Contents lists available at ScienceDirect

Computer Law & Security Review: The International Journal of Technology Law and Practice

journal homepage: www.elsevier.com/locate/clsr

Digital borders and beyond: Establishing normative grounds for cybersecurity and sovereignty in international law

Kasim Balarabe

Jindal Global Law School, O P Jindal Global University, Sonipat, Haryana, India

ARTICLE INFO

Keywords:
Cybersecurity
Digital sovereignty
International law
Cybercrimes
Cyberwarfare
Multistakeholder collaboration

ABSTRACT

In the rapidly evolving digital age, the confluence of cybersecurity threats and the assertion of digital sovereignty by states has created a complex, multi-dimensional challenge for international law. The existing legal regimes governing state behavior in cyberspace are fragmented, outdated, and ill-equipped to address the novel, intangible, and interconnected nature of the digital domain. This article examines the gaps and limitations in the current international legal frameworks and proposes a dynamic, adaptable approach to establishing a normative foundation for cybersecurity and digital sovereignty. The article highlights the urgent need for clear definitions and categories of cybercrimes and cyberwarfare under international law, as well as the development of appropriate legal responses and enforcement mechanisms. It also explores the tensions between state sovereignty and global Internet governance, proposing a balanced framework that upholds both the legitimate security interests of states and the fundamental principles of human rights, transparency, and multistakeholder collaboration. Central to the article's argument is the call for a flexible, evolutionary architecture of international cybersecurity law, capable of keeping pace with rapid technological advancements and the ever-changing threat landscape. This framework should incorporate mechanisms for continuous improvement, effective attribution and accountability, and the active engagement of international organizations and multistakeholder initiatives. The article further emphasizes the critical role of geopolitical challenges in shaping the development of international cybersecurity norms. It advocates for a nuanced, pragmatic approach that acknowledges the competing interests and values of different state actors while striving to find common ground and build trust through dialogue and cooperation. In an era of increasing digital interconnectedness and the erosion of traditional borders, this article presents a compelling case for the adaptation of international law to address the complex realities of the digital age. It offers valuable insights and recommendations for policymakers, legal experts, and scholars seeking to navigate the uncharted territories of cybersecurity and digital sovereignty in the 21st century.

1. Introduction

1.1. *The digital transformation of international security*

In the early years of the 21st century, the rapid development, proliferation, and fusion of digital technologies have irrevocably transformed the global environment, ushering in a new era of unparalleled connectivity, creativity and opportunity. However, while fostering these remarkable advancements, a complex array of challenges stretches the boundaries of existing legal frameworks and challenges foundational principles of international law. At the top of this litany of challenges are the problems of cybersecurity and digital sovereignty, both of which now merit unprecedented attention. With the deeper dependence of societies on digital infrastructure for increasingly broad functional areas – from communication and commerce to healthcare, energy, trade, governance and provision of public services – the imperative of cybersecurity has become urgent and profound [1]. A successful cyber-attack could result in financial losses and reputational damage, compromise of intellectual property, system outages and waste, and loss of physical life [2].

The cyberspace realm is both vast and complex, and the threat landscape is made up of various actors with different motivations and capabilities, ranging from individual hackers to loosely or closely organised criminal organisations, terrorist organisations and nation-states, which might use a wide range of means to exploit the vulnerabilities of computer systems and networks [3]. An additional difficulty relates to the fact that the anonymity and ubiquity of the Internet allow malicious actors to operate with a high degree of secrecy and impunity

E-mail address: kbalarabe@jgu.edu.in.

https://doi.org/10.1016/j.clsr.2025.106180

Available online 12 August 2025

[3–5].

1.2. The emergence of digital sovereignty

The increasing reliance on digital technologies has not only heightened cybersecurity concerns but has also brought the issue of digital sovereignty to the forefront. As states grapple with the challenges of securing their digital infrastructure and protecting their citizens' data, they are also asserting their right to control and regulate the digital space within their borders. Digital sovereignty is the ability of the state to have control over its digital infrastructure, data and online activities within its territory [6–10]. This ambition for digital sovereignty has gained traction over the past decade as an acknowledgement of how the borderless and deregulated early Internet sparked the creation of an 'electric frontier' that few nation-states were prepared to monitor and regulate. Many have expressed concerns about the dominant role played by a few global technology companies, primarily based in the United States, which exert significant control over the digital ecosystem [11,12]. These concerns have been amplified by revelations of mass surveillance programmes, data breaches, and the spread of disinformation and fake news on social media platforms [7,13].

In response to these pressures, many countries are evolving policies and strategies that increase their digital sovereignty by developing more indigenous digital competence, localising data storage and processing, and restricting cross-border data flow [7–9,14]. China has embraced a 'cyber sovereignty' strategy that includes strict control of the domestic Internet, the development of Chinese technology companies, and its own digital standards and protocols [7,8,15]. The European Union has striven to promote EU citizens' digital sovereignty through the EU General Data Protection Regulation (GDPR) and other laws that aim to regulate the behaviour of the technology industry, including social media, with a special 'strategy for digital sovereignty' emphasising digital self-determination [8,13,16,17].

1.3. International legal frameworks: current limitations

The confluence of cybersecurity and digital sovereignty presents international law with a complex, multi-dimensional problem. In the arena of who does what to whom over cyber systems, international law has stumbled out of the starting gate. The existing legal regimes protecting orderly state behaviour in cyberspace are fragmented, outdated, incoherent, and reflexively unhospitable to the characteristics of the new domain [18]. The application of traditional legal concepts such as territorial sovereignty, non-intervention and the lawful use of force to cyberspace is neither obvious nor straightforward [19,20]. The novel, intangible and interconnected nature of cyberspace blurs the boundaries between the physical and the virtual worlds. For example, there exists no commonly agreed-upon definition of what constitutes a cyberattack or cyber-warfare under international law. Over the years, there have been various efforts, such as the Tallinn Manual on the International Law Applicable to Cyber Operations project, started in 2008 (although membership is now inactive), to promote understanding of the legal characteristics of cyber behaviour, and to identify principles and norms of behaviour for states. However, none of these efforts has been adopted by states as law [21].

Another key challenge has been the attribution of cyber-attacks to states and other actors – who, exactly, was responsible for what, and to what extent? Due to the deep technical sophistication of cyber adversaries and the use of proxies and intermediaries, attribution is difficult. This lack of attribution, combined with the absence of clear legal frameworks, has created a sense of impunity and emboldened some states to engage in malicious cyber activities without fear of consequences [22]. Another challenge is reconciling states' legitimate security interests with the openness, interoperability and global cooperation that have underpinned the development of the Internet – a point made, among others, by the European Commission's recent cybersecurity strategy [23].

While the assertion of digital sovereignty has been necessary to maintain national security and safeguard citizens' interests and rights, excessive restrictions on cross-border data flows and the fragmentation of cyberspace along national lines could prove ultimately counterproductive. They could undermine the benefits of digital globalisation and hinder international cooperation on standardisation, law enforcement, scientific research and trade [24]. So far, international law has been established in this area through a fragmented set of multilateral and bilateral treaties, voluntary norms and principles, and soft law instruments that remain largely fragmented and lack clarity and coherence.

At the global level, the United Nations has been at the forefront of efforts to promote international cooperation and develop norms for cyberspace through initiatives such as the Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security and the Open-Ended Working Group (OEWG) on Developments in the Field of Information and Telecommunications in the Context of International Security [25]. The United Nations' efforts have made some headway with voluntary, non-binding norms of responsible conduct by states in cyberspace – for example, respect for the principle of not targeting the critical infrastructure of other countries or respect for the human rights of their citizens [26]. However, the GGE and OEWG have faced difficulties in achieving consensus on matters such as the applicability of international law in cyberspace and whether a cyber-attack or cyberwar amounts to a cyber-armed attack [25,27–29].

