REVIEW OF LAW AND SOCIAL SCIENCES
ISSN (O): 3078-1574, ISSN (P): 3078-610X
Vol. 4, No. 1, 2026, 47-62
https://doi.org/10.71261/rlss/4.1.470.62

# Research on the Interpretation of Customary International Law in Cyberspace: Dilemmas and Solutions

Fenghua Yu[1]

**Abstract**

In recent years, the international community has reached a preliminary consensus on the application of customary international law (CIL) to cyberspace. However, discussions have now entered the deep waters of interpreting specific rules regarding how it applies. Traditionally, the interpretation of CIL is primarily divided into two methods: induction and deduction. Concerning the two constitutive elements of CIL—state practice and opinio juris—the inductive method requires a high degree of consistency in state practice. In cyberspace, inconsistency in state practice is prominent. Strict adherence to induction would make it difficult to genuinely form a CIL norm. The deductive method can relax this requirement, but due to the lack of specific standards regarding the permissible extent of deduction, it is highly susceptible to the adverse influence of power politics in cyberspace, potentially leading to the "hollowing out" of CIL norms. At this juncture, introducing John Rawls' "reflective equilibrium" to interpret the constitutive elements of CIL in cyberspace can address the shortcomings of both deduction and induction. Their combination can provide an analytical tool balancing stability and flexibility for interpreting CIL's constitutive elements, thereby promoting the shift of CIL in cyberspace from "hollowing out" to "substantialization."

**Keywords:** Cyberspace, customary international law, interpretation, deduction, and induction.

## Introduction

Currently, the global governance of cyberspace faces structural challenges. On the one hand, the coverage of cyberspace treaties is limited. In the field of cybercrime, the *United Nations Convention against Cybercrime* adopted in August 2024 established a global legal framework for cybercrime and data access, integrating regional cybercrime treaties such as the *Budapest Convention on Cybercrime*, the *Arab League Convention on Combating Information Technology Crimes*, and the *Shanghai Cooperation Organization Agreement on Cooperation in Ensuring International Information Security*. However, regarding principles like the prohibition of the use of force, non-intervention in internal affairs, and peacetime espionage activities, the global governance of cyberspace still relies on CIL norms for regulation. On the other hand, there is a proliferation of soft law in cyberspace but with insufficient binding force. Consensus reports from mechanisms like the UN Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG), as well as expert documents like the *Tallinn Manual 2.0*, have formed some consensus on regulating state behavior in cyberspace. However, due to their non-treaty nature, they lack enforceability. This "soft law governance" model often struggles to form effective constraints on core issues such as state-sponsored cyberattacks and critical infrastructure protection. Therefore, discussing CIL in cyberspace holds significant practical relevance.

[1] Xiamen University, China. Email: yufh01@126.com . ORCID: https://orcid.org/0009-0009-8306-7123

Although the commentary to the International Law Commission's (ILC) *Draft conclusions on identification of customary international law* only mentions induction and deduction, during the discussions on the draft, different members of the Commission repeatedly used the term "interpretation."(ILC 2014; ILC 2013) Special Rapporteur Sir Michael Wood noted: "Speaking of the interpretation of customary international law, to determine the existence and content of a rule of customary international law is, as it were, to engage in interpretation."(ILC 2017)The interpretation of CIL in cyberspace refers to the process of determining the existence and specific content of CIL rules in this special domain. Although a few foreign scholars have focused on the preliminary application of CIL in cyberspace, attention to its interpretation remains insufficient. In 2007, Professor PP Polanski, in his book *Customary Law of the Internet: In the Search for a Supranational Cyberspace Law*, proposed that in the supranational cyberspace, a spontaneous, community-driven normative system has emerged, possessing many characteristics of "law." He termed this normative system "Internet customary law."(Polanski, P. 2007) However, this customary law differs from CIL as a formal source of international law. In 2023, Professor Ori Pomson criticized the attempt to simply "interpret" existing CIL rules and directly apply them to cyber activities, arguing that one must return to the two elements of "state practice" and "*opinio juris*."(Pomson, O. 2023) Professor Pomson's research reaffirms that interpreting CIL in cyberspace must have reference standards and combine with the traditional "two-element theory" to achieve a scientific interpretation process. However, Professor Pomson did not answer how to conduct interpretive reasoning in cyberspace given the inconsistency in state practice, thus leaving room for subsequent research. Domestically, scholars like Cheng Le and Zhang Hua have analyzed the particularities of cyberspace and the application paths of specific principles therein, but they have yet to provide more optimized solutions from a methodological perspective based on the characteristics of cyberspace.(Cheng, Le 2025; Zhang, Hua 2022)

This paper starts from the basic theory of CIL interpretation. By dissecting the typological distinction and comparison between inductive and deductive methods in interpreting CIL in cyberspace, it reveals the root causes and manifestations of the interpretative dilemma. It then explores the choice of interpretative methods for CIL in cyberspace, using concrete examples such as the principle of prohibition of the use of force. Finally, it introduces Rawls' "reflective equilibrium" as a potential solution to the interpretative problems of CIL in cyberspace, hoping to provide a theoretical reference for advancing the development of CIL in cyberspace.

