

International Law and Transnational Cyber Operations: Sovereignty, State Responsibility, Attribution and Use of Force

Muhammad Faizan Zahid¹

Muhammad Yousaf Raza²

¹ Glasgow Caledonian University, Scotland, United Kingdom: Email: muhammadfaizanzahid2000@gmail.com

ORCID <https://orcid.org/0009-0005-7295-3059>

² Glasgow Caledonian University, Scotland, United Kingdom: Email: Iusafch47@gmail.com

ABSTRACT

Cross-border cyber operations raise a number of challenging legal questions, including sovereignty, non-intervention, the prohibition on the use of force, self-defence, attribution and State responsibility. The basic argument of this article is that existing international law does apply to State conduct in cyberspace, although there is still significant disagreement on how particular rules and thresholds should operate in practice. The present study uses a doctrinal and comparative approach, examining the UN Charter, the law of State responsibility, relevant decisions of the International Court of Justice, UN cyber-process documents, the Tallinn Manuals and the publicly stated positions of the United Kingdom, Australia, Canada, India and Pakistan. The principal problem, therefore, is not the absence of law in cyberspace. And that it is hard to apply existing rules to technically complicated and sometimes deliberately concealed operations. The article distinguishes between three levels of analysis: the primary rules that determine the legality of an operation, the secondary rules that govern attribution and legal consequences, and voluntary norms and confidence-building measures that promote responsible behaviour without being binding law in themselves. It suggests that significant adverse effects and interferences with inherently governmental functions provide a better basis for a sovereignty analysis than either treating every remote intrusion as unlawful or saying that sovereignty has no independent relevance. Coercion remains important for non-intervention, whilst thresholds for use of force and armed attack should be carefully assessed looking at scale and effects. The article also supports a cautious approach to attribution based on evidence and does not consider due diligence as a general stand-alone cyber rule without adequate support in State practice and *opinio juris*. The comparison indicates that States generally agree that existing international law applies to cyberspace, but continue to differ on a number of important details. Instead of assuming that a new comprehensive cyber treaty is immediately needed, the article therefore concentrates on clearer national legal positions, better attribution procedures and practical implementation of existing rules.

ARTICLE HISTORY

Received **01-07-2026**
Accepted **11-09-2026**
Published **10-10-2026**

KEYWORDS

Cyber operations; international law; sovereignty; non-intervention; use of force; self-defence; attribution; State responsibility; due diligence; Tallinn Manual

CORRESPONDING AUTHOR

Muhammad Faizan Zahid
muhammadfaizanzahid2000@gmail.com

CC BY-NC 4.0 © 2026 The Author(s). Published by JuriSocial Research Center Private Limited. This is an open access article distributed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International Licence (<https://creativecommons.org/licenses/by-nc/4.0/>), which permits non-commercial use, distribution and reproduction in any medium, provided the original work is properly cited.



<https://doi.org/10.68740/jjss24>

1. Introduction

States are now routinely using cyber operations for intelligence gathering, disruption, strategic competition, and other purposes. Unlike traditional military or government activity, a cyber operation can be conducted remotely, routed through other States and masked behind compromised computers or networks. It is thus able to have an effect in another country without the operator being physically present there. These features pose hard questions for an international legal system that has traditionally dealt with territory and more visible forms of State conduct. It would be wrong, however, to suggest that there is a total legal vacuum. The Charter of the United Nations, customary international law and the law of State responsibility already contain rules which can apply to State conduct in cyberspace. The more difficult question is how precisely to apply those rules where the technical facts are complex and the evidence available may be incomplete.

The central problem of research is therefore the application and explanation of the existing law and not the creation of an entirely new body of law. The 2013 and 2015 UN Groups of Governmental Experts and the 2021 UN processes, as well as subsequent UN work, have recognised that existing international law is applicable to State conduct involving information and communications technologies. But this general agreement does not resolve all questions. It does not tell us exactly when a remote intrusion is in violation of sovereignty, when a cyber operation constitutes coercive intervention, what level of effects makes a use of force or an armed attack, or what evidence is sufficient to attribute an operation to a State and take action in response. The present article thus attempts to apply the existing rules without suggesting disputed academic arguments as if settled law.

The article distinguishes three methodological basic differences. It first distinguishes primary rules from secondary rules of State responsibility and from voluntary norms concerning responsible State behaviour. Second, it dissociates legal attribution from political attribution. Sometimes intelligence is enough to allow a government to publicly blame another State, but that does not necessarily answer every evidentiary question that would arise before a court or tribunal. Thirdly, public legal positions of States are treated as evidence of State views and practice, but not as a matter of course as customary international law. These distinctions are important because cyber policy documents often blend legal rules with strategic policy and operational guidance.

The comparison of the United Kingdom, Australia, Canada, India and Pakistan is to see how these States deal with the same legal questions. Relatively detailed material on international law and cyberspace has been issued by the United Kingdom, Australia and Canada. India has also become more public about its military cyber doctrine and Pakistan has released a national cyber-security policy and a position on international law in cyberspace in 2023. This comparison does not mean that these countries have the same legal systems, or that cooperation among certain states constitutes international law. It therefore examines what each state has said in public, how unambiguous it has been in expressing its position and the institutional context in which that position emerges.

Cyber incidents are good illustrations of the legal debate, but an incident alone does not make a legal rule. Estonia in 2007, Stuxnet, WannaCry, NotPetya and SolarWinds demonstrate that the effects of cyber operations range from espionage and disruption to physical damage and supply-chain compromise. The public statements blaming specific States also demonstrate why political attribution and legal responsibility should not be conflated. Hence these incidents are here used primarily as illustrations rather than as proof of legally established state responsibility.

