 DOI: https://10.5281/zenodo.22914629

International Law and the Use of Force in Cyberspace: Rethinking Article 2(4) of the UN Charter

Abhinav Singh [1]

© The Author(s), under exclusive licence to Oxford Law Review 2026.

Abstract

The increasing use of cyberspace for strategic, political and military purposes has generated difficult questions concerning the application of the prohibition on the threat or use of force under Article 2(4) of the Charter of the United Nations. This article examines whether, and under what circumstances, a cyber operation may constitute a prohibited use of force under international law. It argues that the technological means employed should not determine the legal character of State conduct. Instead, the assessment should focus upon the scale and effects of the operation, considered in light of factors including severity, directness, immediacy, military character, the nature of the target and the circumstances of the operation. The article distinguishes the threshold of a use of force from the separate and higher threshold of an armed attack under Article 51 and examines the significance of this distinction for responses to cyber operations. It further analyses attribution and State responsibility, emphasising that technical attribution and legal attribution are distinct inquiries governed by the general law of State responsibility. The article concludes that Article 2(4) remains capable of regulating cyber operations without the creation of a separate cyber-specific law of force. A carefully calibrated, effects-based and contextual approach can preserve the effectiveness of the prohibition while preventing its application from extending indiscriminately to all forms of cyber interference.

Keywords: Article 2(4); Use of Force; Cyberspace; Cyber Operations; State Responsibility; International Law

1. Introduction

The prohibition of the threat or use of force occupies a foundational position in the contemporary international legal order. Article 2(4) of the Charter of the United Nations requires States to refrain from the threat or use of force against the territorial integrity or political independence of any State, or otherwise in a manner inconsistent with the purposes of the United Nations (United Nations 1945). The provision is complemented by Article 51, which preserves the inherent right of individual and collective self-defence if an armed attack occurs. Together, these provisions establish the principal legal framework governing the resort to coercive force in international relations.

[1] University of Otago, Otago, New Zealand; ORCiD: https://orcid.org/0009-0003-9089-3518

Copyright © Oxford Law Review. (editor@oxfordlr.com)

The emergence of cyberspace presents a distinctive problem for this framework. Cyber operations can produce consequences traditionally associated with military force without employing conventional weapons or physically crossing an international border. A cyber operation may disrupt electrical grids, disable military systems, interfere with communications, compromise critical infrastructure or cause physical damage through digitally controlled systems. Other operations may generate substantial economic or strategic disruption without causing physical destruction. The legal difficulty is therefore not whether international law applies to cyberspace, but how existing rules governing the use of force should be applied to conduct whose technological means differ fundamentally from the conventional forms of force contemplated when the Charter was adopted.

The international community has increasingly affirmed that existing international law applies to State conduct in cyberspace. The United Nations Group of Governmental Experts concluded that international law, including the Charter of the United Nations, is applicable to State conduct in the use of information and communications technologies and is essential to maintaining international peace and security (United Nations General Assembly 2013). Subsequent UN processes have reaffirmed this position and have addressed responsible State behaviour, international peace and security, and the applicability of international law in the information and communications environment (United Nations General Assembly 2021). The recognition that international law applies, however, does not itself resolve the substantive threshold at which a cyber operation constitutes a prohibited use of force under Article 2(4).

The principal difficulty lies in the absence of a comprehensive definition of "force" within the Charter. The International Court of Justice has developed the relevant principles primarily through disputes involving conventional military conduct. In *Military and Paramilitary Activities in and against Nicaragua*, the Court recognised the prohibition of the use of force as a rule of both treaty and customary international law and distinguished the "most grave forms" of the use of force from less serious forms of coercion (Nicaragua v United States of America 1986, 101–103). The Court further distinguished the concept of an "armed attack" triggering the right of self-defence from other unlawful uses of force (Nicaragua v United States of America 1986, 103–104). In *Armed Activities on the Territory of the Congo*, the Court again treated the prohibition of force and the conditions governing self-defence as distinct legal questions (Democratic Republic of the Congo v Uganda 2005, 222–227). These principles provide the doctrinal foundation for analysing cyber operations, although neither decision directly addresses the technological circumstances presented by cyber operations.