Other organisations, such as the European Union, the Organisation for Security and Cooperation in Europe (OSCE) and the Association of Southeast Asian Nations (ASEAN), have attempted to cultivate cybersecurity cooperation and common approaches to cyber challenges at the regional level. The Budapest Convention on Cybercrime (BCC), approved by the Council of Europe in 2001, remains the most comprehensive international treaty on cybercrime – establishing a legal framework for cooperation and providing a standard for criminalising terrorist and paedophile activities [30]. The BCC helps to harmonise national laws and regimes. However, its status as the leading cybercrime instrument has been harnessed by its limited impact on some dimensions of the issue. The BCC has neither been universally adopted nor seen to keep pace with the rapid innovation in tactics behind cybercrime or new threats such as ransomware or cryptocurrency-enabled money laundering [31,32]. It has even drawn two-sided critiques from 'expansionist interpretation' and 'restrictionist interpretation'. For example, some countries have expressed reservations that its provisions on cross-border access to data could compromise national sovereignty and infringe on privacy rights [33,34].

At the bilateral and plurilateral levels, the United States, the European Union and others have negotiated a series of agreements on cybersecurity cooperation and information-sharing [35–39]. These cover many issues, from anti-terrorism measures – the 2006 Supreme Allied Commanders Europe-US Cyber Commanders agreement on US-European cooperation to counter WMD threats – to commercial cooperation to enhance firewalls and cross-border information transfer between authorities on attacks, including the US-Europe Digital Economy Partnership Agreement of 2019 [35–38]. However, the profusion of bilateral and plurilateral agreements risks creating a no-man's-land of cross-purposes and fractured legal cultures. There is no guarantee that these arrangements will be sufficient to address cyber challenges, now and in the future.

Recent developments have sought to address some of the limitations in the existing legal frameworks for cyberspace, but they have also sparked new debates and controversies. These developments include the ongoing negotiation of a new UN Cybercrime Treaty, the adoption of the Second Additional Protocol to the Budapest Convention on Cybercrime (BCC), and the enactment of the Clarifying Lawful Overseas Use of Data (CLOUD) Act in the United States. While these initiatives aim to enhance international cooperation and provide more effective tools to combat cybercrime, they have also raised concerns about potential abuse, lack of adequate safeguards for human rights and civil liberties, and the concentration of power in the hands of certain states or the executive branch. The debates surrounding these developments highlight the complex challenges of balancing the need for effective law enforcement and national security with the protection of individual rights and the openness and interoperability of the global Internet.

In the face of these challenges, a more coherent and comprehensive international legal framework for cybersecurity and digital sovereignty will be needed. Such a framework must balance the legitimate targeted security and sovereignty interests of nation-states with the openness, interoperability and global cooperation that have characterised the development of the Internet so far [40]. It should aim to develop and articulate definitions of responsible state behaviour in cyberspace, building on international legal concepts such as non-intervention, self-defence and human rights and applying them to the peculiarities of the digital domain [41]. It should support the development of clear attribution, accountability and dispute-settlement mechanisms to deter malicious cyber activities and provide a basis for collective action by those who violate international norms [42]. It should support international cooperation and capacity-building to enhance the resilience of the global digital commons, restart efforts for a just, sustainable digital development agenda for the developing world, and help to narrow the ever-widening digital divide between industrialised and developing countries [43]. That should be done by exchanging information and best practices, harmonising common standards and protocols, and providing financial and technical support for those who do not have the ability to secure their digital networks and infrastructure by themselves [44].

1.4. Research objectives and structure

Of course, all this will happen if, and only if, we adopt a nuanced multistakeholder, open and inclusive framework that involves not only nation-states but also the private sector, civil society and the technical community [45]. It must, however, be mentioned that the existing geopolitical order makes it challenging to create a global, multistakeholder framework for cybersecurity governance. The present world order is increasingly fractured, becoming more a collection of competing blocs rather than a unitary international order. Reference is made here to the Shanghai Cooperation Organisation (SCO) push for cyber sovereignty, different from the position of the Western states, the strong influence of BRICS (Brazil, Russia, India, and South Africa). These geopolitical tensions and competing visions for cybersecurity governance add further complexity to the task of developing an international legal framework that can effectively address the challenges outlined above. Such a framework should be willing to evolve and expand to adapt to the rapidly changing technological landscape, and the geopolitical and economic realities of the digital age. The stakes are high. The future of international peace, security and prosperity in the digital age remains uncertain, as the world has yet to find a stable and sustainable framework for cybersecurity and digital sovereignty. We cannot afford to take the risk of having a fragmented and contested cyberspace.

This article will identify key challenges and opportunities in this regard. The article examines the existing international legal landscape regulating state behaviour in cyberspace and assesses the applicability and limits of those regimes to the problems of cybersecurity and digital sovereignty. It then addresses the challenges in defining and attributing cyber-attacks and cyber war under international law, suggests a framework for classifying cyber incidents and attaching differentiated responses to them, and articulates a vision for cybersecurity and digital sovereignty that critically assesses the logic of national sovereignty and global connectivity in the digital domain and its tensions and trade-offs. It proposes principles and norms by which states can better reconcile these competing imperatives. It also scrutinises the role of international organisations, regional bodies, and multistakeholder efforts in advancing cooperation and capacity building concerning cybersecurity and digital sovereignty issues. Finally, the article concludes with recommendations for the development of an international legal landscape for cybersecurity and digital sovereignty.

2. Existing international legal frameworks for cyberspace

Indeed, the rapid expansion of the realm of cyberspace has ushered in unparalleled opportunities but has also raised questions about the applicability of international law to the conduct of states in cyberspace [46]. It has brought unprecedented possibilities for cybersecurity and cyber-armed conflicts. The fluidity of the geopolitical landscape and the conflicting visions of how to govern cybersecurity highlight the necessity of critically scrutinising the internationally recognised legal frameworks governing state behaviour in cyberspace. This part delineates the existing international rules applicable to state behaviour in cyberspace, sheds light on the shortcomings and gaps of these legal regimes and discusses the implications of these lacunae for international peace and security.

2.1. International rules relevant to state behaviour in cyberspace

The starting point of any analysis of international law relevant to cyberspace is the UN Charter. It sets out general principles concerning the use of force and general rules of the conduct of states vis-à-vis each other. Article 2(4) prohibits the threat or use of force against any State. Article 51 provides for the inherent right of individual or collective self-defence in the event of an armed attack. As a matter of practice, however, it is not self-evident that these principles apply to cyberspace, as the law is unclear on the exact threshold for the use of force and armed attack [47,48]. One influential study that attempted to clarify the application of international law to cyber operations is the Tallinn Manual [49]. The Manual suggests that cyber operations that cause physical damage or injury comparable to a conventional armed attack would likely be considered a use of force under the UN Charter [49]. The Tallinn Manual does, however, acknowledge that there is no general agreement on the level of harm required to amount to a use of force, and States might conceivably arrive at varying assessments [49].

Another legal framework is the law of state responsibility, which holds states accountable for internationally wrongful acts, including those committed through cyber means [50]. The International Law Commission's Articles on State Responsibility provide a set of secondary rules for attributing conduct to states and determining the consequences of internationally wrongful acts. However, applying these rules to cyberspace is complicated by the difficulties in attributing cyber operations to specific states, as well as the challenges in assessing the damage or injury caused by cyber incidents [51].

The inadequacy of traditional international legal frameworks in addressing cyber operations has prompted what Qian characterizes as a necessary paradigmatic redefinition of international law's conceptual architecture [52]. Qian's analysis reveals how the digital transformation necessitates not merely the adaptation of existing principles but the fundamental reconceptualization of sovereignty, territoriality, and jurisdiction. This paradigmatic shift extends beyond doctrinal adjustment to encompass cybersecurity trajectories – the path-dependent evolution of legal frameworks shaped by technological affordances and geopolitical configurations.

International Humanitarian Law (IHL), or the law of armed conflict, constitutes another body of rules that could potentially apply to state behaviour in cyberspace in armed conflict situations [53]. The rules of distinction, proportionality and precaution aimed at averting harm to civilians and protecting civilians and civilian objects from attack could become applicable and useful during cyber operations. Again, how IHL applies to cyberspace is still evolving, and there are ongoing debates, for instance, about the interpretation of fundamental concepts such as 'attack', 'military objective' and 'civilian object' in cyberspace [21].

Alongside these general international legal regimes, several treaties and agreements address specific forms of cybersecurity and even state behaviour in cyberspace. As previously noted, the BCC's goal was to harmonise national cybercrime laws and to facilitate international cooperation in the investigation of cybercrimes. As mentioned, the BCC has suffered from a lack of practical impact and scope, as well as high-profile concerns of interference with national sovereignty and human rights.