## I. The Dilemma of Interpreting Customary International Law in Cyberspace

The identification and interpretation of CIL have long been challenging issues in international law theory. In cyberspace, this emerging domain, traditional interpretative methods face even more severe challenges. Currently, the international legal academia has mainly formed two methods for interpreting CIL: induction and deduction (Worster, WT 2024). Each has its theoretical foundation, operational path, and applicable limitations, presenting distinct typological characteristics in the cyberspace context.

## (I) The Inductive Method

The inductive method, as a bottom-up interpretative approach, (Editorial Group of Jurisprudence, 2017) focuses on observing and analyzing states' specific practices, statements, and interactive behaviors in cyberspace to distill universal rules or principles. This method highly values empirical data and experiential observation, relying on the collection, organization, and analysis of extensive state practice.

In the cyberspace context, applying induction involves systematic study of national cyber policies, position papers, official statements, actual cyber operations, and international reactions. For example, by analyzing the responses of multiple states to cyber operations like Distributed Denial-of-Service (DDoS) attacks, critical infrastructure intrusions, and data theft, and the international community's reactions, one might induce what cyber activities could constitute "use of force" or "intervention in internal affairs" under international law. For instance, New Zealand released a document in 2020 titled *Application of International Law to State Activities in Cyberspace*, dividing cyberspace into two categories: "physical domain" and "cyber domain." The document states that the legal binding force of sovereignty principles in the physical domain is established through norms like the prohibition of the use of force, non-intervention, and territorial sovereignty. In contrast, the legal effect in the cyber domain primarily manifests through the principles of prohibition of the use of force and non-intervention. Simultaneously, the document cautiously suggests that the cyber domain might refer to the principle of territorial sovereignty, but its precise scope of effect needs further clarification through state practice.[2] In other words, New Zealand believes the scope of the prohibition of the use of force and non-intervention principles in the cyber domain requires further induction from state practice.

However, the inductive method faces significant limitations in interpreting CIL in cyberspace. Firstly, state practice in cyberspace is characterized by opacity and asymmetry. Many states keep their cyber capabilities and operations confidential, leading to limited observable practice samples that may lack representativeness. Secondly, rapid technological iteration means state practice often lags behind technological development, so rules induced may be outdated when formed, unable to adapt to new forms of cyber threats. More crucially, disparities in national cyber capabilities mean the practices of technologically advanced states may be overrepresented during induction, leading to unfair rules.

## (II) The Deductive Method

Contrary to induction, the deductive method adopts a top-down interpretative approach, (Editorial Group of Jurisprudence 2017) starting from

[2] See National position of New Zealand (2020) - International cyber law: interactive toolkit. International Cyber Law: Interactive Toolkit. https://cyberlaw.ccdcoe.org/wiki/National_position_of_New_Zealand (accessed 5 September 2025).

existing general principles, rules, or theoretical frameworks of international law and applying them to specific scenarios in cyberspace through logical deduction. This method emphasizes the coherence of legal principles and the integrity of the system, assuming that international law principles from the physical realm can be extended to cyberspace.

In interpreting CIL in cyberspace, a typical application of deduction is the deductive application of basic principles from the *UN Charter*, such as sovereign equality, prohibition of the use of force, and non-intervention, to cyberspace. For example, based on deductive logic, some scholars argue that since Article 2(4) of the *UN Charter* prohibits the use of force, and this provision "does not refer to specific weapons and applies to any use of force, regardless of the weapon,"(Zhang, Hua 2022) then cyberattacks with similar destructive effects should naturally fall within the scope of "use of force."

However, applying deduction in cyberspace also faces challenges. First, the fundamental differences between cyberspace and physical space mean simple analogy may lead to rule misfit. For instance, the effects of cyber operations are often non-kinetic, reversible, and non-intuitive, significantly different from the physical destruction of traditional armed conflict. Second, traditional international law principles may have ambiguous meanings in the cyber context. There is still a lack of international consensus on the specific connotation and extension of core concepts like "force," "attack," and "sovereignty" in cyberspace. Precisely because of this, some scholars criticize over-reliance on deduction as potentially leading to "doctrinal expansion," neglecting the particularities of cyberspace, and even becoming a legal tool for some states to promote their cyber strategies (Cheng, Le 2025).