Where cyber operations impact journalists, personal data or civilian infrastructure, human rights, data protection and cybercrime law might also be applicable. But they are not the main focus of this article. The present study deals with the legal relationship between States: is a State's conduct in conformity with international law, can a State's conduct be attributed to it and what are the international legal consequences of such conduct if another State is injured by it?

1.1 Research Question, Objectives, Scope and Method

The main research question is: How should existing international law regulate State sponsored cyber operations impacting another State? The study aims at several objectives. It discusses the UN understanding that existing international law applies in cyberspace; disentangles sovereignty from non-intervention and from the prohibition on the use of force; considers attribution and State responsibility; considers the uncertain position of due diligence. It explains the legal status of the Tallinn Manuals; compares the public positions of five States; and develops a cautious way of applying existing rules to cross border cyber operations. The research is doctrinal and comparative. Its main sources are treaties, ICJ judgements, ILC materials, UN reports, official national legal positions and selected official policy documents, and relevant peer-reviewed scholarship. It does not purport to establish customary international law by a statistical study of cyber incidents, nor does it use confidential operational information.

The comparative part of the study works with five main criteria. These are: (1) whether the State explicitly accepts that existing international law applies; (2) how it approaches sovereignty; (3) how it explains non-intervention, the use of force and self-defence; (4) how it approaches attribution, State responsibility and due diligence; and (5) how transparent its public legal position is and where that position comes from institutionally. This comparison is thus more than a simple description of five countries. But the method has its obvious limits. Public documents cannot prove classified State practice and different wording does not necessarily mean that States hold different views on customary international law.

2. International legal framework and the UN Consensus

The UN cyber process is a good first step. The 2013 GGE report noted that international law, including the UN Charter, applies to State conduct in cyberspace. This was restated in the 2015 GGE, which also cited the Charter and other established principles. The 2021 GGE report and the 2021 OEWG process similarly treated existing international law as applicable while recognising the need for further common understandings about how it should be applied (United Nations General Assembly, 2013, 2015, 2021a, 2021b). These developments constitute important evidence of broad intergovernmental consensus, but do not by themselves resolve all contested questions of customary international law.

Developments following the 2021 UN processes are also relevant. The UN Global Mechanism on developments in the area of ICTs within the framework of international security started its substantive work in 2026. This reflects an increasing focus on implementation, capacity-building, national positions and responsible State behaviour, rather than on the mere existence of an international legal framework (United Nations Office for Disarmament Affairs, 2026). This development should not be taken to mean that all legal differences have vanished. It is better seen as further evidence of the wide acceptance of the applicability of international law by States, notwithstanding their continuing disagreements about its detailed application.

The voluntary norms of responsible State behaviour should be differentiated from the binding primary rules. The 2015 GGE and subsequent UN processes on critical infrastructure, harmful ICT activity and cooperation, including issues related to CERTs, developed expectations (United Nations General Assembly, 2015, 2021a). Such norms may affect State expectations and diplomatic practice but they do not have the same legal status as treaty obligations or rules of custom. A legal article should therefore refer to the source of each proposition, instead of using the word 'norms' as if it always means binding law.

Confidence-building measures, contact points, information sharing and capacity-building can make the existing framework more user-friendly in practice. They can support communication, decrease the risk of misunderstanding and assist States in responding to incidents. But they do not in and of

themselves create new Charter rights or obligations. They are of great practical importance. In this respect, the emerging Global Mechanism is helpful as it provides States with a forum for the exchange of views and the development of practical understandings, without presupposing that every new practice is already customary international law.

3. Cyberspace Sovereignty

One of the most discussed issues in international cyber law is sovereignty. It is widely agreed that sovereignty applies in cyberspace. However, there is no agreement among States and scholars on whether territorial sovereignty is a separate rule prohibiting all non-consensual remote cyber operations. Canada explicitly treats territorial sovereignty as a rule and references substantial harmful effects, territorial integrity, and interference with or usurpation of inherently governmental functions as relevant factors (Government of Canada, 2022). The United Kingdom adopted a different position in its 2018 Attorney General statement, observing that it was not convinced that international law at present contains a specific rule of sovereignty for cyberspace distinct from the rules that already exist, including non-intervention (Wright, 2018).

This difference is not just academic. If one broadens the understanding of sovereignty, many forms of remote intelligence or network activity could be seen as internationally wrongful. Under the narrower approach, some operations may not fall within a clear legal category unless they meet the higher thresholds of intervention or use of force. Thus, the article regards the Canadian position as important State practice, but not as conclusive proof of customary law. Likewise the UK position is seen as evidence that the disagreement continues, not proof that a rule of independent sovereignty cannot exist. Indeed, recent scholarship has also shown that the problem remains unsolved (e.g., Corn & Jensen, 2018; Schmitt, 2022).

It is useful to adopt an effects and function approach to analyse the issue. The article offers this as a proposed analytical framework, not a settled customary law. Significant harmful effects inside another State, especially effects on essential services or territorial integrity, rather than very minor or temporary access, is a stronger basis for a sovereignty claim. Interference with or usurpation of inherently governmental functions could also be a strong basis. On the flip side, simple intelligence collection is still controversial, and should not automatically be considered a violation of sovereignty simply because it crosses a digital border.

