explicit international law regulations when cyber events involving states or proxies occur, posing serious legal issues.

A larger structural constraint in the GCC States' interaction with international cyber law is shown in the lack of clear legal stances. Responses to cyber events in the GCC are still mostly reactive and locally focused, in contrast to Western States. This strategy restricts their power to influence new standards and erodes their capacity to assert international responsibility. As a result, in the developing field of cyber attribution, the GCC runs the danger of continuing to be norm-takers rather than norm-makers.

5. LEGAL CHALLENGES

5.1. Technical Attribution and Evidence

There are significant legal and technological obstacles to cyber-attribution. It can be challenging to link assaults to a state since attackers can conceal their activities via global botnets, spoofing, or anonymous networks. Logs, virus signatures, and IP data are examples of fragmented evidence that could not satisfy legal requirements. Clear attribution and evidence of a breach are necessary for state liability under ARSIWA; however, confidential intelligence, disparate technological standards, and secrecy make it difficult to translate technical discoveries into legal proof, making many allegations political rather than judicial.

Canada distinguishes between legal attribution and technical or political attribution in cyberspace. [32] While technical attribution identifies who carried out a cyber operation, legal attribution requires linking the act to state instruction or control.[33] Even when legal attribution is established privately, a state is not obliged to make all evidence public. This creates a dilemma: sufficient evidence must often be collected secretly, yet the victim state need not reveal it. In practice, most attributions occur through diplomatic statements rather than formal legal proceedings.[34] In the GCC, the lack of agreed diplomatic channels for cyber claims makes it extremely difficult for victims to prove in court that another state conducted the operation.[35]

5.2. Jurisdiction and Enforcement

Even when attribution of a cyberattack is successfully established, significant jurisdictional challenges remain. Cyber operations often cross multiple borders: the perpetrators may reside in State A, route their attacks through servers in State B, and target victims in State C.[36] This raises the question of which State possesses legal jurisdiction over the incident. Traditionally, criminal prosecutions for hacking rely on principles such as nationality, territoriality, or international cybercrime treaties, including the Budapest Convention. However, these frameworks are generally designed to address individual perpetrators, rather than acts conducted or sponsored by States.[37]

If it is alleged that State A, orchestrated or facilitated an attack from its territory against State C, the latter could theoretically pursue a diplomatic claim or bring a case before the International Court of

[32] Nicholas Tsagourias, 'Cyber Attacks, Self- Defence and the Problem of Attribution' (2012) 17 Journal of Conflict and Security Law, 229, 234–236.

[33] John S Davis and others, 'Stateless Attribution: Toward International Accountability in Cyberspace' (RAND Corporation 2017) 11–12 accessed 6 February 2026

[34] David A Wheeler and Gregory N Larsen, 'Techniques for Cyber Attack Attribution' (Institute for Defence Analysis 2003) P-3972 A-1.

[35] Brian J Egan, 'International Law and Stability in Cyberspace' (2017) 35 *Berkeley Journal of International Law* 169, 177; Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, Cambridge University Press 2017) 83; John S Davis and others, 'Stateless Attribution: Towards International Accountability in Cyberspace' (RAND Corporation 2017) 22 https://www.rand.org/pubs/research_reports/RR1986.html accessed 5 February 2026.

[36] UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, *Report* (2021) UN Doc A/76/135, 29–30, 42–46.

[37] Government of Canada, 'International Law Applicable in Cyberspace' (Global Affairs Canada, 10 April 2022) <https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng> accessed 7 February.

Justice (ICJ) for breach of sovereignty.[38] Such actions, however, require the consent of the concerned States or the existence of an applicable treaty, and multilateral forums like the UN Security Council are often influenced by political considerations. Currently, there is no dedicated enforcement mechanism for addressing internationally wrongful cyber acts.[39]

In practice, and in the absence of bilateral agreements, the most feasible remedy for an injured State consists of countermeasures, including sanctions or diplomatic pressure. Even in these cases, however, the injured State must comply with the conditions set forth in the Articles on the Responsibility of States for Internationally Wrongful Acts (ARSIWA) to ensure that any response is lawful. Consequently, the combination of legal uncertainty and the absence of compulsory dispute resolution mechanisms means that even clear instances of State-backed cyber aggression may remain unremedied from a legal perspective.