### (III) Comparison of the Two

Comparing the two interpretative methods, we can clearly see the core dilemma of interpreting CIL in cyberspace: on the one hand, induction, while reflecting the practical characteristics of cyberspace, is constrained by the opacity and asymmetry of state practice, making it difficult to form universally binding rules; on the other hand, deduction, while providing a clear legal framework, may neglect the particularities of cyberspace, leading to a disconnect between rules and practice. The root of this dilemma lies in the inherent tension between the unique attributes of cyberspace itself—the interweaving of virtuality and reality, enhanced technicality, and blurred sovereign boundaries—and the traditional theoretical architecture of international law based on state sovereignty and territory.

Specifically, the dilemma in interpreting CIL in cyberspace manifests at three levels: First, the dilemma of rule identification. Which state practices can constitute the basis for forming CIL? Can the behavior of technology companies be considered state practice? The virtuality of cyberspace makes traditional state practice difficult to observe and assess directly. Second, the dilemma of content determination. How to define the specific content and scope of application of CIL rules in cyberspace? For example, how should the concept of "force" in the prohibition of the use of force principle be interpreted in cyberspace? What is its threshold standard? The answers to these questions directly affect content determination. Third, the dilemma of interpretative authority. Who has the authority to interpret CIL rules in cyberspace? In cyberspace, non-state actors, such as technical expert communities and standard-setting organizations, play an increasingly important role in rule formation and interpretation, challenging the state-dominated traditional interpretative mechanism.

## III. The Choice of Interpretative Methods for Customary International Law in Cyberspace

### (I) General Discussion on Choosing Interpretative Methods for CIL in Cyberspace

Facing the dilemma of interpreting CIL in cyberspace, exclusive reliance on either induction or deduction shows limitations. Therefore, the choice of interpretative method should not be an exclusive binary one but should seek a path of dynamic balance. This balance must fully consider both the technical characteristics and practical developments of cyberspace while ensuring the continuity and predictability of rules.

In the interpretation process of CIL in cyberspace, one should first acknowledge the complementary value of both methods. Induction provides an empirical basis for identifying CIL by analyzing specific cyber practices, such as national position papers, responses to cyber incidents, and policy statements. Deduction provides a normative framework for behavioral expectations by applying established international law principles, such as sovereignty, non-intervention, and prohibition of the use of force, to cyberspace. Their organic combination avoids the rule fragmentation induction may cause and prevents the rule rigidity deduction may bring.

It is worth noting that discussions within the international community on the application of international law in cyberspace show a trend shifting from theoretical debate to practice-oriented approaches. Intergovernmental processes under the UN framework, such as UNGGE and OEWG, as well as position papers gradually released by various states, provide rich practical material for induction.[3]Simultaneously, academic efforts like the *Tallinn Manual* attempt to construct a systematic framework for international law in cyberspace through deductive logic. These two paths are not diametrically opposed but shape each other through interaction—state practice provides material for theoretical deduction, and theoretical frameworks guide practice.

When choosing interpretative methods for CIL in cyberspace, special attention must also be paid to context sensitivity. Different areas of cyber activity, such as cyber espionage, economic theft, and critical infrastructure attacks, may require different combinations of interpretative methods. For example, for cyber espionage activities, due to the lack of consistency and frequent secrecy of state practice, applying induction faces challenges, potentially requiring more reliance on deductive reasoning. For cyberattacks causing physical damage, it is easier to identify rules from state practice through induction.

[3] See A/RES/80/16, https://docs.un.org/zh/A/RES/80/16 (accessed 8 January 2026).

### (II) Illustration Using the Principle of Prohibition of the Use of Force as an Example

The principle of prohibition of the use of force, as a fundamental principle of international law, presents particularly complex issues regarding its application in cyberspace, providing a typical example for understanding the choice of interpretative methods for CIL in cyberspace. Article 2(4) of the *UN Charter* clearly states: "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." However, how this principle applies to cyberspace, particularly how to define cyber behavior constituting "use of force," remains a point of divergence within the international community.

In interpreting how the prohibition of the use of force applies to cyberspace, three main doctrines have emerged internationally: the "instrument-based approach," the "target-based approach," and the "effects-based approach."(Zhang, Hua 2022) The "instrument-based approach" insists that "use of force" should be understood from the perspective of the weapons and means used. As long as a cyberattack can cause damage similar to that caused by a kinetic weapon attack, the use of a "cyber weapon" constitutes "use of force." The "target-based approach" argues that attacks targeting a state's critical infrastructure constitute use of force. The "effects-based approach" focuses on the consequences of a cyberattack, positing that any cyberattack causing violent consequences like casualties and property damage constitutes use of force, regardless of the target and without needing to compare similarity to traditional kinetic weapon attacks.