Inherently governmental functions are particularly important because they tie cyber operations to the traditional notion that a State has exclusive control over governmental activity within its territory. Examples might include remote modification of official records, interference with election administration, manipulation of law enforcement systems, or the performance of governmental acts through the infrastructure of another State. The precise line between illegal government intrusion and spying is still being debated. Thus, the article treats interference with governmental functions as a factor in the sovereignty analysis, not a rule that answers every case.

Another difficult threshold question is created by persistent access and pre-positioning. A State might be able to inflict immediate physical damage on a foreign network, but not want to do so because it wants to collect intelligence, while still being able to cause serious disruption at a later time. There is no bright line rule that every persistent presence is a use of force. Nor does the lack of immediate damage alone settle the sovereignty issue. The actual effects, the government function involved, the purpose of the operation and the legal context in which it takes place are better considerations. A latent capability is not to be considered an armed attack per se.

4. Non-Intervention

The customary rule of non-intervention safeguards a State's freedom to decide in its domaine réservé without coercive outside interference. The decision of the ICJ in *Nicaragua* is still an important authority on the role of coercion (Military and Paramilitary Activities in and against Nicaragua (*Nicaragua v. United States of America*), 1986). So the key question in the cyber context is not whether an operation had an impact on an important or sensitive system. The question is whether the operation was intended to pressure or coerce the target State in an area in which it is entitled to decide for itself.

Thus, interference in elections, disruption of governmental decisionmaking and manipulation of public authorities may raise non-intervention concerns where coercion can be proven. It's not enough to be politically important. For instance, a cyber intrusion that merely acquires information, without attempting to force a government to make a specific choice, might not be considered a violation of the non-intervention rule, even if it is illegal on some other basis. In contrast, a more solid basis for considering an intervention appears when a system is disabled or tampered with so as to achieve a certain governmental or political result.

The key issue in this case is attribution and evidences. An intelligence assessment could be aided by a piece of malware, a language clue or a link to technical infrastructure but no one indicator should be automatically deemed to be legal proof of a State directing the operation. The analysis must distinguish between the conduct of the State itself, conduct attributable to the State under the law of State responsibility, and conduct by independent criminal or other non-State actors. Purpose, target, timing and operational control can be all relevant. But the legal conclusion must be as strong as the evidence available.

5. Prohibition of Force and Self-defence

Article 2(4) of the UN Charter prohibits the threat or use of force in the circumstances covered by the Charter, while the inherent right of individual and collective self-defence is maintained by Article 51 if an armed attack occurs (Charter of the United Nations, 1945). Cyber operations therefore have to be analysed under the existing *jus ad bellum*, and not through a separate cyber exception. The core difficulty is in determining how the scale and effects of a cyber operation fit within the frameworks of use of force and armed attack.

More persuasive State arguments focus on the effects of an operation, rather than simply on the fact that the operation used computers. A cyber operation that causes death, physical destruction or effects similar in gravity to a kinetic attack may constitute a use of force and, when sufficiently grave, an armed attack. But a serious cyber intrusion does not automatically cross that threshold. The difference is important, because Article 51 only allows for self-defence against an armed attack.

Lawful self-defence is also subject to the limits of necessity and proportionality. These are not blanket permissions to retaliate because a state is angry or wants to send a political message. The response must be defensive in nature and proportional to the armed attack. Thus, the legality of a response cannot be determined by a simple comparison of the technical means used by the two sides.

Collective self-defence also prompts some further questions, including whether an armed attack has in fact occurred and whether the victim State has requested or consented to assistance. Cooperation between allies in cyberspace may be common in practice but the legal position still depends on the Charter. A security partnership does not, in itself, give rise to a right to use force for the benefit of another State. These limits are even more important if the identity of the attacker is not yet known.

The defence of necessity under the law of State responsibility should also be distinguished from the necessity of self-defence. Article 25 of the ILC Articles is a narrow circumstance precluding wrongful acts. In particular, it requires that the grave and imminent peril of an essential interest and the absence

of other reasonable means of protecting that interest, respecting the interests protected by the obligation in question. The exception is therefore not a blanket exception to cyber self-help, and should not be used to bypass the separate requirements of attribution, proportionality and necessity which apply to other legal responses.

6. Attribution and State Liability

The ILC Articles on Responsibility of States for Internationally Wrongful Acts are the main secondary-law framework for these issues. Article 4 addresses the conduct of State organs. Article 8 deals with persons or groups acting on behalf of, or under the direction or control of, a State. Article 11 relates to conduct which a State subsequently accepts and adopts (International Law Commission, 2001). These rules must therefore be carefully applied to cyber operations involving proxies, contractors or criminal groups. Technical assistance or political sponsorship must not be blindly equated with legal attribution.

The distinction between political attribution and legal attribution is especially important in the case of cyber incidents. Sometimes intelligence is used by a government to publicly blame another State, when that intelligence cannot be made public for diplomatic, deterrent or sanctions reasons. But the court or tribunal would have to apply the relevant legal rules to the evidence before it. The fact that a judicial determination has not been made on an incident does not make a political attribution irrelevant, but a political statement should not be presented as if it were a judicial finding.

Cyber evidence may pass through compromised third party systems and may also be deliberately tampered with. Attribution should therefore be based on a combination of evidence and not on a single technical indicator. Legal advisers should retain a record of the evidence on which they relied and distinguish between the various levels of confidence and the final legal conclusion and indicate whether the conduct is apparently that of a State organ, an instructed or controlled group or a private actor whose conduct is not attributable. This is especially so where a proposed legal response depends on the prior determination that another State has committed an internationally wrongful act.