The principal scholarly approaches have therefore attempted to determine whether the existing concept of force can be applied according to the consequences and circumstances of a cyber operation rather than the physical instrument employed. The *Tallinn Manual 2.0* adopts an effects-oriented approach, providing that a cyber operation constitutes a use of force when its scale

Copyright © Oxford Law Review. (editor@oxfordlr.com)

and effects are comparable to those of non-cyber operations that would amount to a use of force (Schmitt 2017, 328–356). The approach identifies factors relevant to determining the character of a cyber operation, including its severity, immediacy, directness, invasiveness, measurability of effects and military character (Schmitt 2017). The Manual nevertheless represents expert legal analysis rather than an authoritative statement of positive international law; its propositions must therefore be distinguished from rules established through treaty, customary international law, judicial decisions and State practice.

The central legal problem is consequently one of classification. A cyber operation may constitute unlawful intervention without reaching the threshold of a use of force; a use of force may occur without amounting to an armed attack; and an armed attack may, subject to the requirements of Article 51, give rise to the right of self-defence. Treating these categories as synonymous would obscure important distinctions within the Charter framework. At the same time, an interpretation of Article 2(4) that depends exclusively upon physical destruction could leave significant forms of coercive cyber conduct outside the prohibition merely because the mechanism of harm is digital rather than kinetic.

This article examines when, and on what legal basis, a cyber operation should be characterised as a "use of force" within the meaning of Article 2(4) of the UN Charter. It distinguishes the prohibition of force from the separate rules governing intervention, countermeasures and self-defence and examines the relevance of attribution to the legal characterisation of State conduct. It argues that Article 2(4) should apply to cyber operations without creating a separate cyber-specific law of force. The assessment should instead focus upon the operation's scale and effects, considered together with factors such as severity, directness, immediacy, military character and the circumstances in which the operation is undertaken. Such an approach preserves the restrictive function of Article 2(4) while permitting the prohibition to respond to technologically mediated forms of coercive force without treating every serious cyber operation as equivalent to an armed attack.

2. Article 2(4) and the Concept of Force in International Law

Article 2(4) of the Charter of the United Nations establishes a general prohibition on the threat or use of force in international relations. It requires Members to refrain from force directed against the territorial integrity or political independence of any State, as well as from force employed in any other manner inconsistent with the purposes of the United Nations (United Nations 1945). The provision is not confined to particular categories of weapons or methods of warfare. Its central legal function is to constrain unilateral coercive conduct between States and to preserve the Charter's broader system of international peace and security. The prohibition has also acquired the status of

Copyright © Oxford Law Review. (editor@oxfordlr.com)

customary international law, independently of its treaty basis (Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America) 1986, 98–101).

The text of Article 2(4), however, does not define "force". This omission has required international law to develop the content of the prohibition through interpretation, State practice and judicial reasoning. The International Court of Justice's jurisprudence indicates that the concept is concerned principally with armed or military force, while distinguishing the prohibition of force from other forms of unlawful coercion. In *Nicaragua*, the Court differentiated the "most grave forms" of the use of force from less serious forms of coercion and treated the distinction as relevant to the separate question of whether an armed attack had occurred (Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America) 1986, 101–104). This distinction is essential because Article 2(4) and Article 51 do not establish identical thresholds: conduct may constitute an unlawful use of force without necessarily amounting to an armed attack capable of triggering the right of self-defence.

The Court's subsequent jurisprudence reinforces the gravity and contextual character of the prohibition. In *Armed Activities on the Territory of the Congo*, the Court characterised Uganda's military intervention in the Democratic Republic of the Congo as a grave violation of the prohibition expressed in Article 2(4), while separately examining whether the circumstances justified self-defence (Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda) 2005, 223–227). The significance of this jurisprudence for cyberspace lies less in the factual circumstances of conventional military intervention than in the underlying legal structure: the existence of force, its gravity, the circumstances in which it occurs, and the availability of self-defence are analytically distinct questions.