In recent years, the "effects-based standard" has become increasingly mainstream, as evidenced in the two *Tallinn Manuals* compiled by the International Group of Experts invited by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Rule 11 of the *Tallinn Manual on the International Law Applicable to Cyber Warfare* and Rule 69 of the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* use identical wording: "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." Since 2019, in position papers on the application of international law in cyberspace, states have also tended to adopt the effects-based standard, arguing that "cyber operations that are comparable in scale and effects to traditional military operations should also fall within the prohibition of Article 2(4) of the UN Charter."(Schmitt, M 2017).

The mainstreaming of the effects-based standard reflects the interweaving of induction and deduction. On the one hand, the proposal of the effects-based standard itself originates from the deductive interpretation of Article 2(4) of the *UN Charter*—since the provision does not limit the specific form of force, then cyber operations with similar effects naturally fall within its regulatory scope. On the other hand, the process of this standard gaining state acceptance reflects the logic of induction—confirming the degree of acceptance through observing state practice, such as position papers and reactions to specific cyber incidents.

However, applying the effects-based standard in cyberspace still faces multiple legal uncertainties. First, what are the specific measurement criteria for "scale and effects"? The effects of cyber operations may be delayed, diffuse, and non-physical; do these constitute components of "effects"? Second, is the effects-based standard sufficient to cover all cyber uses of force that should be regulated? For example, interference with electoral systems may not affect physical infrastructure but seriously infringe upon a state's political independence. Addressing the limitations of the effects-based standard, scholars have proposed a "contextualist approach" as a supplement. This approach emphasizes case-by-case analysis, comprehensively considering various factors such as the specific context, technical characteristics, target, intent, and consequences of a cyber operation, rather than relying solely on the effects-based standard (Zhang, Hua 2022). The contextualist approach essentially represents a return to induction—forming a more refined rule system through specific analysis of the nature of cyber operations in different contexts. Simultaneously, it absorbs the strengths of deduction—using the fundamental values of the prohibition of the use of force principle as guidance to ensure interpretative coherence.

The interpretative journey of the prohibition of the use of force principle in cyberspace indicates that the choice of interpretative methods for CIL in cyberspace should be a dialectical, comprehensive process—using deduction to establish the basic framework and core values, using induction to enrich specific content and applicable standards, and then achieving continuous adaptation of rules to reality through contextualized case analysis. This comprehensive method respects the stability of traditional international law while accommodating the developmental nature of cyberspace, potentially offering a feasible path to resolve the interpretative dilemma of CIL in cyberspace.

## IV. The Way Forward for Interpreting Customary International Law in Cyberspace: Introducing Reflective Equilibrium

### (I) The Theoretical Framework and Applicable Value of Reflective Equilibrium

Facing the difficulty of the contextualist path in making precise trade-offs in individual cases, this paper proposes introducing the theory of reflective equilibrium as theoretical guidance, aiming to construct a more reasonable and effective interpretative path. Reflective equilibrium originates from moral philosophy and legal theory, emphasizing repeated adjustment and revision between general principles and specific judgments until a coherent state between the two is achieved. This theoretical method, developed by John Rawls among others, focuses on achieving dialectical unity between theory and practice through continuous movement between belief systems at different levels of abstraction (Rawls, J 1971).

Applying reflective equilibrium to the interpretation of CIL in cyberspace holds significant applicable value. First, it provides a middle path that transcends the induction-deduction dichotomy. In the process of reflective equilibrium, existing international law principles, such as sovereign equality and prohibition of the use of force, serve as "provisional fixed points" providing initial guidance for interpretation. Specific cyberspace practices and national judgments serve as "objects of scrutiny" constantly testing and revising the applicability of these principles. Through this two-way adaptation, one can avoid the excessive abstraction and rigidity of deduction and overcome the fragmentation and uncertainty of induction.

Second, reflective equilibrium aligns with the multi-stakeholder participation characteristic of cyberspace governance. The global and technical nature of cyberspace dictates that its rule formation and interpretation must balance national interests, technological feasibility, and ethical values. Reflective equilibrium requires interpreters to fully consider the perspectives and positions of different stakeholders, seeking overlapping consensus through repeated weighing, which highly coincides with the multilateralism principle of cyberspace governance.

Third, reflective equilibrium adapts to the dynamic nature of technological development in cyberspace. As cyber technology evolves rapidly and threat forms constantly change, the interpretation of CIL needs a degree of flexibility and foresight. Reflective equilibrium is not a closed argumentative system but an open, continuous process capable of adjusting the interpretative framework with technological development and practical accumulation, maintaining the timeliness of rules.

### (II) Specific Application of Reflective Equilibrium in Interpreting CIL in Cyberspace

In interpreting CIL in cyberspace, the application of reflective equilibrium can be realized through a three-layer structure: initial judgment, reflective adjustment, and equilibrium attainment.