Measures may be taken when another State has committed an internationally wrongful act, but the conditions of the law of State responsibility apply. Articles 49-53 concern the purpose, scope and conditions of the ILC Articles. Countermeasures should aim at inducing compliance, be proportionate, respect obligations not affected by countermeasures and meet the procedural requirements of Article 52 subject to the recognised debates of urgency and notification (International Law Commission, 2001). "While all cyber countermeasures must always be technically reversible" is not accurate. Reversibility is an important aspect of the temporary nature of countermeasures.

Unlike retorsion, retorsion is unfriendly but lawful conduct and therefore does not require a prior internationally wrongful act. This can be important in cyber situations where attribution is uncertain or where a State wants to respond without having to rely on the legal consequences of State responsibility. In some cases, sanctions, diplomatic measures, export controls and public attribution may be used without having established all the elements required for a countermeasure or self-defence.

7. Due Diligence: Rule, Standard or Voluntary Norm?

Another is due diligence. The Corfu Channel is significant for the proposition that a State must not knowingly permit its territory to be used for acts which infringe the rights of other States. (Corfu Channel (United Kingdom v Albania) 1949). But there is no automatic implication that application of that idea to cyberspace demonstrates the existence of one general cyber due-diligence obligation. Whether cyber due diligence is to be considered a part of customary international law, a series of primary obligations that would apply in particular instances, or simply a voluntary norm of responsible

behaviour continues to be debated among scholars and States (Kenny, 2024; Moynihan, 2024; Coco & de Souza Dias, 2023).

So instead of a universal cyber test of 'knowledge plus feasibility' it is better to take a more prudent approach. Instead, due diligence should be measured against the particular primary obligation at hand, what the State knew or ought to have known, the character of the activity, the capacity of the State, and the preventive or responsive measures reasonably available. The UN norm on malicious ICT activity emanating from a State's territory should also be described as a voluntary norm, and not as a norm that automatically becomes customary law, given the support of many States.

Notice from an affected State is legally and practically important but does not automatically trigger a universally recognised 'diligence clock'. Whether a State has violated an obligation depends on the relevant primary rule, the facts of the incident and the measures which were reasonably available. The capacity of the territorial State is relevant but lack of capacity cannot necessarily answer every case. The analysis should therefore steer clear of both strict liability and a treatment of due diligence as merely aspirational.

The State affected by a cyber incident also has practical reasons to cooperate if it wants the territorial State to take preventive action. Cooperation can be more effective if useful technical indicators are shared, infrastructure that may be affected is identified when possible, and established channels of communication are used. These steps are better understood as a matter of good-faith inter-State cooperation than as legal conditions that must always be met before a due-diligence claim can be made.

8. The Tallinn Manuals and the Status of Expert Restatements

The Tallinn Manual 2013 focused primarily on grave cyber operations and issues pertaining to armed conflict. Tallinn Manual 2.0, published in 2017, expanded the discussion to peacetime issues such as sovereignty, intervention, jurisdiction, State responsibility and human rights. In 2021, the CCDCOE initiated the Tallinn Manual 3.0 project as a five-year revision and expansion project to reflect new State practice and legal developments (NATO Cooperative Cyber Defence Center of Excellence, 2021–2026). This is still an expert revision project, not a treaty-making process, as of September 2026.

The Tallinn Manuals are useful secondary sources, but are not themselves sources of international law. Their proposals will therefore have to be tested against the provisions of the treaties, customary international law, judicial decisions and State practice. Their value for this article lies primarily in organising a specialised and technically difficult area of legal debate, and in showing where the experts disagree. Nor should they be cited as if expert agreement automatically establishes *opinio juris*.

An example of this is the discussion on collective countermeasures. Some scholars and experts have debated whether States other than the injured State are allowed to take countermeasures in response to an internationally wrongful cyber operation. Therefore, there is no express provision in the ILC Articles for a general right of collective countermeasures. The issue is controversial. Hence, a national legal stance or a statement in the Tallinn Manual should be advanced as argument or interpretation and not as established customary law.

The publication of Tallinn Manual 3.0 is especially opportune as State practice has evolved since the publication of Tallinn Manual 2.0. The ultimate significance of it will depend on how sensitively the project treats different State positions rather than on the authority of the experts who engage in it. The project can help identify questions that require more detailed study for research purposes, including espionage, sovereignty, due diligence, collective responses, AI-enabled operations and international humanitarian law. The legal sources underpinning still have to be analysed separately.

The use of generative AI does not in itself create a new category of State responsibility. The usual rules of attribution, primary responsibility and the UN Charter still apply, even if a State organ or other

actor attributable to a State uses AI to carry out a cyber operation. However, artificial intelligence can still change the factual and evidentiary picture through increased speed, scale and automation, and through making human control more difficult to evaluate. What has to be done, therefore, is to apply the existing legal rules with special attention to the new evidentiary problems that the technology creates.

9. Relative national positions

9.1 United Kingdom

A 2018 statement by the Attorney General of the United Kingdom remains an important public articulation of its position. It accepted the applicability of international law in cyberspace, considered the principles of non-intervention and the Charter prohibition on force to be important rules, and rejected the notion that current international law contains a separate cyber-specific rule on sovereignty. It also accepted that cyber operations causing death and destruction on the scale of an armed attack could trigger self-defence (Wright, 2018). This should be understood as the UK's public position on the legal issues and not as a statement of international law binding other States.