More recently, the multistakeholder Paris Call for Trust and Security in Cyberspace, launched in 2018, seeks to unite a coalition of states, international organisations and non-state actors around a set of voluntary norms and principles for the responsible use of cyberspace by states. The Paris Call recognises the applicability of international law to cyberspace and encourages states to uphold human rights and fundamental freedoms online. Yet, because the Paris Call is non-binding and remains without the support of many of the world's major states, including the US, Russia and China, questions remain about its impact on state behaviour.

Since 2018, the UN has been negotiating a new Cybercrime Treaty, which, according to China and Russia (with the support of other countries), would be a more open and all-encompassing system for combating cybercrime [54]. Its proponents argue that this new treaty could plug the holes in the current patchwork regime and promote greater international cooperation, especially amongst developing countries [55]. Opponents worry that the draft text relies on overbroad language that permits repressive governments and human rights abusers to use the treaty to justify disinformation campaigns and censor dissent [56].

In 2022, the Council of Europe adopted the Second Additional Protocol to the BCC, which aims to enhance international cooperation and provide more effective tools to combat cybercrime, such as direct cooperation between law enforcement authorities and service providers in other countries [57]. While the Protocol includes safeguards to protect human rights and due process, such as requiring judicial oversight and data protection standards, some civil society groups have raised concerns about the potential for abuse and the lack of adequate transparency and accountability measures [58].

At the domestic level, the United States enacted the CLOUD Act in 2018, which allows US federal law enforcement to obtain data stored abroad by US technology companies under certain safeguards and subject to bilateral agreements between the US and the governments of foreign states [59]. Proponents say that the CLOUD Act creates a more streamlined, transparent and legally consistent mechanism for cross-border access to data by US law enforcement, while reducing conflicts of law and protecting the privacy of users [60]. Critics, on the other hand, contend that the Act, by creating a licence for governments to engage in an executive-branch arms race for access to data held by technology companies abroad and by permitting executive action for the conclusion of agreements with foreign governments, significantly threatens human rights and civil liberties, especially in states with weak rule of law and data protection standards, and gives too much power to the executive without appropriate congressional oversight [61].

2.2. Gaps and limitations of the legal frameworks and implications to international security

In light of these multiple international legal instruments and initiatives, it is important to note that the extant normative regime for state behaviour in cyberspace still contains many gaps and limitations. An obvious example is the lack of a comprehensive and universally accepted definition of what constitutes a cyber-attack or an act of cyber war under international law [48]. Without such a definition, it is challenging to agree on an objective and uniform threshold for the applicability of international legal rules and for the range of permissible responses to malicious activities undertaken by adversarial states in cyberspace. The complexities of attribution and accountability in cyberspace are addressed in Section 3.1, which establishes a graduated framework for addressing these challenges.

It is also important to add that it is questionable whether the current set of international legal rules is sufficiently clear and comprehensive to cover all state activities in the cyber domain – which can range from sub-threshold, low-level cyber incidents (hacks, breaches and other disruptive activity) to so-called grey zone activities (covert and often deniable cyber espionage, sabotage and warfare that falls short of the 'threshold' of armed conflict). As a result, reliance on the use of force and armed conflict as the basis to trigger various sets of rules in the UN Charter and IHL frameworks does not capture the less kinetic and more gradual forms of cyber coercion and interference that a state may employ below armed-conflict thresholds.

These gaps and deficiencies have important implications for international peace and security because they can cause instability and uncertainty by giving states more leniency to take advantage of the grey areas, and they provide more incentives to conduct malicious cyber activities with a higher degree of impunity. As discussed above, a lack of attribution mechanisms, combined with a lack of credible cost or consequences for state cyber activities in the face of such malicious activities, can also undermine the principle of deterrence by denial. As a consequence, it opens the door for an incentivisation of impunity [62]. Apart from the massive operational risks caused by these deficiencies, the current fragmented and inconsistent international legal frameworks also undermine global coordination and cooperation to maintain international peace and security in cyberspace [63]. Different conceptions of what states' rights and duties under international law are can lead to conflicts and disagreements in states' responses to cyber incidents, and states can also find it difficult to develop a common baseline to establish a shared understanding of responsible state behaviour in cyberspace ('live and let live'). Moving forward, there is an increasing agreement on the fact that the current disjointed and uncoordinated approach to international cyber law in various international legal regimes is insufficient. Instead, there is an increasing call for a comprehensive and coherent framework of international cyber law that can clean up the application of existing international law to cyberspace and develop new norms and principles to fill the gaps in the existing law, overcome the unique characteristics of cyberspace that challenge the effectiveness of the existing principles and norms.

Weber's analysis of international law as a 'policy driver' for cybersecurity governance offers critical insight into the normative influence of legal frameworks on policy development [64]. Rather than treating law as merely constraining or enabling policy choices, he demonstrates how international legal principles – such as the doctrines of global public goods, shared spaces, and state responsibility – actively shape policy imagination, defining not only what states may do but also what they perceive as feasible or legitimate. This constitutive function of international law in cybersecurity governance underscores Weber's argument that legal reform must precede and guide policy innovation, rather than merely react to it.

There are a few ways forward. We could, for instance, negotiate a new international cyber security treaty [65,66]. Even though such a treaty – due to the very different interests and perspectives of states – would face political and practical challenges, it could, however, specify the existing international law's application to cyberspace by establishing definitions of key terms such as cyber-attacks and cyber war, and rules on the lawful exercise of the right to self-defence in cyberspace [65]. A comprehensive cybersecurity treaty could also specify the conditions for the invocation of *jus ad bellum* and *jus in bello* in cyberspace, rules for attribution and the exercise of countermeasures, as well as requirements for dispute settlement and conflict resolution.

Another approach could be to enhance the existing international legal frameworks through a combination of interpretation, adaptation, and norm development [66,67]. Such an approach could clarify the application of the UN Charter and IHL to cyberspace through treaty interpretation, promote the universalisation and implementation of existing treaties, such as the BCC, and generate new non-binding norms and confidence-building measures developed through multistakeholder dialogue, like the Paris Call.

Weber's revisitation of digital sovereignty concepts reveals how earlier formulations have evolved through practical implementation and contestation [68]. His analysis traces a shift from viewing digital sovereignty as a defensive strategy focused on resisting external interference, toward an affirmative vision centered on capacity building, digital self-determination, and multistakeholder governance. While Weber does not formally divide sovereignty into discrete stages, his framework implies a progression—from defensive control, through regulatory authority, to a participatory and normative shaping of digital futures. This evolving perspective offers a crucial temporal lens for understanding how digital sovereignty is being redefined in response to contemporary global challenges.

Addressing the gaps and deficiencies in the existing international legal frameworks will require efforts in the four domains above. It will also require goodwill among states to engage in honest and meaningful dialogue on how to rationalise the existing law, as well as to prioritise a strong commitment to international peace and security over narrow, selfish national interests.

Having examined the limitations of existing frameworks and their inability to adequately address the complexities of cyberspace governance, we must now turn to the emerging doctrinal innovations that attempt to bridge these gaps. The evolution of attribution mechanisms and sovereignty concepts represents a critical frontier in international cyber law, where traditional principles undergo fundamental reconceptualization to address the unique challenges posed by digital technologies and transboundary cyber operations.

3. Attribution and sovereignty: evolving doctrines in cyberspace

The application of traditional sovereignty principles and attribution frameworks to cyberspace has catalysed profound doctrinal evolution in international law. As states grapple with the technical complexities of cyber operations and the emergence of new actors and modalities of harm, international legal scholarship has witnessed a renaissance in theoretical approaches to both attribution and sovereignty. This section examines these evolving doctrines, exploring how classical frameworks adapt to digital realities and how alternative epistemologies challenge Western-centric conceptualizations of cyber governance.

3.1. A unified framework for cyber attribution

The attribution of malicious cyber operations to state actors represents one of the most vexing challenges in contemporary international law, necessitating a comprehensive framework that synthesizes doctrinal evolution, comparative methodologies, and practical implementation mechanisms. This unified framework must accommodate the technical complexities of cyberspace while maintaining fidelity to established principles of state responsibility.