In the *initial judgment* stage, interpreters first form a preliminary interpretation of a specific CIL rule based on existing international law principles and state practice. Taking the prohibition of the use of force principle as an example, the initial judgment might be adopting the effects-based standard, i.e., considering cyber operations causing significant physical damage as constituting use of force. This judgment stems both from deductive interpretation of Article 2(4) of the *UN Charter* and references the mainstream trend presented in national position papers.

In the *reflective adjustment* stage, interpreters need to compare the preliminary interpretation with counter examples, exceptional situations, and critical opinions, and revise the interpretative scheme based on the examination results. Continuing with the prohibition of the use of force example, when applying the effects-based standard to cyber operations like data theft or electoral interference that do not cause physical damage but may have severe impacts, interpreters will find the insufficiency of a single effects-based standard. This necessitates introducing other factors, such as "nature of the target" (whether it targets critical infrastructure), "intent of the conduct" (whether it aims to infringe territorial integrity or political independence), etc., to supplement or revise the preliminary interpretation.

In the *equilibrium attainment* stage, interpreters seek a coherent interpretative scheme that achieves maximum coordination between general principles and specific judgments. This scheme should be acceptable to most members of the international community while maintaining internal consistency within the rule system. For example, in interpreting the prohibition of the use of force principle, a tiered interpretative scheme might be formed: cyber operations causing physical damage uniformly constitute use of force; for operations not causing physical damage but producing similarly severe effects, a comprehensive judgment considering factors like target, intent, and consequences is needed.

### (III) Constructing an Interpretative Path Based on Reflective Equilibrium

Based on the theoretical framework of reflective equilibrium, a more systematic interpretative path for CIL in cyberspace can be constructed. This path includes the following key steps:

*First*, comprehensive utilization of diverse evidence. Reflective equilibrium requires interpreters to go beyond traditional materials of state practice and widely incorporate various forms of evidence, including: national position papers, resolutions of international organizations, judicial precedents, academic discourse, technical standards, and practices of non-state actors. This diverse evidentiary base enriches the sources for identifying customary law and enhances the democracy and legitimacy of interpretation. As scholars have pointed out, "States and international organizations, in the process of applying international law, need the assistance of non-state actors regarding technology and related norms to enhance the applicability of state responsibility law in cyberspace."(Liu, B. 2020).

*Second*, establishment of an iterative interpretative process. Reflective equilibrium is a continuous, dynamic process, not a one-time act. In interpreting CIL in cyberspace, an iterative interpretative mechanism should be established, allowing for continuous revision of the interpretative scheme based on new cyber practices, technological developments, and value considerations. This iterative process can be realized through periodic review mechanisms under the UN framework, such as the UNGGE and OEWG processes, enabling CIL interpretation to keep pace with the times.

*Third*, design of differentiated interpretative schemes. The diversity of cyber activities dictates that interpreting CIL may require designing differentiated schemes based on the characteristics of different fields. For example, interpreting CIL in the realm of cyber armed conflict may need to emphasize the dominant role of deduction to ensure consistency with the basic principles of International Humanitarian Law. For lower-intensity activities like cyber economic espionage, induction may be more suitable, forming specific rules gradually through analysis of state practice. This differentiated approach embodies the "context sensitivity" of reflective equilibrium.

China should actively participate in the formulation of international rules for cyberspace, enhancing its discourse power and influence in constructing the international order of cyberspace. Based on reflective equilibrium, China can propose interpretations of CIL in cyberspace that integrate Chinese characteristics with an international perspective. For example, in interpreting the prohibition of the use of force principle, China can advocate for a "contextualist approach," arguing for comprehensive consideration of various factors such as the nature, target, and effects of cyber operations, avoiding the excessive militarization tendency a single standard might cause. Simultaneously, China can promote establishing a multilateral consultation mechanism for interpreting CIL in cyberspace under the UN framework, ensuring the democratic nature of the interpretative process and the fairness of its outcomes.

## V. The Elaboration of Interpreting Customary International Law in Cyberspace: A Concrete Example

The principle of non-intervention in internal affairs, as a fundamental principle of international law, faces fundamental challenges in its interpretation in cyberspace. According to Article 2(7) of the *UN Charter*, this principle prohibits intervention "in matters which are essentially within the domestic jurisdiction of any state." Traditionally, this principle mainly focused on tangible forms of intervention like military intervention, political subversion, and economic coercion. However, "intervention" in cyberspace presents new characteristics of being technicalized, concealed, and normalized, making the traditional interpretative framework difficult to apply directly.

Starting from the initial judgment of reflective equilibrium, the preliminary consensus formed within the international community is: the principle of non-intervention in cyberspace should continue its core value of protecting states' political independence and right to autonomously choose their social systems. The 2015 report of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE) pointed out that the principle of state sovereignty applies to cyberspace and that state sovereignty implies a state's jurisdiction over cyber infrastructure within its territory. This consensus serves as our "provisional fixed point" for interpretation.