According to the due diligence concept, states must not willfully let activities that endanger other states to take place on their territory.[40] States are required by ARSIWA and fundamental principles to stop wrongdoing by private individuals, including cybercriminals. A state may be held accountable if it disregards reliable warnings concerning assailants within its boundaries.[41] Due diligence is inferred by sovereignty and non-intervention, even if ARSIWA does not expressly codify it.[42] The ILC further points out that a State cannot use a non-state actor argument if it does nothing. In reality, states seldom ever acknowledge responsibility without unambiguous proof of agreement, so victims can place political blame but are unable to enforce legal action.[43]

5.3. Application of ARSIWA to Cyberspace

The application of ARSIWA in cyberspace calls into question whether, namely sovereignty, non-intervention, and the prohibition of the use of force, are violations of a state's responsibilities. These duties might be broken by a cyberattack that interferes with government operations or damages vital infrastructure. While France points out that cyber operations that are similar to kinetic assaults in effect might be considered the use of force, Canada and Japan declare that sovereignty and non-intervention apply online. While serious activities, like cutting off another State's electrical infrastructure for days, might establish liability and need countermeasures, minor crimes, like espionage or data theft, are often below ARSIWA's breach threshold.[44]

The burden of evidence in cyberspace is high under ARSIWA.[45] According to the Nicaraguan ICJ, attribution necessitates demonstrating that a proxy acted in accordance with a State's "instructions or control.[46]

Tribunals often need concrete proof of government participation; technical signs alone are rarely enough.[47] Because facts in cyber disputes are sometimes less specific and more difficult to confirm, they are significantly more difficult.[48]

States are subject to legal duties once attribution is established under ARSIWA. While Article (31) requires complete reparations, which in the context of cyberspace may include reparatory punishments or guarantees against recurrent incursions, Article (30) calls for cessation and promises of non-repetition. Under Article (49), victims may take appropriate actions without resorting to force, such as ICT limitations or diplomatic expulsions. Cyber reactions cannot, however, be considered unlawful force in and of themselves such as countermeasures cannot contravene peremptory rules or amount to retaliation in kind. In reality, this legal framework is not frequently used in the (GCC), as official legal countermeasures are frequently replaced by unilateral political or economic actions, such as travel restrictions or media campaigns.[49]

---

[38] Michael N Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2nd edn, Cambridge University Press 2017) 20, para 10, hereinafter Tallinn Manual 2.0.
[39] Government of Canada (n 5).
[40] UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 'Report of the Group of Governmental Experts' (22 July 2015) UN Doc A/70/174, 12–13.
[41] Secrétariat général de la défense et de la sécurité nationale (SGDSN), *Strategic Review of Cyber Defence* (2018) annex 7, 159.
[42] UN Group of Governmental Experts (n 32) 27–28.
[43]France, *International Law Applied to Operations in Cyberspace, n(1),* 9
[44] Ministry of Foreign Affairs of Japan, *Basic Position of the Government of Japan on International Law Applicable to Cyber Operations, n(y17),* 1-6.
[45] International Law Commission (n 4), 34.
International Law Commission (n 4), 47.
[47] International Law Commission, International Law Commission (n 4), 48
[48] International Law Commission (n 4), 72.
[49] Government of Canada (n 5).