A further difficulty arises from the relationship between "force" and the other forms of prohibited State conduct. The Charter does not establish a single category of unlawful coercion. The principle of non-intervention, the prohibition of force and the law governing self-defence address different forms and degrees of interference with State sovereignty. The International Court of Justice has accordingly treated intervention and force as distinct legal principles, notwithstanding their potential factual overlap (Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America) 1986, 108–110). This distinction becomes particularly important in cyberspace because cyber operations may interfere with governmental functions, political processes or economic activity without producing effects that readily correspond to conventional military force. The fact that an operation falls below the Article 2(4) threshold therefore does not, by itself, establish its legality under international law.

The absence of a technologically specific definition has encouraged an effects-based approach to the application of Article 2(4) in cyberspace. The *Tallinn Manual 2.0* adopts the position that a cyber operation constitutes a use of force when its "scale and effects" are comparable to those of

Copyright © Oxford Law Review. (editor@oxfordlr.com)

non-cyber operations rising to the level of a use of force (Schmitt 2017, 330). The approach is significant because it rejects the proposition that the legal character of an operation should depend principally upon whether the State employed missiles, aircraft or other conventional instruments. Instead, the inquiry focuses upon what the operation does and the circumstances in which it does so. The Manual identifies factors including severity, immediacy, directness, invasiveness, measurability of effects, military character, the extent of State involvement and the circumstances surrounding the operation (Schmitt 2017, 331–334). These factors are not presented as an exhaustive legal test, nor does the Manual itself constitute binding international law.

The effects-based approach nevertheless encounters an important boundary problem. Physical injury, death or destruction resulting directly from a cyber operation provides a relatively strong analogy with conventional force. The position is considerably less certain where an operation produces only loss of functionality, temporary disruption or economic consequences. Contemporary scholarship notes that State positions increasingly tend to assess cyber operations by reference to their scale and effects, but substantial uncertainty remains concerning operations that produce serious disruption without physical damage (Schmitt 2017; Tsagourias 2013). The difficulty is particularly acute where disruption of digital systems indirectly produces physical consequences—for example, where interference with a hospital, electricity network or industrial control system contributes to injury or destruction. In such cases, the question is not simply whether harm occurred, but whether the cyber operation is sufficiently connected to the resulting harm to constitute force in the legal sense.

Physical consequences should therefore not be treated as an automatic requirement of Article 2(4), nor should every significant non-physical consequence automatically satisfy the threshold. A purely physical-effects test would risk making the prohibition dependent upon technological characteristics rather than the coercive substance of the conduct. Conversely, treating any substantial economic or political consequence as "force" could collapse distinctions between force, intervention and other forms of unlawful conduct. The more defensible approach is consequently one of contextual assessment in which the operation's scale and effects provide the starting point, while severity, directness, immediacy, military character and the nature of the target inform the ultimate legal characterisation (Schmitt 2017, 331–337).

The concept of force must also be distinguished from the concept of an armed attack. The *Tallinn Manual 2.0* expressly treats the two as separate standards serving different normative purposes: the use-of-force standard determines whether Article 2(4) has been violated, whereas the armed-attack standard determines whether the exceptional right of self-defence under Article 51 may arise (Schmitt 2017, 337–342). This distinction follows the reasoning of the International Court of Justice in *Nicaragua*, where the Court recognised that not every use of force constitutes an armed attack (Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of

Copyright © Oxford Law Review. (editor@oxfordlr.com)

America) 1986, 101–104). Applying this distinction to cyberspace is essential. A cyber operation may cross the Article 2(4) threshold while remaining below the higher threshold associated with an armed attack. Conversely, where a cyber operation produces consequences comparable in scale and effects to a grave kinetic attack, the possibility of characterising it as an armed attack requires a separate analysis under Article 51.