However, when directly mapping this traditional principle onto cyberspace, we immediately face the dilemma of conceptual ambiguity. What constitutes "internal affairs" in cyberspace? Do cyber public opinion guidance, regulation of cross-border data flow, and election system security fall within the scope of "internal affairs"? What kind of cyber behavior constitutes "intervention"? Is it cyberattacks, data theft, or information manipulation? These fundamental questions lack international consensus, reflecting the limitations of simple deductive extension.

States have significant differences in defining "intervention" in cyberspace. These differences stem from both imbalances in technological capabilities and deep-seated divergences in value positions. China tends to emphasize "cyber sovereignty", advocating that the state has comprehensive jurisdiction over online activities within its territory and opposing any form of information hegemony. [4]In documents such as the "International Strategy of Cooperation in Cyberspace", China clearly states its core concern as safeguarding national sovereignty and security in cyberspace. Russia promotes "information sovereignty", viewing information security as an

[4] Strategic Plan for International Cooperation in Cyberspace, https://www.mfa.gov.cn/web/wjb_673085/zzjg_673183/jks_674633/zclc_674645/qt_674659/201703/t20170301_7669140.shtml (accessed 8 January 2026).

important part of national security and explicitly opposing external "digital interference". The core of the draft "United Nations Convention on Information Security" and other documents it has pushed for lies in maintaining traditional sovereignty principles in the information space. [5]The United States and its Western allies focus on "cyber freedom", advocating the free flow of information and usually taking a cautious stance on the definition of "interference", while emphasizing the need to consider the intent and coercive elements of the behavior. The "Tallinn Manual 2.0" and relevant position papers of the US State Department prominently reflect their core concerns about freedom of speech and the openness of the Internet. [6]The non-aligned movement countries (often represented by the Group of 77) are concerned about preventing "digital colonialism" and technological hegemony, emphasizing the need to take into account the special needs of developing countries in the digital age. The core demands of their related statements are to promote technological equality and bridge the digital divide. [7]The table below outlines the different tendencies of major states or groups on this issue:

**Table Caption：Tendency of Magor States in Defining "Cyber Intervention"**

| **State/Group** | **Tendency in Defining "Cyber Intervention"** | **Representative Position Documents** | **Core Concerns** |
|---|---|---|---|
| **China** | Emphasizes "cyber sovereignty," advocates for comprehensive state jurisdiction over domestic cyber activities, opposes information hegemony. | *International Strategy of Cooperation on Cyberspace* | National sovereignty and security in cyberspace. |

[5] As early as 2000, the Russian Federation underlined that the Armed Forces were ‘guided’–and ‘with respect to the peculiarities of military activity in the global information space’–by the principle of ‘non-interference in the internal affairs of other States’. See Russian Federation Armed Forces’ Information Space Activities Concept’, http://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle (accessed 8 January 2026).

[6] National position of the United States of America (2024), https://cyberlaw.ccdcoe.org/wiki/National_position_of_the_United_States_of_America_(2024)?section=13 (accessed 8 January 2026).

[7] Statements by the Chair of the Group of 77, https://www.g77.org/statement/ (accessed 8 January 2026).

| State/Group | Tendency in Defining "Cyber Intervention" | Representative Position Documents | Core Concerns |
|---|---|---|---|
| **Russia** | Advocates "information sovereignty," considers information domain security a component of national security, opposes "digital intervention." | Draft *UN Convention on International Information Security* | Traditional sovereignty principles in information space. |
| **US & Western Allies** | Focuses on "cyber freedom," advocates free flow of information, adopts a cautious stance on defining intervention, emphasizes intent and coercive elements. | *Tallinn Manual 2.0*, US State Department position papers | Freedom of expression and an open internet. |
| **Non-Aligned Movement** (often represented by G77) | Concerned about "digital colonialism" and technological hegemony, emphasizes the special needs of developing countries. | Relevant statements by the Group of 77 | Technological equality and bridging the digital divide. |

Overall, these positional differences constitute the main lines of the current international rule contestation in cyberspace, with profound disagreements among parties regarding the prioritization of values such as sovereignty, security, freedom, and development. (See table above)

Based on the equilibrium attainment stage of reflective equilibrium, there is a need to construct a tiered interpretative framework that neither detaches from the core value of the non-intervention principle nor fails to respond to the characteristics of cyberspace.