The UK example also demonstrates why domestic cyber powers and international legality should not be confused. The National Cyber Force is an element of the domestic institutional architecture. But whether a particular UK operation against another State is legal is a matter of international law. The 2025 National Security Strategy shows the continued importance attached to cyber capabilities and hostile State activity, but is a strategy document, not a full statement of international cyber law (Cabinet Office, 2025). Therefore it is used here mainly as background.

The public law position of the UK could also be further considered in light of developments in other States since 2018, particularly in relation to sovereignty and attribution. This article does not presume that the UK has changed its position because of other States publishing newer views. Instead, the 2018 statement is referred to as a clear illustration of one side of an ongoing legal dispute.

9.2 Australia

Australia has consistently supported the application of existing international law to the conduct of States in cyberspace. Its public documents acknowledge the importance of the UN Charter, international humanitarian law in armed conflict, State responsibility and the legal difficulties surrounding sovereignty, attribution and jurisdiction (Australian Government, 2017, 2019). What makes these materials valuable is that they illustrate how legal rules can be explored in relation to wider norms of responsible conduct. But still the legal position should be kept apart between the two.

9.3 Canada

Canada's April 2022 statement highlights sovereignty especially. It explicitly recognises territorial sovereignty as a rule and territorial integrity and interference with or usurpation of inherently governmental functions as possible bases for a violation. It also adopts an effects-based approach which considers the scope, scale, impact and severity of disruption. At the same time, Canada acknowledges that some cyber espionage does not violate territorial sovereignty (Government of Canada, 2022). The Canadian position is therefore useful to consider in an effects-and-function approach, but it remains a national position and cannot be treated automatically as customary international law.

Canada also serves to demonstrate the difference between peacetime *jus ad bellum* and international humanitarian law. It is framed publicly as a recognition of the relevance of IHL where an armed conflict exists but IHL should not be used to normalise ordinary peacetime cyber operations or to evade the separate Charter analysis. The Canadian material is thus of the greatest utility when these distinct areas of law are kept separate.

9.4 India

A significant development for the Indian material took place in 2025, when the Ministry of Defence released the declassified Joint Doctrine for Cyberspace Operations. The doctrine states that cyberspace operations can support military objectives and that they may be perceived as a response to hostile action against national sovereignty, and not only to cyber-attacks (Ministry of Defence, Government of India, 2025). This is useful evidence on military thinking, but it should not be seen as an official Indian statement of customary international law or a substitute for a legal position issued by the foreign ministry.

The Indian example thus exposes the need to disaggregate the military doctrine and international legal positions. In this article the Joint Doctrine is used as evidence of military policy and emerging operational thinking. The article avoids a conclusion on India's legal position on sovereignty, force or self-defence unless that position is based on more direct legal material. This is a more prudent approach than to deduce legal conclusions from military terminology.

9.5 Pakistan

Pakistan has presented its 2023 position on the application of international law in cyberspace via the UN process and adopted the National Cyber Security Policy 2021 (Government of Pakistan, 2021; United Nations Office for Disarmament Affairs, 2023). These materials indicate that Pakistan recognises the importance of existing international law and has developed a domestic policy framework for cyber security. The 2021 policy defines a cyber-attack against Pakistani critical infrastructure as an act of aggression against the national sovereignty and refers to appropriate response measures. But policy language must not be conflated with the legal threshold for an armed attack under the Charter.

Pakistan's public cyber framework has also continued to evolve in 2026. National CERT material and government reporting National CERT Pakistan 2026: Work on Pakistan Information Security Framework 2026 and 90 days cyber-security strategic action plan, including strengthening of federal and provincial CERT arrangements. These developments are useful for implementation and institutional capacity considerations, but do not, in themselves, establish Pakistan's detailed international law position on sovereignty, intervention or Article 51. Pakistan's public international law position is therefore to be read vis-à-vis the domestic policy framework rather than instead of it.

The comparison with India is particularly pertinent as cyber incidents in the region can stoke broader security and escalation concerns. A cyber hotline or other confidence-building measure would not in itself make a new rule of international law. But it might help with incident notification and clarification and crisis management. Its value would be practical: reducing uncertainty and promoting good faith application of current rules.

10. Comparison Results and Analytical Framework

Table 1

Emphasis in national approaches to international law in cyberspace

Doctrine	UK	Australia	Canada	Pakistan/India
IL existing	Yes; AG Wright 2018 & later practice	Yes; UN framework champion	Yes; 2022 national position	Pakistan 2023 position; India no detailed memo
Sovereignty as a rule	Scepticism of stand-alone rule for each intrusion	Sovereignty applies; effects-based analysis	Territorial sovereignty is a rule; integrity + governmental functions	Pakistan accepts sovereignty; India silent on details
Use of force / Art. 51	Scale and effects; no cyber exceptionalism	Scale and effects	Full application of Charter	Full application of Charter; emerging operational doctrines

Doctrine	UK	Australia	Canada	Pakistan/India
Attribution	Political + legal; public calling-out discretionary	Public attributions with Five Eyes partners	Public attributions in selected cases	South Asian attributions politically fraught
Due diligence	Acknowledged with caution regarding scope	Supported as part of responsible behavior	Recognized as part of sovereignty obligations	Discussed more as capacity than claim

10.1 Thresholds and Legal Effect

The threshold ladder is kept since it provides a simple picture of the analytical structure proposed in this article. But it does not mean that there are five fixed and universally accepted cyber thresholds in customary international law. On the low end, the intelligence collection might be lawful, unlawful under a different rule, or still legally challenged depending on the facts. Where the relevant legal position recognises such a rule, a greater harmful effect or interference with governmental functions may sustain a claim of sovereignty. Non-intervention may be engaged by coercive conduct. More serious effects may reach the prohibition on the use of force, and only sufficiently serious armed attacks may activate Article 51.