3.1.1. Doctrinal foundations and evolutionary trajectories

The International Law Commission's Articles on State Responsibility (ASR), provide the architectural foundation for attribution, yet their application to cyberspace demands fundamental reconceptualization [69]. Article 8́s requirement of state 'instructions,' 'direction,' or 'control' encounters unprecedented challenges when cyber operations involve loosely affiliated networks operating through subtle influence rather than hierarchical command structures [70,71]. The phenomenon of 'cyber militias' exemplifies this complexity: groups like APT28 advance state interests without documentable command relationships, operating through subtle control mechanisms that evade traditional evidentiary standards [72,73].

The jurisprudential evolution from Nicaragua's 'effective control' to Tadić's 'overall control' test illuminates attribution tensions in cyberspace [74,75]. Nicaragua's stringent standard, requiring control over specific operations, proves particularly unsuitable for cyber operations characterized by general support rather than operational command, as demonstrated by the 2007 Estonian attacks [75,76]. While Tadić's relaxed standard offers greater flexibility, it still struggles with the fluid affiliations and technical obfuscation characteristic of cyber operations [77].

3.1.2. A graduated attribution framework

The complexity of cyber operations necessitates a graduated attribution framework that transcends binary determinations. This framework establishes three distinct tiers of attribution, each with corresponding evidentiary standards and legal consequences:

i. Tier One – Direct State Operations: Attribution at the highest level applies to operations conducted by state organs or entities exercising governmental authority. Technical indicators include the use of state-exclusive infrastructure, deployment of capabilities requiring significant state resources, and operational patterns consistent with state intelligence tradecraft [78]. Legal consequences include full state responsibility under Article 4 of the ASR.

ii. Tier Two – Controlled Operations: This intermediate tier encompasses operations subject to effective or overall control, where states exercise sufficient direction over non-state actors to warrant attribution. Evidence requirements include demonstrable command relationships, provision of specific targeting information, and operational coordination. The framework acknowledges varying degrees of control, from Nicaragua's effective control to Tadić's overall control, with proportionate legal consequences [78].

iii. Tier Three – Facilitated Operations: The lowest attribution tier addresses situations where states knowingly facilitate malicious cyber operations through regulatory choices, deliberate inaction, or provision of safe havens. This tier operationalizes the Corfu Channel principle in cyberspace, establishing obligations to prevent territorial misuse while acknowledging capacity limitations [79–81]. States actively facilitating operations through regulatory design face enhanced responsibility approaching strict liability, while capacity-limited states bear responsibility only for deliberate indifference [82–85].

3.1.3. Methodological integration across jurisdictions

The unified framework must accommodate divergent national and regional approaches to attribution while establishing minimum common standards. The United States' forensic-intelligence hybrid model, employing 'attribution mosaics' that integrate technical indicators with strategic assessments, offers methodological insights for evidence aggregation [86,87]. European collective attribution through frameworks like the EU Cyber Diplomacy Toolbox demonstrates the value of coordinated declarations over unilateral claims, enhancing legitimacy through multilateral validation [88,89].

Non-Western approaches, particularly those of China and Russia, challenge technical-deterministic attribution by emphasizing sovereignty and political dimensions [90,91]. Rather than dismissing these as obstructionist, the unified framework acknowledges attribution as simultaneously technical and political, requiring mechanisms that respect epistemic diversity while maintaining accountability standards.

3.1.4. Implementation mechanisms

Operationalizing this unified framework requires specific implementation mechanisms:

International Notification Protocols: States must establish clear procedures for notifying potentially responsible states of attribution determinations, providing opportunities for explanation or remediation before public attribution. These protocols should specify timeframes, evidentiary disclosure requirements, and escalation procedures.

Technical Evidence Standards: Development of internationally recognized standards for technical attribution evidence, including chain of custody requirements, forensic methodologies, and confidence thresholds. These standards should accommodate varying national capabilities while establishing minimum reliability criteria.

Capacity Building Integration: Recognition that attribution capabilities vary significantly across states necessitates integrated capacity-building programs. These should focus not merely on technical capabilities but on developing institutional frameworks for attribution assessment and international cooperation.

Accountability Gradations: Legal consequences must be calibrated to attribution tiers and certainty levels. High-confidence Tier One attributions warrant full state responsibility measures, while lower-tier attributions might trigger enhanced due diligence obligations or cooperative remediation requirements.

This unified framework transcends the current fragmented approach to cyber attribution by providing clear doctrinal foundations, practical methodologies, and implementation mechanisms while respecting the technical complexities and political sensitivities inherent in cyberspace operations.

3.2. Multistakeholder governance in cyberspace: principles, tensions, and evolution

The multistakeholder model of Internet governance represents both a foundational principle and a contested terrain in contemporary cyber law. This consolidated analysis examines the theoretical underpinnings, practical manifestations, and inherent tensions within multistakeholder approaches to cyber governance, providing a comprehensive framework for understanding its role in balancing sovereignty with global coordination.

3.2.1. Theoretical foundations and normative justifications

Multistakeholder governance emerged from the Internet's technical origins, where collaborative decision-making among diverse actors proved essential for developing interoperable protocols and standards [92]. This model rejects both pure state-centric governance and unfettered market control, instead positing that cyberspace's global, interconnected nature demands inclusive participation from governments, private sector entities, civil society organizations, technical communities, and academia [93].

The normative justification for multistakeholderism rests on three pillars. First, legitimacy through inclusion: decisions affecting global digital infrastructure gain greater acceptance when stakeholders participate in their formulation. Second, expertise distribution: technical knowledge, policy experience, and operational capabilities are distributed across different stakeholder groups, necessitating collaborative approaches. Third, accountability enhancement: multiple stakeholder participation creates checks and balances, preventing capture by any single interest group [40].

3.2.2. Institutional manifestations and evolutionary trajectories

The Internet Governance Forum exemplifies multistakeholder principles in practice, providing a non-binding dialogue platform where diverse actors engage on equal footing [94]. Similarly, ICANN's governance structure, despite criticisms, demonstrates how technical coordination functions can incorporate multistakeholder input while maintaining operational efficiency. The Paris Call for Trust and Security in Cyberspace represents an evolution toward issue-specific multistakeholder initiatives, uniting states, companies, and civil society around shared cybersecurity principles.

However, institutional evolution reveals persistent challenges. Power asymmetries persist despite formal equality, with well-resourced actors exercising disproportionate influence. The TWAIL critique illuminates how multistakeholderism can perpetuate inequalities by privileging actors with existing technological capacity while marginalizing Global South participants lacking resources for meaningful engagement [95]. This creates what critical scholars term 'participatory subordination' – formal inclusion on terms that reinforce existing hierarchies.

3.2.3. Reconciling multistakeholderism with sovereignty imperatives

The tension between multistakeholder governance and digital sovereignty represents a fundamental challenge in cyber law. States asserting sovereign prerogatives view multistakeholderism as diluting legitimate governmental authority, particularly when non-state actors influence decisions affecting national security or cultural values [96, 97]. The SCO's cyber sovereignty model explicitly rejects multistakeholder approaches, advocating state-centric multilateral frameworks. Yet this binary opposition oversimplifies complex governance realities. Effective cyber governance requires acknowledging that different issues demand different governance configurations. Critical infrastructure protection may necessitate state leadership, while technical standards development benefits from multistakeholder collaboration. The framework must therefore embrace 'variable geometry' governance, calibrating stakeholder involvement to specific issue areas while maintaining baseline participation principles.

3.2.4. Operational principles for enhanced multistakeholder governance

Moving beyond theoretical debates requires operational principles that enhance multistakeholder effectiveness while addressing legitimate concerns:

i. Differentiated Participation: Rather than uniform stakeholder roles, governance mechanisms should recognize differentiated capacities and responsibilities. States retain primary responsibility for security and human rights protection, while technical communities lead on standards development, with cross-cutting issues requiring collaborative approaches.
ii. Capacity-Building Integration: Meaningful multistakeholder participation requires addressing capacity asymmetries through integrated support mechanisms. This includes funding for Global South participation, technical training programs, and institutional strengthening to enable substantive rather than merely formal engagement.
iii. Accountability Frameworks: Multistakeholder processes must incorporate clear accountability mechanisms, including transparency requirements, decision-making criteria, and review procedures. This addresses concerns about diffuse responsibility while maintaining governance flexibility.
iv. Cultural and Regional Adaptation: Recognizing that multistakeholderism itself embeds certain cultural assumptions, governance frameworks must accommodate regional variations and alternative participation modalities while maintaining core inclusive principles.