5.4. Comparative Practice: France, Germany, Canada, Japan

A number of Western states have explicitly stated how they interpret ARSIWA in relation to cyberspace. Canada's 2019 statement emphasizes that states cannot avoid accountability by operating through proxies and confirms that the law of State responsibility fully applies in cyberspace.(50) Similarly, Germany's 2021 position statement affirms that the concept of State responsibility and other current customary international law are unquestionably applicable online. Germany specifically uses Article (8) of the ARSIWA's attribution standards such as the benchmark for assessing State accountability in cyber activities.(51)

In line with ARSIWA, France takes a conventional stance in its 2021 report to the UN OEWG. It confirms that, in accordance with Article 8, State accountability for non-state actors' actions only emerges when such actors act under a state's directives or effective control. In line with established ICJ reasoning, France likewise argues that attacks carried out exclusively by independent non-state actors are not covered by the right to self-defence. In general, France has a constant dedication to implementing ARSIWA without establishing unique exclusions for online, much like Canada and Germany do.(52)

Western States have different priorities even if they all use ARSIWA in the cyber domain.(53) While France emphasizes stringent evidence criteria and views public attribution such as a political decision, Canada places a greater emphasis on sovereignty and does not consider minor incursions to be breaches.(54) Japan specifically cites ARSIWA Articles (4–8) for credit,(55) whereas Germany emphasizes the necessity of reliable factual basis. Although these States believe that current international law is enough, the GCC States have not expressed similar views, hence they are forced to depend on broad guidelines without specific national directives.

Even though Western States seem to agree that ARSIWA is applicable, there are still notable differences in how they actually handle attribution. For example, Canada stresses sovereignty without specifying thresholds for transgressions, but France uses a careful evidential approach. Japan has a more formal doctrinal approach, whereas Germany concentrates on factual certainty. This discrepancy emphasizes the lack of a common standard of proof for cyber attribution, which erodes legal certainty and strengthens states' propensity to use political attribution rather than legal attribution. GCC States, on the other hand, are at a structural disadvantage when it comes to asserting state accountability since they not only lack common norms but also lack clearly stated stances.[56]

6. RECOMMENDATIONS

The GCC states should take the following actions to enhance and clarify the legal framework for state accountability and cyber attribution in order to fill up the gaps mentioned above:

- Clearly state national legal stances. Every GCC nation and preferably the GCC bloc as a whole ought to formulate and make public its position on the application of international law to cyber activities. This might be a joint GCC proclamation, a White document, or a government position document. International commitments, such as sovereignty, non-intervention, UN Charter, etc. Should be confirmed in the document. Apply online and describe how their national practice would apply ARSIWA's attribution guidelines (Articles 4–8). For instance, "participating in the formation of international rules" is already included in Qatar's cyber policy; the country may expand on this by outlining the standards it anticipates. The UAE or Saudi Arabia might also make public their threshold for "use of force" or "armed attack" in cyberspace. Having a definite stance would help decision-makers and let others know that the State is ready to take legal action if needed. According to one expert, states ought to encourage public attribution and specify "what legal or evidentiary standards must be met" in order to allocate accountability. A sensible first step in achieving that objective is to draft a national position document.

(50) Khalifa ALKUWARI, Collective Countermeasures and Regional Cooperation: Strengthening Cybersecurity in Qatar and the Gulf Cooperation Council, (PhD thesis, University of Bradford 2025), p.31-32.
(51) Federal Government of Germany (n 16), 1-11
(52) France, *International Law Applied to Operations in Cyberspace, (n 1) 6–9.*
(53) Canada, International Law applicable in cyberspace, above.
(54) France, *International Law Applied to Operations in Cyberspace, (n 1),* 8-9.
(55) Ministry of Foreign Affairs of Japan (n 17) 4.
56 Abhijeet Shrivastava, Error 404, Responsibility Not Found? Evidentiary Dilemmas in Attributing Cyber Operations, (Opinio Juris, 24 August 2022)
https://opiniojuris.org/2022/08/24/error-404-responsibility-not-found-evidentiary-dilemmas-in-attributing cyber-operations, accessed 22 feb, 2026