Table 2

Typical legal reactions by operation type and main rules

Operation Type	Primary Rule Applied	Typical Lawful Response
Passive intelligence collection	Often described as unregulated or tolerated spying	Defensive hardening; rarely public law claims
Intrusion that disables civilian systems below force	Sovereignty and/or due diligence; possible intervention	Retorsion; possible countermeasures if attribution is established
Coercive election or police interference	Non-intervention	Countermeasures; public attribution; sanctions
Similar destruction as kinetic strike	Art. 2(4) use of force	countermeasures or self-defence if armed attack threshold met
Campaign leading to death or equivalent destruction	Armed attack, art. 51	Self-defence, necessity and proportionality

Table 2 should also be seen as an analytical framework and not as a list of responses that are automatically lawful. The level of attribution required will depend on the legal response being considered. Countermeasures must be preceded by an internationally wrongful act attributable to the State against which they are directed. Self-defence requires an armed attack. Necessity and proportionality. Retorsion involves no prior wrongful act. International humanitarian law applies if the criteria for an armed conflict are met, but it usually does not authorise disruptive cyber operations in peacetime.

10.2 Critical Infrastructure, Third States and Private Actors

Publishing national legal positions might reduce uncertainty but publication alone does not make international law. Its main value is that it allows other States, courts and scholars to see and evaluate the State's interpretation. The article therefore contends that States should publish their positions on sovereignty, non-intervention, the use of force, self-defence, attribution, countermeasures and due diligence where security considerations permit. It would also be useful if such documents clearly state if a specific position is based on a treaty, on customary international law, on an interpretation of existing rules, or on a policy preference.

11. Conclusion

The conclusion is qualified by the analysis. Existing international law already applies to State behaviour in cyberspace, but there is still disagreement about precise thresholds and types of evidence required in particular cases. The UN process provides a strong intergovernmental basis for arguing that cyberspace does not exist outside the UN Charter or the general law of State responsibility (United Nations General Assembly, 2013, 2015, 2021a, 2021b). The harder questions are how sovereignty, intervention, force, self-defence, attribution and preventive obligations work out in the case of an actual cyber incident.

The article's main analytical contribution is an effects-and-function approach to sovereignty and a clear distinction between primary rules, secondary rules and voluntary norms. The article does not say that this is already customary international law. Rather, it is offered as a pragmatic doctrinal approach to the analysis of contested operations within the limits of the data available. More extensive sovereignty analysis than minor access issues is required when major adverse effects and interference with governmental authority occur. Non-intervention is founded on coercion, and force or armed attack should be assessed in terms of gravity and effects, and political attribution should be distinguished from legal attribution.

Due diligence requires special care. The Corfu Channel is still relevant, but there is still no consensus in the literature as to whether a general rule of cyber due diligence has emerged as customary international law. A prudent approach is to examine the specific primary obligation, what the State knew, its capacity and the measures that were reasonably available instead of announcing one universal cyber standard (Kenny, 2024; Moynihan, 2024; Coco & de Souza Dias, 2023). Countermeasures are only possible in case of satisfaction of the requirements of State responsibility. Retorsion might be of relevance if the conduct is unfriendly but lawful. Self-defence is still an exceptional response to an armed attack and is subject to necessity and proportionality.

The comparison also shows that the United Kingdom, Australia, Canada, India and Pakistan have provided different types and levels of public material on their approaches to cyberspace. Canada has published a detailed position on sovereignty, the UK presents an important counter-point, Australia has laid out a broad legal framework, India has made public its military cyber-doctrine and Pakistan has coupled a 2023 international-law position with a domestic cyber-security policy framework. The existence of similar ideas in a number of documents should not be made a universal legal rule for any of those materials.

For now, the most practical improvement would be a more disciplined use of the law already on the books. This includes more precise communication after incidents, clearer national legal positions, better attribution procedures and a careful differentiation between binding legal obligations and voluntary norms. A comprehensive new treaty could be useful if States were eventually to agree on rules sufficiently specific, but the evidence discussed here does not support treating a new treaty as a necessary condition for the regulation of cyber operations. Now the task is to apply the law as it stands with care and not to claim more than the evidence will bear.

Thus the research questions can be answered as below. Cross-border cyber operations are governed by existing international law, including the UN Charter, customary rules and the law of State responsibility. Sovereignty is not a given in every case, it is contested and should be understood as a function of the effects of the operation and any disruption to government functions. Non-intervention is based upon force. The thresholds of use-of-force and armed attack are dependent on the gravity and effects of operation. Attribution is a precondition to resort to legal responses based on a previous internationally wrongful act. Finally, due diligence should be approached carefully, as its precise customary status in cyberspace remains contested. The conclusions drawn are the basis for further research on State practice and comparative law.