The legal problem presented by cyberspace is therefore not the absence of an applicable prohibition but the difficulty of determining how an existing prohibition operates when the means of coercion have changed. Article 2(4) should not be interpreted as a rule applicable only to technologically recognisable forms of twentieth-century military force. At the same time, its application must preserve the distinctions that structure the Charter system. The relevant inquiry is consequently whether the scale, effects and circumstances of a particular cyber operation are sufficiently comparable to conduct traditionally understood as a use of force, while maintaining a separate threshold for an armed attack. Such an interpretation permits Article 2(4) to retain its central protective function without transforming every serious cyber operation into a prohibited use of force.

3. Cyber Operations and the Threshold of the Use of Force

The application of Article 2(4) to cyber operations requires the identification of a threshold capable of distinguishing a prohibited use of force from other forms of unlawful or unfriendly State conduct. The absence of a physical weapon does not, in itself, remove an operation from the scope of the prohibition. The relevant legal question is whether the consequences and circumstances of the cyber operation are sufficiently comparable to conduct that international law recognises as a use of force. This approach is increasingly reflected in State practice. The United Kingdom, for example, has expressly stated that a cyber operation may constitute a use of force where its actual or threatened effects are the same or similar to those produced by kinetic means (United Kingdom 2021). The Netherlands has likewise taken the position that the effects, rather than the technological means through which they are produced, should determine whether Article 2(4) applies (Netherlands 2019).

The most influential formulation is found in Rule 69 of the *Tallinn Manual 2.0*, under which "[a] cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force" (Schmitt 2017, 330). The formulation is deliberately comparative. It does not create a separate threshold for cyberspace but asks whether the operation, judged by its consequences and circumstances, is functionally comparable to a conventional use of force. This avoids making the legality of State conduct dependent upon the physical characteristics of the technology employed. It is also consistent with the broader proposition that the Charter's

Copyright © Oxford Law Review. (editor@oxfordlr.com)

rules governing the use of force apply irrespective of the particular means through which force is exercised (Schmitt 2017, 328–330).

The difficulty lies in determining what consequences are sufficiently grave to satisfy the threshold. Physical injury, death, destruction of property and comparable material damage provide the clearest cases. A cyber operation that causes a dam to release water over a populated area, disables an air-traffic control system resulting in aircraft crashes, or causes a nuclear facility to malfunction in a manner producing substantial physical destruction would possess characteristics closely analogous to conventional military force (Schmitt 2017, 332–334). The decisive consideration in such cases is not that the operation was conducted through computer systems, but that its effects are materially comparable to those produced by conventional force.

More difficult cases arise where a cyber operation causes extensive loss of functionality without physical destruction. A prolonged operation disabling a State's electricity grid, telecommunications network, banking infrastructure or essential governmental systems may impose consequences of considerable national significance even where the underlying hardware remains intact. The legal classification of such operations remains contested. Scholarly analysis has observed that State practice generally accepts a scale-and-effects approach, while uncertainty persists concerning operations producing serious non-physical effects (Tsagourias 2013; Schmitt 2017). The distinction is particularly important because modern States depend upon digital infrastructure for the continuous operation of functions that were previously performed through physical systems. Treating physical destruction as an indispensable condition of "force" could therefore produce an artificial distinction between materially equivalent consequences achieved through different technological mechanisms.

A broader interpretation has consequently been advanced by scholars who argue that substantial loss of functionality should, in appropriate circumstances, be capable of satisfying the threshold. Tsagourias argues that substantial disruption of a system may constitute a use of force where the resulting loss of functionality is sufficiently serious, particularly when critical infrastructure is targeted (Tsagourias 2022). This reasoning is persuasive to the extent that the legal significance of an operation should not depend upon whether functionality is eliminated through physical destruction or through sufficiently serious digital interference. Nevertheless, loss of functionality cannot automatically be equated with force. The duration, extent, recoverability and consequences of the disruption remain relevant to determining its gravity.