- Create a model declaration and harmonize geographically. As a regional body, the GCC might support a unified stance on cyber standards, similar to the Arab League's stance on some global problems. A GCC-wide agreement might improve bargaining leverage in multilateral forums and guarantee uniformity, avoid "friendly fire" or blame games. This agreement may bind the member governments to refrain from sheltering cybercriminal proxies, share technical evidence, and support one another in cyber attribution investigations. A GCC Model Cyber Norms Declaration, which would outline consultation processes for cyber incidents and indicate when a cyber event among them would be considered a breach of international law, is one workable suggestion. Additionally, any future cybersecurity pact or cooperation mechanism including the whole area would be easier to execute with this harmonization.
- Participate actively in global forums. Every GCC state ought to take an active role in multilateral and UN procedures, such as the OEWG on responsible state behaviour in cyberspace and the UN GGE. By participating, they may influence international standards to take into account local security issues. They should also take note of other people's experiences. A few years ago, Canada and Japan took formal stances; the GCC states may follow suit. Capacity might potentially be increased by collaboration with like-minded governments (perhaps through coalitions of willing). Building a common understanding of cyber-law is crucial for avoiding misconceptions, such as the Canadian declaration points out.
- Build the ability to gather and disseminate evidence. Technical and legal capacities must advance in order to finally hold states accountable. The GCC may spend money on legal avenues (such mutual legal aid treaties) and cyber-forensics laboratories dedicated to cyber evidence. Having strong protocols to track assaults and preserve data will make any future legal attribution plausible, even if it is not strictly a legal change. This might involve using the multi-state Tallinn Manual 2.0, such as a legal reference, while it offers authoritative counsel, it has no binding force or doing cooperative training with friendly countries.
- Be ready for multilateral reactions and countermeasures. A GCC state should be prepared to respond in accordance with international law in the event of a globally unlawful cyber conduct. This entails using countermeasures in accordance with ARSIWA's guidelines, which state that they must be reasonable, reversible, and free from unlawful force, among other requirements. When a member is attacked, the region may even consider setting up a permanent investigation mechanism, perhaps at a GCC cyber center to gather information. This might give any allegation more credibility. A declaratory rule or UN-backed standards on state commitments have also been supported by some experts. For instance, a UN General Assembly resolution on cyber norms that GCC states may accept. The area would benefit from at least investing in clarity on countermeasures, such as what constitutes acceptable retaliation in cyberspace in the absence of new accords.

In general, the GCC shouldn't let cyberattacks be seen as merely criminal or security problems. The GCC should provide legal clarification because sophisticated cyber activities are common. A "viable cyber attribution regime" is currently lacking, according to academic observers like Banks, who urge nations to enact attribution laws. Accordingly, the GCC may be the first to create a GCC Model Declaration on Responsible State Behaviour in Cyberspace or a regional framework. This declaration, which was written by legal experts from the member states, may specify that each member respects cyberspace sovereignty and accepts responsibility for cyberattacks that originate on its territory or under its control. Practically speaking, it may be similar to current voluntary standards, such the 2015 UN standards, but it would have legal power, at least in the area. Developing such a model will also get GCC states ready for any future developments in international treaties or customary law.

7. CONCLUSION

Cyber occurrences in the Gulf area, such as the political hack of the Qatari news agency or the Shamoon assaults on Saudi energy infrastructure, show how new technology puts pressure on established international law. There is currently no clear legal definition in the GCC regarding when state accountability is triggered by a cyber operation. The general law of state responsibility, or ARSIWA, is theoretically applicable in cyberspace in the same way as it is on land or at sea. However, instead of using that legislation, victims in the GCC frequently accept diplomatic protest and technological remedy. Because victims lack a clear policy or evidentiary trail, cyber-aggressors might avoid direct legal

repercussions, which leads to an accountability gap.

In contrast, nations such as Canada, Japan, France, and Germany have officially stated that cyber activities are governed by international law and have started to define their own interpretations of that law. None of these governments assert a legal "cyber exception" to state accountability; instead, they all depend on ARSIWA's attribution guidelines. This approach has lessons for the GCC. According to our study, the GCC states would gain by creating their own legal stances on the application of sovereignty, due diligence, and state accountability to cyber acts, both nationally and in a standardized regional format. This would help control expectations for when countermeasures or UN responses are warranted, in addition to strengthening deterrence, by guaranteeing legal accountability.