References

- Abbott, K. W., & Snidal, D. (2000). Hard and soft law in international governance. *International Organization*, 54(3), 421--456.
- Amsden, A. H. (1989). *Asia's next giant: South Korea and late industrialization*. Oxford University Press.
- Autor, D. H., Dorn, D., & Hanson, G. H. (2013). The China syndrome: Local labor market effects of import competition in the United States. *American Economic Review*, 103(6), 2121--2168.
- Babb, S. (2013). The Washington Consensus as transnational policy paradigm: Its origins, trajectory and likely successor. *Review of International Political Economy*, 20(2), 268--297.
- Baldwin, R. (2016). *The great convergence: Information technology and the new globalization*. Harvard University Press.
- Barnett, M., & Finnemore, M. (2004). *Rules for the world: International organizations in global politics*. Cornell University Press.
- Basinger, S. J., & Hallerberg, M. (2004). Remodeling the competition for capital: How domestic politics erases the race to the bottom. *American Political Science Review*, 98(2), 261--276.
- Bennett, C. J. (1991). What is policy convergence and what causes it? *British Journal of Political Science*, 21(2), 215--233.
- Bhagwati, J. (2004). *In defense of globalization*. Oxford University Press.
- Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Oxford University Press.
- Cardoso, F. H., & Faletto, E. (1979). *Dependency and development in Latin America*. University of California Press.
- Castells, M. (1996). *The rise of the network society*. Blackwell.
- Castles, S., de Haas, H., & Miller, M. J. (2014). *The age of migration: International population movements in the modern world* (5th ed.). Palgrave Macmillan.
- Cerny, P. G. (1997). Paradoxes of the competition state: The dynamics of political globalization. *Government and Opposition*, 32(2), 251--274.
- Chang, H.-J. (2002). *Kicking away the ladder: Development strategy in historical perspective*. Anthem Press.
- Colantone, I., & Stanig, P. (2018). Global competition and Brexit. *American Political Science Review*, 112(2), 201--218.
- Dobbin, F., Simmons, B., & Garrett, G. (2007). The global diffusion of public policies: Social construction, coercion, competition, or learning? *Annual Review of Sociology*, 33, 449--472.
- Dollar, D., & Kraay, A. (2004). Trade, growth, and poverty. *The Economic Journal*, 114(493), F22--F49.
- Drezner, D. W. (2001). Globalization and policy convergence. *International Studies Review*, 3(1), 53--78.
- Drezner, D. W. (2007). *All politics is global: Explaining international regulatory regimes*. Princeton University Press.
- Esping-Andersen, G. (1990). *The three worlds of welfare capitalism*. Princeton University Press.
- European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons

- with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *Official Journal of the European Union*, L 119.
- Freeman, G. P. (1995). Modes of immigration politics in liberal democratic states. *International Migration Review*, 29(4), 881--902.
- Garrett, G. (1998). *Partisan politics in the global economy*. Cambridge University Press.
- Garrett, G., & Mitchell, D. (2001). Globalization, government spending and taxation in the OECD. *European Journal of Political Research*, 40(2), 145--177.
- Genschel, P., & Schwarz, P. (2011). Tax competition: A literature review. *Socio-Economic Review*, 9(2), 339--370.
- Giddens, A. (1990). *The consequences of modernity*. Polity Press.
- Gygli, S., Haelg, F., Potrafke, N., & Sturm, J.-E. (2019). The KOF Globalisation Index -- revisited. *The Review of International Organizations*, 14(3), 543--574.
- Hall, P. A., & Soskice, D. (Eds.). (2001). *Varieties of capitalism: The institutional foundations of comparative advantage*. Oxford University Press.
- Harvey, D. (2005). *A brief history of neoliberalism*. Oxford University Press.
- Hays, J. C. (2009). *Globalization and the new politics of embedded liberalism*. Oxford University Press.
- Held, D., McGrew, A., Goldblatt, D., & Perraton, J. (1999). *Global transformations: Politics, economics and culture*. Polity Press.
- Hirst, P., & Thompson, G. (1996). *Globalization in question: The international economy and the possibilities of governance*. Polity Press.
- Hollifield, J. F., Martin, P. L., & Orrenius, P. M. (Eds.). (2014). *Controlling immigration: A global perspective* (3rd ed.). Stanford University Press.
- Inglehart, R., & Norris, P. (2016). *Trump, Brexit, and the rise of populism: Economic have-nots and cultural backlash* (HKS Faculty Research Working Paper Series RWP16-026). Harvard Kennedy School.
- Joppke, C. (1998). Why liberal states accept unwanted immigration. *World Politics*, 50(2), 266--293.
- Kapur, D. (2010). *Diaspora, development, and democracy: The domestic impact of international migration from India*. Princeton University Press.
- Kaufman, R. R., & Segura-Ubiergo, A. (2001). Globalization, domestic politics, and social spending in Latin America: A time-series cross-section analysis, 1973--97. *World Politics*, 53(4), 553--587.
- Keck, M. E., & Sikkink, K. (1998). *Activists beyond borders: Advocacy networks in international politics*. Cornell University Press.
- Keohane, R. O., & Nye, J. S. (2000). Globalization: What's new? What's not? (And so what?). *Foreign Policy*, 118, 104--119.
- Knill, C. (2005). Introduction: Cross-national policy convergence: Concepts, approaches and explanatory factors. *Journal of European Public Policy*, 12(5), 764--774.
- Levi-Faur, D. (2005). The global diffusion of regulatory capitalism. *The Annals of the American Academy of Political and Social Science*, 598(1), 12--32.
- Meyer, J. W., Boli, J., Thomas, G. M., & Ramirez, F. O. (1997). World society and the nation-state. *American Journal of Sociology*, 103(1), 144--181.
- Milanovic, B. (2016). *Global inequality: A new approach for the age of globalization*. Harvard University Press.
- Mosley, L. (2003). *Global capital and national governments*. Cambridge University Press.