The emerging State practice supports a contextual rather than purely mechanical assessment. The United Kingdom considers that the determination must depend upon the facts and circumstances of each operation (United Kingdom 2021). The Netherlands similarly endorses consideration of both qualitative and quantitative factors, including the seriousness and reach of the consequences and the military character of the operation (Netherlands 2019). More recent

Copyright © Oxford Law Review. (editor@oxfordlr.com)

 DOI: https://10.5281/zenodo.22914629

comparative analysis of State positions indicates that an increasing number of States have adopted some form of scale-and-effects methodology, while differing over the significance of non-physical effects and the precise factors that should determine the threshold (Pakkam and Schmitt 2024). This developing practice is important not because it establishes a universally settled test, but because it demonstrates an emerging methodological convergence around effects, gravity and contextual assessment.

The *Tallinn Manual 2.0* provides a useful framework for undertaking that assessment by identifying severity, immediacy, directness, invasiveness, measurability of effects, military character, State involvement and the circumstances surrounding the operation as relevant considerations (Schmitt 2017, 332–337). These factors should not, however, be treated as independent cumulative requirements. Severity remains particularly significant because Article 2(4) is concerned with force rather than every form of coercion. Other considerations assist in determining severity and legal characterisation where the consequences do not provide an unequivocal answer. An operation producing limited and temporary inconvenience would ordinarily remain distinguishable from an operation that disables essential national infrastructure for an extended period, even if both technically involve a cyber intrusion.

The nature of the target may also affect the assessment, although targeting critical infrastructure should not by itself establish a use of force. An intrusion into a military command system, for example, may possess a stronger military character than an intrusion into an ordinary commercial network. Similarly, interference with a hospital, energy facility or air-traffic system may have consequences qualitatively different from temporary disruption of a non-essential service. Yet the legal classification must ultimately remain connected to the operation's actual or reasonably foreseeable consequences rather than the label attached to the target. Otherwise, the threshold could become dependent upon the target's formal status rather than the coercive character of the operation.

The problem of economic effects illustrates the limits of an expansive approach. Severe cyber-induced economic disruption may affect a State's capacity to govern and may produce extensive social consequences, but international law has traditionally distinguished economic and political coercion from armed force. The Netherlands has nevertheless recognised that it cannot presently exclude the possibility that a cyber operation producing a very serious financial or economic impact could qualify as a use of force (Netherlands 2019). This position illustrates the unresolved boundary between economic coercion and force in a digital environment. The more indirect the causal chain between the cyber operation and the resulting harm, the greater the difficulty of characterising the conduct as force without eroding the conceptual distinction between Article 2(4) and other rules of international law.

Copyright © Oxford Law Review. (editor@oxfordlr.com)

The threshold must also be distinguished from that applicable to an armed attack under Article 51. The International Court of Justice established in *Nicaragua* that only the "most grave forms" of the use of force constitute armed attacks, thereby recognising a qualitative and quantitative distinction between the two concepts (Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America) 1986, 101–104). The same distinction is essential in cyberspace. A cyber operation may constitute a prohibited use of force without reaching the higher threshold necessary to trigger the right of self-defence. Treating every Article 2(4) violation as an armed attack would improperly collapse two distinct Charter standards and could substantially expand the circumstances in which States may resort to force in response to cyber operations (Schmitt 2017, 337–342).

Accordingly, the most defensible approach is neither a strict physical-damage requirement nor an unrestricted effects test. The threshold should be determined through a structured assessment of the operation's scale and effects, with particular attention to the severity, directness, immediacy, duration, nature of the target, military character and consequences of the operation. Where the effects are comparable to those produced by conventional force, the technological means employed should not prevent the application of Article 2(4). Where the consequences remain materially below that level, the operation may nevertheless engage other rules of international law, including the prohibitions on intervention or violations of sovereignty (Schmitt 2017, 330–337). The principal legal challenge is therefore not to create a new cyber definition of force, but to apply the existing prohibition in a manner sufficiently sensitive to the distinctive ways in which digital operations can exercise coercive power.