**(I) Core Layer: Prohibition of Coercive Cyber Intervention**

Cyber operations with a coercive nature aimed at forcing the target state to change its policy choices should be clearly identified as violating the non-intervention principle. Interpretation at this level is relatively clear, drawing lessons from the "effects-based standard" of the prohibition of the use of force principle. Prohibited coercive cyber intervention can be divided into *direct coercion* and *indirect coercion*. *Direct coercion* refers to directly interfering in another state's internal affairs through violence, coercion, or other means, such as paralyzing government systems through cyberattacks to force policy changes or manipulating election results to directly impact the political process. *Indirect coercion* refers to interfering in another state's internal affairs through indirect means, such as systematic data theft placing the target state at a disadvantage in negotiations or using cyber operations to create social unrest to exert political pressure.

### (II) Intermediate Layer: Prudent Treatment of Influential Cyber Activities

For cyber activities lacking direct coerciveness but potentially having intervention effects, a multi-factor balancing test needs to be established. This test framework centers on *intent, nature, and impact of the activity*, while also considering *target attributes* and *technical characteristics*, using *transparency* as a reference, forming a multi-level, focused comprehensive evaluation system. Specifically, the highest-weight core considerations include: *Intent of the conduct*—whether there is a clear purpose to change the target state's policy or political process; *Nature of the conduct*—whether deceptive, coercive, or destructive malicious means are employed; and *Degree of impact*—the actual consequences for the target state's political independence and autonomous decision-making. For example, manipulating public opinion via social media or disseminating disinformation affecting voter cognition requires comprehensive judgment considering factors like scale, coordination, and attribution clarity. Small-scale, dispersed information dissemination may fall within the scope of freedom of expression, but large-scale, organized "information operations" led by foreign governments may constitute intervention. These three are regarded as key judgment factors. Medium-weight indicators include *target sensitivity* and *technical means*, focusing on whether the conduct targets highly sensitive political processes like elections or sovereign decision-making, and whether it employs technical attack methods like vulnerability exploitation or malware. *Transparency* serves as a low-weight auxiliary indicator, primarily examining whether the conduct is open/transparent and can be clearly attributed to a specific actor, with relatively limited influence in the overall assessment.

This multi-factor consideration avoids excessive expansion of the "intervention" concept, preventing normal cyber activities like diplomatic criticism or information exchange from being inappropriately labeled as intervention, while providing finer judgment standards for technically complex cyber operations.

### (III) Outer Layer: Promoting Norms of Responsible State Behavior

The core objective of outer layer norms is to address cyber activities that have not yet reached the legal threshold of "intervention" but may erode international trust, trigger miscalculation, or undermine long-term stability. For this "gray zone," direct regulation by hard law is often inadequate and prone to controversy. Therefore, it is necessary to guide and regulate through soft law mechanisms and Confidence-Building Measures (CBMs), essentially establishing a preventive, cooperative international culture of behavior. For example, regarding norms for cross-border data flow, it is necessary to balance free data flow with state data sovereignty, seeking a balance between local storage of important data and global data circulation. Here, extreme positions of "absolute free flow" or "comprehensive local storage" are both undesirable. Outer layer norms should strive to build a tiered, classified, risk-oriented governance framework, focusing on "*classification management*" and "*risk control*": Advocate for states to establish tiered management systems based on data sensitivity. For general commercial data, promote establishing efficient, secure cross-border flow mechanisms. For "important data" involving critical infrastructure, national security, or significant public interest, recognize states' rights to adopt necessary localization measures, but such measures should be transparent, non-discriminatory, and proportionate. Another example: Regarding norms for cyber information governance, distinctions should be made between disinformation, propaganda warfare, and legitimate expression, avoiding the suppression of freedom of expression under the guise of "countering intervention." It is advocated that regulation of information content should primarily target actions with clear malicious intent, such as intentionally inciting violence, undermining social stability, interfering in elections, and likely causing provable substantive harm, rather than viewpoints or stances based on content. The governance focus should be on state-supported or led, large-scale, coordinated malicious information operations, not individual erroneous statements.

## VI. China's Position on Interpreting Customary International Law in Cyberspace: Based on Reflective Equilibrium

As a major cyber power, China, guided by reflective equilibrium, can propose an interpretative scheme that both adheres to core principles and possesses practical flexibility, contributing key ideas to constructing clear norms for non-intervention in cyberspace.

*Upholding cyber sovereignty as the cornerstone and logical starting point of the non-intervention principle.* Cyber sovereignty is the natural extension of state sovereignty in cyberspace. It clarifies a state's exclusive jurisdiction over cyber infrastructure, data, and activities within its territory, providing the fundamental spatial boundary and legal basis for determining the scope of "internal affairs." China should advocate that equal cyber sovereignty is the prerequisite for resisting any form of cyber hegemony and external intervention, and it is also the solid foundation for maintaining a stable global cyberspace order.