The evolution of multistakeholder governance in cyberspace thus requires moving beyond ideological commitments to pragmatic frameworks that balance inclusive participation with effective decision-making, acknowledge power asymmetries while working to address them, and respect sovereignty concerns while maintaining the global coordination essential for cyberspace stability.

3.3. Pluralist approaches to cyber sovereignty

The hegemonic discourse of cyber sovereignty, predominantly shaped by Western liberal traditions privileging individual rights and technological neutrality, obscures alternative conceptualizations emerging from non-Western epistemologies that offer fundamentally divergent approaches to digital governance. These frameworks challenge universalist assumptions, revealing radically different ontological foundations for understanding sovereignty, technology, and social order.

3.3.1. Chinese legal epistemology: confucian harmony and socialist cybernetics

Chinese cyber sovereignty emerges from a synthesis of Confucian philosophy, Marxist-Leninist theory, and socialist market economics. The foundational principle of hexie (harmony) conceptualizes cyberspace not as a domain of competing rights but requiring orchestration for collective flourishing. This rejects liberal assumptions of state-citizen adversariality, positing complementary relationships where state guidance enables human development [98–100].

Confucian li (ritual propriety) translates into governance prioritizing behavioral guidance over juridical enforcement. The Cybersecurity Law's comprehensive 'network operator' responsibilities reflect distributed moral authority, contrasting with Western neutral intermediary conceptualizations. Party-state constitutionalism operationalizes these principles through 'digital Leninism' – using technology to perfect rather than limit governance. The Social Credit System exemplifies this logic, reconceptualizing surveillance as care, data collection as planning, and censorship as guidance [101].

Article 1′s wangluo zhuquan extends beyond territorial control to encompass informational and developmental sovereignty – asserting authority over data flows while claiming rights to divergent modernization paths. This multidimensional concept reflects historical experiences with informational imperialism, positioning cyber sovereignty as anti-colonial resistance [102].

3.3.2. Global south cyber jurisprudence: postcolonial resistance and digital self-determination

Brazil's Marco Civil da Internet, emerging from NSA surveillance revelations, demonstrates how Global South frameworks arise from digital subordination experiences. Its conceptualization as 'Internet Constitution' embeds digital rights within broader social justice architectures [103,104]. Brazilian net neutrality emphasizes funç̃ao social (social function) transforming technical principles into mechanisms preventing digital reproduction of social inequalities. India's data localization exemplifies postcolonial consciousness shaping sovereignty claims. Requirements must be understood through historical informational extraction experiences, with contemporary localization representing resistance to 'data colonialism' – Global South data extraction for Global North value creation. This reconceptualizes data as national resources requiring sovereign control for developmental autonomy [105]. The African Union's Digital Transformation Strategy articulates pan-African approaches emerging from shared technological dependency experiences. Emphasizing 'digital sovereignty and ownership' reflects collective ownership traditions, reconceptualizing sovereignty as regional self-determination capacity. Unlike European privacy focus or Chinese security emphasis, African frameworks prioritize preventing digital resource extraction and ensuring African data generates African development [106–108].

3.3.3. TWAIL critique: decolonizing cyber governance

Having examined Chinese and Global South epistemologies that emphasize distinct philosophical, historical, and socio-economic contexts underpinning cyber sovereignty, it is crucial to adopt a critical lens to interrogate how these alternative approaches contest the purported universality of prevailing cyber governance frameworks. To achieve this, Third World Approaches to International Law (TWAIL) offers a particularly insightful perspective, revealing the underlying power dynamics and structural inequalities embedded in dominant international cyber norms. TWAIL scholarship provides critical tools for analyzing how supposedly universal cyber governance frameworks embed particular cultural assumptions and perpetuate global inequalities. The TWAIL critique reveals how the dominant governance discourse naturalizes Western technological trajectories, regulatory approaches, and normative commitments while marginalizing alternative visions emerging from the Global South [95]. This critical examination extends beyond identifying bias to excavating the epistemological foundations of cyber law and their entanglement with histories of colonialism, ongoing patterns of subordination, and possibilities for emancipatory alternatives.

The analysis of the BCC illustrates how technical legal instruments may embed civilizational hierarchies and developmental assumptions: the Convention criminalizes certain technological behaviours while protecting others, reflecting Western priorities around intellectual property and system integrity that can conflict with Global South needs for technological adaptation and knowledge diffusion. Its procedural requirements presuppose institutional capacity and legal infrastructures often lacking in many Global South states. This dynamic may amount to kicking away the digital ladder (using international law to foreclose the same developmental strategies that enabled Western technological ascendancy), though this interpretation remains under-theorized in TWAIL scholarship.

The critique of Western-centric cyber norms extends to fundamental concepts like 'multistakeholder governance' that appear neutral but embed particular assumptions about state-society relationships. TWAIL analysis reveals how multistakeholderism privileges actors with existing technological capacity and resources (predominantly Western corporations, NGOs, and technical communities) while marginalizing Global South states and communities that lack such capacities. The apparent horizontality of multistakeholder governance masks vertical power relations, creating what TWAIL scholars would term 'participatory subordination' – inclusion in governance processes on terms that perpetuate rather than challenge inequalities.

Alternative sovereignty conceptualizations emerging from TWAIL scholarship reconceive cyber sovereignty not as territorial control but as effective capacity for self-determination in digitally mediated contexts. This approach distinguishes between formal sovereignty – the juridical right to regulate cyberspace – and effective sovereignty – the actual capacity to shape digital futures. Many Global South states possess formal cyber sovereignty but lack effective sovereignty due to technological dependency, infrastructural subordination, and regulatory capture by foreign platforms. TWAIL frameworks thus advocate for international legal reforms that enhance effective sovereignty through technology transfer, capacity building, and restrictions on digital monopolization.

South-South cooperation constitutes a framework of technical and governance collaboration among Global South states, based on principles of sovereignty, equity, and non-conditionality [109]. Although originally led by China, the Digital Silk Road has the potential to evolve into a BRICS-style initiative pooling complementary capabilities across Global South states – creating an alternative digital pathway distinct from Western-dominated systems [110,111]. Additionally, Global South states are increasingly active participants in cyber governance diplomacy, including at forums such as the United Nations Open-Ended Working Group (UN OEWG) and the Internet Governance Forum (IGF). These states have advocated for multilateral and developmental approaches to international cyber norms, emphasizing digital inclusion, capacity building, and the equitable distribution of technological benefits. While national regulatory frameworks remain central to their digital strategies, there is growing recognition that technological sovereignty can be meaningfully enhanced through collective capacity building and regional collaboration. This is reflected in the emergence of regional digital infrastructures (including payment systems, messaging platforms, and cloud services) that illustrate early but significant forms of South–South cyber cooperation.

3.3.4. Toward polycentric normative development

Recognizing epistemic diversity necessitates abandoning universalist pretensions for polycentric development, acknowledging multiple legitimate approaches. This requires not relativism but genuine dialogue reaching universal principles through synthesis rather than hegemonic extension. Current frameworks' entanglement with particular histories (European privacy reflecting Protestant individualism, American innovation privileging specific constitutional traditions) opens space for alternatives premised on different human flourishing concepts. Institutional innovations enabling genuine dialogue might include ‘cyber governance laboratories’ testing different approaches without presuming convergence. Regional experiments should be understood as contributions to global conversations rather than deviations from universal norms.

Having established the evolving doctrinal foundations for attribution and sovereignty in cyberspace, we must now examine how these theoretical advances translate into practical frameworks for defining and prosecuting malicious cyber activities. The complexity of attribution mechanisms and the contested nature of sovereignty concepts directly impact our capacity to establish juridically coherent categories for cybercrimes and cyberwarfare. The graduated attribution framework developed in Section 3.1, combined with the pluralist sovereignty approaches examined in Section 3.3, necessitates a correspondingly nuanced approach to criminalization that acknowledges both technical uncertainties and epistemological diversity.