4. Attribution, State Responsibility and the Prohibition of Force in Cyberspace

The application of Article 2(4) to cyber operations depends upon a prior question that is distinctive in practical terms, although not conceptually novel in international law: whether the conduct can legally be attributed to a State. A cyber operation may originate from infrastructure located within a State's territory, employ servers or networks situated in that State, or appear to bear technical characteristics associated with a State, without the operation necessarily constituting an act of that State under international law. The International Law Commission's Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA) establish the general principle that the conduct of State organs is attributable to the State, while conduct of private persons is attributable only in circumstances satisfying the applicable rules of attribution (International Law Commission 2001, arts 2, 4–11). The same principles apply to cyber operations; cyberspace does not create a separate law of attribution.

Copyright © Oxford Law Review. (editor@oxfordlr.com)

This distinction is particularly important because technical attribution and legal attribution are not synonymous. Technical investigation may identify the infrastructure used to conduct an operation, establish the location from which malicious code was deployed, or identify characteristics associated with a particular actor. None of those findings necessarily establishes that the conduct is legally attributable to a State. The UN Group of Governmental Experts expressly recognised that a State may be held responsible for cyber operations conducted by State organs or by entities exercising governmental authority, while operations by non-State actors may be attributable where they are carried out on the State's instructions, direction or effective control (United Nations General Assembly 2021, paras 21–22). The evidentiary difficulty of establishing such a relationship does not alter the underlying legal standard. Attribution is consequently a legal determination based upon evidence rather than a conclusion derived automatically from technical indicators.

The distinction assumes particular significance where States employ proxies. Cyber operations may be conducted through private groups, criminal organisations or ostensibly independent actors, creating deliberate uncertainty concerning the identity of the responsible State. Article 8 of the ARSIWA provides that conduct of a person or group is attributable to a State where that person or group is in fact acting on the instructions of, or under the direction or control of, that State (International Law Commission 2001, art 8). The International Court of Justice has treated the attribution of conduct under this provision as requiring a sufficiently established relationship of State involvement, rather than merely evidence that a State supported or was politically sympathetic towards the relevant actors (Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America) 1986, 109–115). This distinction places an important legal limit on attempts to attribute every cyber operation associated with a State's geopolitical interests to that State.

The problem becomes more complex where a State does not itself conduct a cyber operation but knowingly permits its territory or infrastructure to be used for harmful operations against another State. This situation engages a different legal question from attribution. The UN framework on responsible State behaviour recognises that States should not knowingly allow their territory to be used for internationally wrongful acts using information and communications technologies (United Nations General Assembly 2021). The obligation is therefore capable of arising independently of proof that the harmful operation itself is attributable to the territorial State. This distinction is analytically important: a State may incur responsibility because of its own failure to comply with an international obligation without the underlying cyber operation necessarily becoming an act attributable to that State.

Once attribution has been established, the ordinary law of State responsibility applies. Article 2 of the ARSIWA requires both attributable conduct and breach of an international obligation before an internationally wrongful act exists (International Law Commission 2001, art 2).

Copyright © Oxford Law Review. (editor@oxfordlr.com)

 DOI: https://10.5281/zenodo.22914629

Consequently, attribution does not itself establish a violation of Article 2(4). The relevant cyber operation must first be legally attributable to the State and must then satisfy the substantive threshold of the prohibition of force. The two inquiries should therefore remain separate. A State may be responsible for an internationally wrongful cyber operation that violates another international obligation without having committed a use of force; conversely, where a cyber operation is attributable to a State and reaches the Article 2(4) threshold, the prohibition of force is engaged.

This separation is particularly important in relation to cyber operations conducted through non-State actors. The use of a proxy does not, by itself, remove the operation from the scope of international law. The legal question is whether the evidence establishes the requisite relationship between the State and the conduct. Where such attribution is established, the State cannot avoid responsibility merely because the immediate technical execution was undertaken by a private actor. Conversely, attribution should not be inferred solely from the sophistication of an operation, the identity of the apparent beneficiary, or the geographic origin of digital infrastructure. Maintaining this evidentiary discipline is essential to preventing the law of State responsibility from becoming a mechanism for speculative attribution.