*Establishing a tiered, differentiated responsibility framework based on the nature of conduct.* Faced with complex types of cyber behavior, a single standard is ineffective. China's approach advocates precise differentiation: For behaviors with clear malice and destructiveness like cyberattacks, the non-intervention principle should be strictly applied, and efforts should be made to promote internationally recognized attribution and accountability mechanisms. For "gray zone" areas like cross-border data flow and information dissemination, "responsible state behavior norms" should be formulated through multilateral consultation to avoid subjective presumption and unilateralism. For unknown challenges brought by new technologies like AI, advocate establishing inclusive, forward-looking international dialogue platforms to dynamically balance multiple values such as security, development, and openness.

*Actively leading the multilateral consensus-shaping process centered on the United Nations.* The vitality of principles lies in universal recognition. China should proactively promote establishing a standing expert discussion mechanism under the UN framework to systematically collect and review state practices, gradually building interpretative consensus. Simultaneously, advocate for establishing technical international cooperation on attribution to enhance the capability to attribute cyber behavior, providing an objective factual basis for accurately identifying and determining intervention acts, making the application of the non-intervention principle more credible and operable.

In summary, China's path aims to seek dynamic balance between traditional sovereignty principles and the reality of cyber technology through sustained multilateral dialogue and practical adaptation. This is both a necessary move to safeguard its own cyber sovereignty and development interests, and a proactive responsibility as a major power to lead the construction of a fair, reasonable, and inclusive international order in cyberspace. The ultimate goal is to make the non-intervention principle a solid shield defending the legitimate rights and interests of all states in the digital age, rather than a tool for technologically powerful states to impose unilateral regulations or an excuse to move towards a closed-off internet.

## Concluding Remarks

The interpretation of the principle of non-intervention in internal affairs in cyberspace is, in essence, a process of adaptation between traditional sovereignty logic and the characteristics of cyber technology. Reflective equilibrium provides a third way beyond simple deduction or pure induction—constructing an interpretative framework that maintains both continuity and adaptability through continuous dialogue between principled adherence and practical adaptation. This interpretative process requires the joint participation and sustained dialogue of the international community. Technological development will not stop, and forms of cyber intervention will continue to evolve. The interpretation of the non-intervention principle must remain dynamically open, seeking balance between maintaining the basic stability of international relations and adapting to the development of cyber technology.

For China, actively participating in this interpretative process is both a commitment to international responsibility and a necessary act to safeguard its own cyber sovereignty and development interests. Through arguments based on reflective equilibrium, proposing interpretative schemes that conform to the basic principles of international law while reflecting the characteristics of cyberspace, China can play a leading role in the process of building a community with a shared future in cyberspace. Ultimately, the interpretation of the non-intervention principle in cyberspace should not become a tool for technologically powerful states to impose their own standards, nor an excuse for a closed-off cyberspace. It should become the normative cornerstone for promoting the construction of a fair, reasonable, and inclusive international order in cyberspace.

**Acknowledgements:** Thanks, my tutor Prof. Xu, for his patience and guidance.
**Conflict of interest statement:** None

## References

Cheng, L. (2025) 'International law mapping, dilemmas and breakthroughs of the metaphor of network "space"', *Political and Legal Forum,* 3: 75-90. (in Chinese)

Editorial Group of Jurisprudence: Jurisprudence (2017) Beijing: People's Publishing House Press.

ILC, UN Doc A/CN.4/SR.3225 'Summary Record of the 3225th Meeting as of 18 September 2014' YILC (2014) Vol. I 124 [37] ; See also ILC, UN Doc A/CN.4/SR.3184 'Summary Record of the 3184th Meeting' YILC (2013) Vol. I 100[53].

ILC, 'Provisional Summary Record of the 3338th Meeting from 2 May 2017' UN Doc A/CN.4/SR.3338 5.

Polanski, P. (2007) *Customary Law of the Internet: In the Search for a Supranational Cyberspace Law.* Hague: T. M. C. Asser Press The Hague Press.

Pomson, O. (2023). Methodology of identifying customary international law applicable to cyber activities. *Leiden Journal of International Law*, *36*(4), 1023-1047.

Rawls, J. (1971). *A Theory of Justice*. Massachusetts: Harvard University Press.

Schmitt, M (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* trans. by Huang Zhixiong et al.. Beijing: Social Sciences Academic Press.

Worster, WT. (2024). '*The Application of Logic and Reason in CIL Identification and Interpretation'*, in Fortuna M, Gorobets K, Merkouris P, Føllesdal A, Ulfstein G, Westerman P (eds.) Customary International Law and Its Interpretation by International Courts: Theories, Methods and Interactions. The Rules of Interpretation of Customary International Law, pp. 105-129, Cambridge: Cambridge University Press.

Zhang, H. (2022). 'Legal pathways for applying the principle of prohibiting the use of force in cyberspace', *China Legal Science*, 2: 283-304. (in Chinese)