While the evolution of attribution and sovereignty doctrines represents a significant theoretical advancement in international cyber law, the practical challenge of defining and prosecuting cybercrimes remains paramount. The doctrinal innovations examined above provide crucial context for understanding how states conceptualize responsibility and authority in cyberspace, yet they must be translated into operational frameworks capable of addressing the immediate threats posed by malicious cyber activities. We now turn to the concrete challenges of establishing clear definitions and enforcement mechanisms for cybercrimes and cyberwarfare under international law.

4. Defining and punishing cybercrimes and cyberwarfare

With the rapid advancement of technology and the growing dependence of societies upon digital infrastructure, new forms of criminality and warfare have emerged in cyberspace. Cybercrimes and cyberwarfare test the boundaries of international law and provide challenges for legal definitions, criminal investigations, and punishment as they often involve non-state actors [5]. In this section, I first discuss the challenges that arise in defining cybercrimes and cyberwar under international law and then propose some clear and understandable definitions and classifications of offences, as well as ways to improve jurisdiction over these crimes and a framework for measures and enforcement mechanisms.

4.1. Challenges in defining cybercrimes and cyberwarfare under international law

Building upon the attribution framework established in Section 3.1, the primary challenge in defining cybercrimes and cyberwarfare lies in developing internationally recognized categorizations that correspond to the graduated attribution tiers and their respective evidentiary standards. Likewise, while the Tallinn Manual 2.0 aims at clarifying the interpretation and application of international law to a grey area between peace and war (a term often used for cyber activities), it uses a narrow definition of cyber warfare but admits that there is not universally accepted one. It suggests that cyber warfare can be understood as the use of cyber operations that constitute a use of force under international law or that occur in the context of an armed conflict. However, this definition is subject to interpretation and debate, as the threshold for what constitutes a use of force in cyberspace remains unclear.

To address these challenges, it is essential to develop clear and internationally recognised definitions and categorisations of cybercrimes and cyber warfare. To do this, a ’tiered approach’ could work. For instance:

1. Cybercrime: Criminal activities using digital technologies, generally with non-political motives, often for personal gain or revenge, e.g., hacking, malware, online fraud, and intellectual property theft.
2. Cyber-attacks: Malicious cyber activities potentially aiming to cause harm or disrupt the operation of computer systems and networks with political or strategic motives but below the threshold of the use of force under international law.
3. Cyberwarfare: The use of cyber operations as a means of warfare, either in addition to, or as a substitute of, activities of physical force, that constitutes a use of force under international law or that is carried out in the context of an armed conflict.

Inherent to such a tiered approach are the following propositions: First, it distinguishes cybercrime from cyber-warfare; second, it distinguishes varying degrees or severity of impact such malicious cyber activities may have; third, it aims to avoid using broad and generic language applicable indiscriminately to other categories of malicious cyber activities; and, fourth, it permits for a more nuanced application of international law, bearing the severity or impact of various cyber phenomena in mind. In addition, there needs to be a single set of definitions and diverse categorisations, with common punishment and enforcement mechanisms for dissuading and punishing cybercrimes and cyberwar.

The implementation of this tiered framework must incorporate the graduated attribution mechanisms, ensuring that legal responses align with attribution certainty levels. High-confidence Tier One attributions would trigger full criminal or state responsibility measures, while lower-tier attributions might invoke enhanced monitoring, capacity-building requirements, or diplomatic engagement. This calibrated approach prevents both over-reaction based on uncertain attribution and under-reaction that enables impunity.

4.2. Recommendations for establishing a universal framework for punitive measures and enforcement mechanisms

One model would be to enhance existing international legal treaties, such as the BCC, by broadening their scope of application and including provisions on more general cybercrimes, cyber-attacks and even cyber warfare [32]. Doing so would entail amending the BCC to criminalise attacks carried out by protecting state and private actors, including computer intrusion and contamination – as long as they are carried out in a way that causes significant damage exceeding a certain threshold. It could also be modified to include more robust and detailed mechanisms for international cooperation and mutual legal assistance [32].

Another alternative is to develop a new international treaty dealing exclusively with cybercrimes and cyber warfare. The treaty would include definitions for types of cyber-crimes and cyber warfare, mechanisms for prevention and deterrence, rules to punish offenders and means of addressing related conflicts among nations [112]. It would also contain provisions on capacity building and technical support to enable countries to build cybersecurity capacities and plan for cyber resilience.

With cybercrime and possibly also cyberwar, however, negotiating a new international convention remains unlikely because there are simply too many national interests and different views on what should and should not be done. States might not want to accept intrusive limitations regarding using cyber capabilities for national security or strategic purposes; for others, it may be important to protect human rights and individual freedoms on the Internet.

The implementation of these legal instruments must incorporate the multistakeholder governance framework articulated in Section 3.2, ensuring inclusive participation across governmental, private sector, civil society, and technical community stakeholders.

Secondly, applicable to both international and non-international offences, states should adopt and comply with national laws and regulations targeting internet-related criminal activities, particularly cybercrimes and cyber warfare. Such legislation must conform to international standards and best practices, including the ones prescribed in the BCC, which can serve as a model for adopting cybercrime laws that are legally enforceable, effectively implemented, and politically sustainable. State parties must also adopt clear policies and procedures on responding to cyber incidents, such as mechanisms on attribution and counter-attribution of an attack and cooperation with and assistance to another state in the prevention, investigation, and prosecution of a cyber offence that has a cross-border element.

Thirdly, states must adopt measures to reduce the digital divide. This involves increasing cyber security capacities and resilience. At the national and international levels, there could be a need to invest in building capacities and developing awareness of cyber warfare. At the national level, this is an issue for law enforcement, judicial authorities, and other national actors that may be involved in investigating and prosecuting cyber offences. In this regard, staying current on cybercrime statistics comes in handy. National responses could be developed by first identifying both the policing challenges posed by cyber offences and the risks that may be suffered because of cyber-enabled warfare. This would likely require the forming of specialised cybercrime units within the police and other national law enforcement agencies and the creation of cybercrime courts or tribunals, provided that cyber trials will be conducted in accordance with due process standards. The police, in turn, may need to develop cybercrime-specific training curricula and other tools for participating in the investigative process. Further, raising awareness about threats in cyberspace – that is, educating the public on how people can lower the risk of becoming a victim of cybercrimes and cyberwarfare – would help to create a sense of responsibility and encourage those being victimised to come forward [113].

Finally, international cooperation and information sharing are essential for successfully addressing cybercrimes and cyber warfare. Given the cross-border element of cyber violations and the fact that no state can address the issue on its own, concluding bilateral and multilateral agreements and signing instruments adopted by multilateral fora and organisations, for example, the UN GGE, are indispensable for states to share intelligence and best practices, to coordinate investigations and responses, and to increase their global resilience to cyber offences [113].

5. Balancing digital sovereignty and international cooperation

As the global spread of digital technologies continues relentlessly and cyberspace becomes an ever more important political, economic, and social space for states, digital sovereignty has emerged and is now a leitmotif in debates about the future form of international legal order. Digital sovereignty describes a state's capacity to control its digital infrastructure, data and online activities within its territory [114]. In the past decade, the idea of digital sovereignty has obtained increasing prominence in international discourse, as many states have started to stridently assert sovereignty over the digital domain as a matter of national security in the context of continuing globalisation and mounting dominance of a few powerful digital technology conglomerates [115]. At the same time, the reality and the essential importance of the global nature of the Internet and its transnational elements mean that digital sovereignty often operates at odds with international cooperation or a truly global approach to Internet rule [116]. The borderless nature of cyber-space and the reality that many activities online take place across multiple states raise difficulties for states going it alone on matters of cybersecurity and data protection, while the very rules constraining cross-border internet connectivity may undermine the benefits of the open global digital ecosystem, innovation and free flow of information that have been defining features of the digital age so far [117].

This part addresses the systemic tensions between state sovereignty and global internet governance, considers the key legal principles that could guide such a balanced approach, and proposes a framework that upholds the pertinence of individual state rights while preserving the space for international cooperation and shared security of cyberspace.

5.1. The dialectic of sovereignty and cooperation in cyberspace

Digital sovereignty and international cooperation exist in dialectical tension, each concept simultaneously necessitating and constraining the other. The exercise of digital sovereignty can conflict with other important legal principles – such as the protection of human rights and fundamental freedoms online – that are vital to the full enjoyment of individuals in a digital age. Article 19 of the Universal Declaration of Human Rights, for instance, affirms the right 'to seek, receive and impart information and ideas through any media and regardless of frontiers', while the International Covenant on Civil and Political Rights recognises the rights to freedom of expression and privacy. Imposing assertions of state sovereignty in cyberspace can undermine the rule of law by suppressing dissent, stifling innovation, and fragmenting the global Internet [97].