- Norris, P., & Inglehart, R. (2019). *Cultural backlash: Trump, Brexit, and authoritarian populism*. Cambridge University Press.
- Ohmae, K. (1995). *The end of the nation state: The rise of regional economies*. Free Press.
- Organisation for Economic Co-operation and Development. (2011). *Divided we stand: Why inequality keeps rising*. OECD Publishing.
- Ostry, J. D., Loungani, P., & Furceri, D. (2016). Neoliberalism: Oversold? *Finance & Development*, 53(2), 38--41.
- Polanyi, K. (1944). *The great transformation*. Farrar & Rinehart.
- Robertson, R. (1992). *Globalization: Social theory and global culture*. Sage.
- Rodrik, D. (1998). Why do more open economies have bigger governments? *Journal of Political Economy*, 106(5), 997--1032.
- Rodrik, D. (2011). *The globalization paradox: Democracy and the future of the world economy*. W. W. Norton.
- Rodrik, D. (2018). Populism and the economics of globalization. *Journal of International Business Policy*, 1(1--2), 12--33.
- Rudra, N. (2008). *Globalization and the race to the bottom in developing countries: Who really gets hurt?* Cambridge University Press.
- Ruggie, J. G. (1982). International regimes, transactions, and change: Embedded liberalism in the postwar economic order. *International Organization*, 36(2), 379--415.
- Sassen, S. (1996). *Losing control? Sovereignty in an age of globalization*. Columbia University Press.
- Scholte, J. A. (2005). *Globalization: A critical introduction* (2nd ed.). Palgrave Macmillan.
- Simmons, B. A., & Elkins, Z. (2004). The globalization of liberalization: Policy diffusion in the international political economy. *American Political Science Review*, 98(1), 171--189.
- Slaughter, A.-M. (2004). *A new world order*. Princeton University Press.
- Stiglitz, J. E. (2002). *Globalization and its discontents*. W. W. Norton.
- Strange, S. (1996). *The retreat of the state: The diffusion of power in the world economy*. Cambridge University Press.
- Swank, D. (2002). *Global capital, political institutions, and policy change in developed welfare states*. Cambridge University Press.
- United Nations Department of Economic and Social Affairs, Population Division. (2020). *International migration 2020 highlights* (ST/ESA/SER.A/452). United Nations.
- United Nations General Assembly. (2018). *Global compact for safe, orderly and regular migration* (Resolution 73/195). United Nations.
- Vogel, D. (1995). *Trading up: Consumer and environmental regulation in a global economy*. Harvard University Press.
- Wade, R. (1990). *Governing the market: Economic theory and the role of government in East Asian industrialization*. Princeton University Press.
- Wade, R. H. (2003). What strategies are viable for developing countries today? The World Trade Organization and the shrinking of "development space." *Review of International Political Economy*, 10(4), 621--644.
- Wallerstein, I. (1974). *The modern world-system: Capitalist agriculture and the origins of the European world-economy in the sixteenth century*. Academic Press.
- Weiss, L. (1998). *The myth of the powerless state*. Cornell University Press.
- Williamson, J. (1990). What Washington means by policy reform. In J. Williamson (Ed.), *Latin American adjustment: How much has happened?* (pp. 5--20). Institute for International Economics.

- Woods, N. (2006). *The globalizers: The IMF, the World Bank, and their borrowers*. Cornell University Press.
- World Bank. (2020). *World development report 2020: Trading for development in the age of global value chains*. World Bank

Declarations

◆ Funding	This research received no external funding.
◆ Conflict of Interest	The author declares no conflict of interest.
◆ Data Availability Statement	Data sharing is not applicable to this article, as no new data were created or analysed in this study.
◆ Ethical Statement	Ethical approval was not required because the study is based exclusively on publicly available legal materials and published literature and did not involve human participants.
◆ AI Use Disclosure	Generative artificial intelligence tools were used in a limited and assistive capacity during the preparation of this manuscript, primarily for idea development, language refinement, and grammatical correction. The authors retain full responsibility for the originality, accuracy, analysis, interpretation, and final content of the manuscript.

Journal Policies *JuriSocial Journal of Social Sciences*

OPEN ACCESS & LICENCE

All articles are freely available on publication under CC BY-NC 4.0. Readers may share and adapt the work for non-commercial purposes with proper attribution.

PEER REVIEW

Every research article undergoes double-blind peer review by at least two independent reviewers.

PLAGIARISM POLICY

All submissions are screened with similarity-detection software; plagiarism in any form leads to rejection.

CORRECTIONS & RETRACTIONS

Errors are corrected through published corrigenda; retractions follow COPE guidelines.

PUBLICATION CHARGES

No article publishing fee charged.

COPYRIGHT

Authors retain copyright and grant JJSS the right of first publication.

PUBLICATION ETHICS

JJSS follows the Committee on Publication Ethics (COPE) Core Practices and guidelines.

GENERATIVE AI POLICY

AI tools cannot be listed as authors. Any substantive use must be disclosed; authors remain fully responsible for the content.

ARCHIVING & INDEXING

Content is preserved through [PKP Preservation Network / LOCKSS]. DOIs are registered with Crossref.

DISCLAIMER

The views expressed are those of the authors and do not necessarily reflect the views of the editors or the publisher.

Submissions & enquiries editor@jjss.jurisocial.org ◆ <https://socialsciences.jurisocial.org/>