The problem of attribution also bears directly upon the evidentiary requirements associated with the prohibition of force. Cyber operations are often designed to obscure their origin through compromised infrastructure, false digital signatures, intermediary States and deliberately misleading technical indicators. The resulting uncertainty has led scholars and States to emphasise that the legal assessment of a cyber operation may have to proceed on the basis of incomplete evidence. Yet uncertainty of attribution does not lower the legal threshold. The obligation to establish that particular conduct is attributable to a State remains distinct from the strategic or political assessment that a State was probably responsible. International law requires the former if State responsibility is to be legally asserted.

Attribution should therefore be understood as a constitutive element of the legal assessment rather than a preliminary technical exercise. The prohibition in Article 2(4) regulates State conduct, and its application to cyberspace depends upon identifying conduct for which the State bears international legal responsibility. Where a cyber operation is attributable to a State and possesses the scale and effects necessary to constitute force, Article 2(4) may apply notwithstanding the absence of conventional military means. Where attribution is not established, the operation may nevertheless raise questions under other international rules, including obligations relating to sovereignty, non-intervention or due diligence, depending upon the facts.

The relationship between attribution and the prohibition of force consequently reinforces the need for a sequential legal analysis: first, identify the conduct; second, determine whether it is attributable to the State; third, establish whether the attributable conduct breaches Article 2(4); and

Copyright © Oxford Law Review. (editor@oxfordlr.com)

 DOI: https://10.5281/zenodo.22914629

finally, where relevant, determine whether the gravity of that conduct reaches the separate threshold of an armed attack under Article 51. This structure prevents the technological difficulty of identifying cyber actors from obscuring the substantive requirements of State responsibility. It also preserves an important principle of the international legal order: technological anonymity may complicate the application of international law, but it does not alter the legal standards by which State responsibility is determined.

5. Conclusion

The application of Article 2(4) of the UN Charter to cyberspace does not require the creation of a separate legal regime governing digital force. The existing international legal framework is capable of regulating cyber operations, but its application requires careful attention to the distinctive characteristics of cyberspace. The United Nations has expressly recognised that existing international law, including the Charter, applies to State conduct involving information and communications technologies (United Nations General Assembly 2021). The central difficulty therefore lies not in the absence of applicable law, but in determining how established concepts such as force, armed attack, attribution and State responsibility operate when coercive effects can be produced without conventional weapons.

The analysis demonstrates that the legal character of a cyber operation should not depend upon the technological instrument through which it is conducted. An effects-based assessment provides the more coherent basis for applying Article 2(4), particularly where a cyber operation produces death, injury, physical destruction or severe disruption of critical State functions. The assessment should nevertheless remain contextual. Factors such as severity, immediacy, directness, invasiveness, measurability, military character, State involvement and the nature of the target may assist in determining whether the operation is sufficiently comparable to conventional force (Schmitt 2017, 330–337). The UN framework has similarly recognised that cyber operations producing death, injury, physical damage or severe disruption of critical infrastructure may constitute a use of force, while emphasising a case-by-case assessment (United Nations General Assembly 2021).

This approach does not justify treating every serious cyber operation as a violation of Article 2(4). Economic disruption, espionage, political interference and temporary loss of functionality may engage other rules of international law without necessarily reaching the threshold of force. Maintaining the distinctions between prohibited intervention, use of force and armed attack is therefore essential. In particular, the higher threshold applicable to an armed attack under Article 51 must remain analytically distinct from the broader prohibition contained in Article 2(4). The existence of a use of force does not, without more, establish a right of self-defence.

Copyright © Oxford Law Review. (editor@oxfordlr.com)

 DOI: https://10.5281/zenodo.22914629

Attribution presents a separate but indispensable stage of the analysis. Technical evidence indicating the origin or infrastructure associated with a cyber operation cannot automatically establish legal attribution to a State. The ordinary rules of State responsibility apply: attributable conduct must exist and that conduct must constitute a breach of an international obligation (International Law Commission 2001, art 2). The UN's work on responsible State behaviour similarly recognises attribution as a necessary condition for holding a State internationally responsible for a cyber operation (United Nations General Assembly 2021). The distinction between technical attribution and legal attribution is consequently fundamental to any lawful assessment of State responsibility.