The evolution of surveillance jurisprudence in the digital age illuminates this tension. The development of comprehensive bulk surveillance jurisprudence represents one of the most significant evolutions in international human rights law's engagement with digital sovereignty. The transformation from targeted to mass surveillance paradigms necessitates a fundamental reconceptualization of privacy rights vis-à-vis state security. The European Court of Human Rights' (ECtHR) jurisprudential evolution from *Liberty* [118] through *Big Brother Watch* [119] reveals judicial struggles to maintain meaningful rights protection while acknowledging technological realities. The concept of 'Bulk interception' challenges traditional surveillance categories, as fiber optic infrastructure requires intercepting entire data streams for subsequent filtering – a technological necessity creating legal complexities. The emerging 'stage-based' approach recognizes that interception's significance lies less in initial collection than in subsequent selection, (search, examination, use) each of which raises distinct human rights compliance issues and sovereignty–rights boundary points.

International jurisprudence's metadata protection framework represents a critical evolution in digital privacy understanding. The CJEU's Digital Rights Ireland judgment established that metadata enables profiling no less sensitive than actual content, requiring states to justify metadata collection under stringent standards previously reserved for content interception, thereby constraining sovereignty-based arguments for unrestricted harvesting [120,121].

Cross-border data access frameworks epitomize sovereignty-rights intersection complexity. While data's physical location becomes increasingly irrelevant to accessibility, legal frameworks remain territorial, creating simultaneous multi-state authority assertions based on varying connecting factors: storage location, subject nationality, collection place, or investigating authority location [122]. Mutual Legal Assistance Treaties (MLATs) attempt to reconcile sovereignty with investigative necessities but struggle with the volume, velocity, and volatility of digital data [123]. Executive agreements under frameworks like the CLOUD Act evolve toward agility but raise concerns about circumventing domestic protections and creating lowest-common-denominator privacy standards. Data sovereignty responses through localization requirements encounter human rights boundaries. Such measures must satisfy proportionality, demonstrating that less restrictive alternatives cannot achieve legitimate objectives while accounting for collective digital rights dimensions – how localization affects participation in global digital communities.

Encryption's reconceptualization from technical tool to human rights imperative fundamentally shifts digital discourse. The UN Special Rapporteur's declaration that encryption provides necessary privacy and security for digital expression elevates technical standards to rights requirements, challenging sovereignty-based restrictions by establishing positive state obligations ensuring availability [124]. The encryption debate illuminates deeper tensions between sovereignty-as-control and rights-as-empowerment. Encryption creates privacy zones challenging traditional territorial authority assumptions. Proportionality analysis for encryption restrictions requires systemic assessment: weakening encryption for law enforcement necessarily creates universal vulnerabilities, mandating holistic security evaluation that effectively forecloses categorical bans, establishing encryption as foundational to digital rights architecture [125].

5.2. Normative principles for balancing competing imperatives

It is imperative to identify and develop the core legal principles that can guide state behaviour in cyberspace. One such principle is the duty of a state and of people under its jurisdiction to cooperate in dealing with transnational challenges and to promote the common interests of the international community [25]. This duty emerges – almost self-evidently – from many international legal instruments, including the UN Charter, the UN Convention against Transnational Organized Crime, and the Paris Agreement on climate change. In the context of cyberspace, the responsibility to cooperate also provides a basis for states to collaborate in developing and implementing norms, standards and best practices for responsible state behaviour while respecting each other's legitimate interests and sovereign rights. This could take the form of developing international standards on data protection, cybercrime prevention, capacity building and sharing information and best practices on cybersecurity and digital resilience [92].

Human Rights Council Resolution 32/13′s declaration that rights existing offline must be protected online belies profound complexities in transposing material rights to immaterial digital existence [93]. The resolution's treatment of internet access as a rights-enabler creates positive state obligations fundamentally altering traditional negative liberty frameworks, requiring navigation between regulatory prerogatives and obligations ensuring rights realization through technical architecture decisions.

General Comment 34′s articulation of digital expression boundaries establishes that restrictions must account for digital communication's special characteristics (instantaneous dissemination, collapsed publisher-reader distinctions, global reach) necessitating reconceptualized proportionality analysis. The prohibition on generic bans presumes against broad technological restrictions, recognizing architectural interventions achieving censorship through technical rather than legal means [126]. The Special Rapporteur's jurisprudence distinguishes between surveillance capabilities and authorities, establishing that mass surveillance technology existence creates presumptive privacy interference. By framing encryption as enabling multiple rights enjoyment, technical standards become elevated to human rights obligations, fundamentally challenging sovereignty-based restriction arguments [124,127].

Regional human rights systems demonstrate divergent approaches to digital boundndaries. The ECtHR's Big Brother Watch judgment articulates end-to-end safeguards penetrating surveillance systems' operational aspects (authorization, selection, examination, retention, disclosure) establishing human rights as infrastructure design constraints. Centrum för rättvisa refined this approach through objective reasonable suspicion requirements, establishing substantive boundaries transcending technological capabilities [119,128]. The Inter-American Court's Escher analysis extends beyond individual violations to address surveillance's chilling effect on democratic participation, requiring broader harm conceptualization. The 'strictly necessary' standard and 'least invasive means' principle create technological intervention hierarchies privileging targeted over mass surveillance [129]. The African Commission's Declaration emphasizes universal, equitable, affordable access as rights prerequisite, establishing infrastructure development as human rights obligation. The near-absolute internet shutdown prohibition reflects regional experiences with digital repression, constraining sovereignty claims through bright-line rules [130].

Digital proportionality analysis confronts unique challenges: binary intervention nature, technical measure scalability, and difficulty constraining effects within intended boundaries. Legitimate aim assessment must address cybersecurity threats' speculative nature, requiring concrete threat demonstrations, preventing blanket security invocations [131]. Suitability evaluation demands understanding technical capabilities and 'function creep' phenomena, necessitating dynamic rather than static assessment. Necessity analysis confronts rapidly evolving technological alternatives (privacy-enhancing technologies, selective encryption, algorithmic transparency), transforming analysis into forward-looking feasibility assessment. Proportionality *stricto sensu* must weigh incommensurable values accounting for digital amplification effects, developing 'digital proportionality' doctrines acknowledging cyberspace's unique characteristics: record persistence, correction difficulty, and network effects amplifying individual into collective harms.

5.3. Geopolitical challenges to cooperative frameworks

Digital sovereignty is at odds with international cooperation because of competing visions of Internet governance. On the one hand, advocates of the multilateral approach – seeing the vision of states playing a greater role in regulating and controlling the Internet within their territories as a superior model of Internet governance – present this approach as more advantageous than the bottom-up, multistakeholder approach [132]. This attribute places emphasis on the role of nation-states in guarding national security, safeguarding sovereign cultural values, and preserving political stability while asserting that the cyber-space must not be opened up to external influence from foreign actors or global corporations that attempt to interfere in domestic relations [133].

The SCO is rapidly becoming a key player in the world's cybersphere, pushing for an understanding of the Internet that emphasises 'cyber sovereignty', understood as state control over its domestic internet and its domestic data [134–136]. The interpretation of the term 'cyber sovereign' by Beijing and Moscow is fundamentally different from an open, multistakeholder understanding of internet governance favoured by Western states and organisations like the G7, NATO and the Quad.

The SCO's push for cyber sovereignty is also proving attractive among the developing world, particularly countries suspicious of Western dominance in the digital realm. The SCO adopted an 'Intergovernmental Agreement on Cooperation in the Field of Ensuring International Information Security' to bolster cooperation against cyber threats [137]. It features several drastic proposals, including cooperation to prevent the misuse of information technology for terrorist purposes, curbing the actions of terrorist, extremist and criminal elements and the protection of critical information infrastructure while still upholding the principle of non-interference in the domestic affairs of states.