In conclusion, one of the Gulf's most important tasks is to make clear the law of state accountability in cyberspace. Recent events highlight the value of both technical security and legal clarity. As a workable solution, the GCC may demonstrate its commitment to the rule of law in cyberspace by issuing a model declaration on cyber standards. Such a statement would assert, for instance, that states must not intentionally permit cyberattacks to occur on their territory, repeating ARSIWA Articles (4–8) and that cyberattacks that cause substantial injury are an infringement on territorial sovereignty. The statement may also obligate the governments to cooperate in the investigation of claims and to uphold the values of the UN Charter on the internet. In other words, even if technology is developing quickly, the fundamental idea that states are still accountable for wrongdoing in cyberspace must not be forgotten. To the cost of everyone, the GCC runs the prospect of ongoing uncertainty if a cyber conflict breaks without prompt action.

BIBLIOGRAPHY

International Materials

Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries, UN Doc A/56/10 (2001), Yearbook of the International Law Commission, 2001, vol II, Part Two.

Khalifa Alkuwari, *Collective Countermeasures and Regional Cooperation*, Strengthening Cybersecurity in Qatar and the Gulf Cooperation Council, (PhD thesis, University of Bradford 2025).

League of Nations, *Conference for the Codification of International Law*, The Hague, 1930, in Yearbook of the International Law Commission, 1956, vol II, p 225, UN Doc A/CN.4/96, Annex 3.

Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc A/70/174 (22 July 2015).

Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, UN Doc A/76/135 (14 July 2021).

Books and Edited Collections

Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, Cambridge University Press 2017).

SGDSN, *Strategic Review of Cyber defence* (2018), Annex 7.

Journal Articles

William C Banks, 'Cyber Attribution and State Responsibility' (2021) 97 International Law 1040.

Brian J Egan, 'International Law and Stability in Cyberspace' (2017) 35 Berkeley Journal of International Law 169.

Nicholas Tsagourias, 'Cyber Attacks, self-defence and the Problem of Attribution' (2012) 17 Journal of Conflict and Security Law 229.

Online Sources and Government Documents

Canada, *International Law Applicable in Cyberspace* (Global Affairs Canada, 10 April 2022) https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng

David A Wheeler and Gregory N Larsen, 'Techniques for Cyber Attack Attribution' (Institute for Defence Analysis 2003) P-3972 A-1.

Federal Government of Germany, *On the Application of International Law in Cyberspace* (Position Paper, March 2021).

France, *International Law Applied to Operations in Cyberspace* (2021).

Japan, Ministry of Foreign Affairs, *Basic Position of the Government of Japan on International Law Applicable to Cyber Operations* (28 May 2021).

John S Davis and others, *Stateless Attribution: Toward International Accountability in Cyberspace* (RAND Corporation 2017).

David A Wheeler and Gregory N Larsen, *Techniques for Cyber Attack Attribution* (Institute for Defence Analysis 2003) P-3972.

National Cybersecurity Authority (Saudi Arabia), *National Cybersecurity Strategy* https://nca.gov.sa/en/national-cybersecurity-strategy/ accessed 10 February 2026.

Permanent Mission of the United Arab Emirates to the United Nations, *Peace and Security: Addressing Evolving Threats in Cyberspace* (20 June 2024) https://uaeun.org/statement/unsc-uae-threats-in-cyberspace-20june/ accessed 6 February 2026.

Qatar, *Qatar National Cyber Security Strategy* (May 2014).

Qatar, Ministry of Foreign Affairs, 'Foreign Minister: "Qatar Will Address the Media Campaign Targeting It"' (25 May 2017) https://mofa.gov.qa/en/qatar/latest-articles/latest-news/details/2017/05/25/foreign-minister-%27qatar-will-address-the-media-campaign-targeting-it%27 accessed 4 February 2026.

Zakariya D and Norah A, *Saudi Arabia's Response to Cyber Conflict: A Case Study of the Shamoon Malware Incident* (Information School, University of Washington, Seattle, USA, 2013).