The principal conclusion is therefore that cyberspace changes the means through which force may be exercised, but it does not alter the fundamental legal standard governing the resort to force. Article 2(4) should remain technologically neutral while legally disciplined. A cyber operation should be characterised according to its scale, effects and relevant circumstances, rather than according to the absence of a conventional weapon. At the same time, the threshold must remain sufficiently demanding to preserve the distinction between force and other forms of unlawful State conduct.

The future development of the law will depend significantly upon State practice and the articulation of *opinio juris*. Existing State positions already demonstrate substantial agreement that international law applies to cyber operations, while disagreement persists over the precise threshold at which non-physical cyber effects constitute force. This developing practice should therefore be treated neither as evidence that the law is wholly unsettled nor as establishing a universally accepted test. The more defensible position is that Article 2(4) provides an existing legal framework whose application to cyberspace is progressively being specified through State practice, international institutional processes and scholarly interpretation.

Ultimately, the legitimacy of applying Article 2(4) to cyberspace depends upon preserving both effectiveness and restraint. The prohibition must be capable of addressing technologically mediated coercion that is materially equivalent to conventional force, but it must not be expanded so broadly that every significant cyber incident becomes an act of force. A carefully calibrated effects-based and contextual approach best preserves this balance, allowing the Charter's prohibition to remain effective in a changing technological environment while maintaining the legal distinctions upon which the international law governing the use of force depends.

Copyright © Oxford Law Review. (editor@oxfordlr.com)

References

International Court of Justice. 1986. *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)*, Merits, Judgment, I.C.J. Reports 1986, p. 14.

International Court of Justice. 2005. *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda)*, Judgment, I.C.J. Reports 2005, p. 168.

International Law Commission. 2001. *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*. Report of the International Law Commission on the Work of Its Fifty-Third Session, UN Doc A/56/10. New York: United Nations.

Kingdom of the Netherlands. 2019. *Appendix: International Law in Cyberspace*. Letter from the Minister of Foreign Affairs to the President of the House of Representatives, 26 September 2019.

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

Schmitt, Michael N., and Anusha S. Pakkam. 2024. "Cyberspace and the Jus ad Bellum: The State of Play." *International Law Studies* 103: 194–229.

Tsagourias, Nicholas. 2012. "Cyber Attacks, Self-Defence and the Problem of Attribution." *Journal of Conflict and Security Law* 17 (2): 229–244. doi:10.1093/jcsl/krs019.

Tsagourias, Nicholas. 2012. "The Tallinn Manual on the International Law Applicable to Cyber Warfare: A Commentary on Chapter II—The Use of Force." *Yearbook of International Humanitarian Law* 15: 19–43. doi:10.1007/978-90-6704-924-5_2.

Tsagourias, Nicholas. 2023. "Digitalization and Its Systemic Impact on the Use of Force Regime: Legal Uncertainty and the Replacement of International Law." *German Law Journal* 24 (3): 494–507.

United Kingdom Foreign, Commonwealth & Development Office. 2021. *Application of International Law to States' Conduct in Cyberspace: UK Statement*. London: Foreign, Commonwealth & Development Office, 3 June 2021.

United Nations. 1945. *Charter of the United Nations*. San Francisco, 26 June 1945. 1 UNTS XVI.

United Nations General Assembly. 2021. *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. New York: United Nations.

Copyright © Oxford Law Review. (editor@oxfordlr.com)

 DOI: https://10.5281/zenodo.22914629

United Nations General Assembly. 2021. *Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States*. UN Doc A/76/136. New York: United Nations.

Publisher's Note

Oxford Law Review remains neutral with regard to jurisdictional claims in published maps and institutional affiliations. Oxford Law Review or its licensors retain the rights to this article pursuant to the applicable publishing agreement with the author(s) or other rightsholder(s). Any self-archiving, reproduction, distribution, or reuse of the accepted manuscript or published version is subject to the terms of the applicable publishing agreement and applicable law.