At the same time, the BRICS have also become a major player in the world of cyberspace, trying to forge a parallel infrastructure and technical standards system for cutting its dependency on Western technologies and platforms [138]. In 2020, these five countries adopted the Moscow Declaration, which, among others, contains information on countering the use of information and communications technologies for criminal purposes as well as a call for prompt adoption of an international treaty on cybercrime under the auspices of the UN for the purposes of joint actions against this growing crime phenomenon globally [139]. This was deemed a pushback against the Budapest Convention on Cybercrime to which Western countries are major proponents [54].

The Asia-Pacific region's approach to digital integration, as analyzed by Mishra and Valencia, offers a distinctive model that prioritizes a development-oriented form of digital governance – strategically designed to advance economic development objectives while preserving regulatory autonomy [140]. This approach differs markedly from both the EU's rights-based framework and the US's market-oriented model, instead emphasizing state capacity building, strategic industrial policy, and selective integration. Mishra and Valencia's empirical analysis reveals how Asia-Pacific states employ what may be characterized as 'calibrated openness' – varying degrees of digital market access based on developmental priorities and domestic capacity constraints [140].

India, which sits in both the SCO and the Quad, lies at the heart of a fractured geopolitical landscape. On the one hand, India shares many of the Western countries' anxieties about the flow of data and the protection of human rights online. On the other, however, India has been reluctant to become an ally of either bloc [141]. The Personal Data Protection Act, which sought to control how personal information is collected and used by domestic and foreign actors alike, has been interpreted as a reflection of India's desire to hedge between these competing interests.

On the other hand, proponents arguing for a multistakeholder approach stress that internet governance should involve a wide range of actors, including governments, the private sector, civil society and the technical communities [142]. This view reflects the global and interconnected nature of cyberspace and the need to develop norms and policies through collaboration and consensus-building to solve cross-border issues while encouraging the Internet to remain open, interoperable and universal for innovation, expression and economic development [143]. The tension between these approaches has played out, including in successive rounds at the UN GGE and the Internet Governance Forum (IGF). Although these processes have resulted in some progress in developing norms and establishing explicit principles of responsible state behaviour in cyberspace, international efforts have also brought out divergences among member states and their stakeholders in terms of their interests and their perception of the underlying problems and solutions, as well as alternative pathways [144].

Chaisse's metaphor of the 'black pit' illuminates the regulatory vacuum created by the disjuncture between territorial sovereignty and deterritorialized data flows [145]. This conceptualization reveals how cross-border data transfers create what is considered as jurisdictional arbitrage opportunities, whereby data controllers exploit regulatory differentials to minimize compliance obligations while maximizing data extraction capabilities. The power dynamics inherent in these flows reflect deeper structural inequalities in the global digital economy, where data-rich nations exercise what was identified as data imperialism – the extension of economic and political power through control over data flows and processing capabilities [145].

Geopolitical rifts and competing multilateral frameworks constitute powerful forces of resistance to the emergence of a truly global, multistakeholder approach to Internet governance. The differential interests and values of the different blocs make it extremely hard to find common normative ground: go-it-alone suburbanisation of global cyberspace will continue to be exerted by different states in pursuit of their particular worldviews and interests over key issues – such as data localisation, encryption and the role of the state in governing the internet [146]. In addition, the growing assertiveness of the SCO and the BRICS to push their own agendas over an institutional approach for global internet governance may further spur greater fragmentation of the global cyber landscape, with countries aligning themselves with one bloc or the other based on their political and economic interests.

Addressing these issues will require an appreciation of the distribution of power, interests, and norms that are driving the cyber-geopolitical complexities throughout the world, as well as a pragmatic attitude to realise the limitations and the potential of multistakeholder governance. Reinforcing dialogue and cooperation between the blocs, and in particular addressing the legitimate security concerns and cultural differences of the blocs, will also play a major role in building cyber trust and cooperation. At the same time, existing international frameworks and institutions, such as the GGE OEWG, should be strengthened and utilised accordingly in confirming the emergence of new cyber norms and principles [147]. Navigating these geopolitical challenges requires a nuanced approach that balances the legitimate interests of states in asserting their digital sovereignty with the need for international cooperation to address global cybersecurity threats.

These geopolitical tensions and competing multilateral frameworks underscore the imperative of developing an integrative approach that transcends binary oppositions between sovereignty and cooperation. The framework proposed below acknowledges the legitimacy of diverse governance philosophies while establishing minimum standards necessary for meaningful collaboration. Drawing upon the theoretical insights developed in Section 3 regarding attribution complexity and sovereignty pluralism, this framework operationalizes a pragmatic synthesis that accommodates variation while ensuring accountability.

5.4. Toward an integrative framework

Based on the above principles discussed in the previous sections, a framework for balancing digital sovereignty and international cooperation could involve the following elements:

i. Recognition of the sovereign rights of states to regulate and control their digital infrastructure and online activities within the limits of international law and human rights obligations, with human rights serving as both legitimating and limiting principles.
ii. Development of international norms, standards, and best practices for responsible state behaviour in cyberspace through inclusive and transparent multistakeholder processes that embed human rights considerations at every stage [40].
iii. Establishment of international cooperation mechanisms, such as information sharing, capacity building, and mutual legal assistance, that incorporate human rights safeguards and proportionality assessments to address transnational challenges while protecting individual freedoms.
iv. Promotion of digital literacy, empowerment, and participation as both sovereignty-enhancing and rights-realizing objectives, enabling individuals and communities to benefit from the opportunities of the digital age while contributing to legitimate governance frameworks.
v. Creation of differentiated cooperation frameworks that acknowledge varying geopolitical positions while maintaining minimum human rights standards, allowing for flexible implementation that respects cultural contexts without compromising fundamental protections.
vi. Establishment of Regional Cyber Governance Laboratories as experimental spaces for testing differentiated approaches to digital sovereignty and cooperation. These laboratories would operate as juridical sandboxes where states within specific regions could pilot alternative governance frameworks that reflect their particular epistemological traditions, developmental priorities, and security concerns. Drawing from the polycentric normative development analysis presented earlier, these laboratories would not presume convergence toward a universal model but rather contribute to a global repository of governance innovations. Each laboratory would be required to maintain minimum human rights standards while enjoying flexibility in institutional design, decision-making processes, and implementation mechanisms.
vii. Development of comprehensive South-South cooperation mechanisms that transcend bilateral arrangements to create multilateral frameworks for technological capacity building, normative development, and collective bargaining vis-à-vis dominant digital platforms. Building upon the Digital Silk Road's infrastructure while avoiding hegemonic capture, these mechanisms would pool complementary capabilities across Global South states—combining, for instance, India's software expertise, Brazil's social digital innovation, and African states' mobile technology leapfrogging experiences. Such cooperation would include joint development of technical standards resistant to technological lock-in, shared regulatory frameworks for data governance that prioritize developmental objectives, and collective negotiation strategies for engaging with multinational technology corporations.
viii. Implementation of TWAIL-informed capacity-building approaches that fundamentally reconceptualize technical assistance from a transfer model to a co-creation paradigm. Rather than reproducing Western institutional templates, these approaches would support Global South states in developing autochthonous cyber governance frameworks that reflect their specific historical experiences, cultural values, and developmental trajectories. This

includes establishing South-based centres of excellence for cyber law that privilege non-Western epistemologies, creating scholarship programs that support critical legal research on digital colonialism and its alternatives, and developing pedagogical materials that decentre Western-centric assumptions about technology, law, and governance. Capacity building would explicitly address structural inequalities in global cyber governance participation, including funding mechanisms that ensure meaningful rather than tokenistic inclusion in international norm-setting processes.

This framework could be implemented through a combination of hard and soft law instruments. These include binding legal instruments, such as treaties and conventions, and non-binding instruments, like declarations, recommendations, and guidelines. The framework must account for what has been identified as the investment-sovereignty paradox in digital contexts – the tension between states' desire to attract digital foreign direct investment (FDI) and their imperative to maintain sovereignty over critical digital infrastructure [145]. Chaisse's analysis of digital FDI patterns reveals how investment flows embed power relationships that transcend traditional economic metrics, creating what may be termed structural digital dependency. This dependency manifests through platform dominance, algorithmic governance, and data extraction mechanisms that collectively constitute a new form of economic subordination. The proposed framework must therefore incorporate safeguards against digital dependency while enabling beneficial technology transfer and capacity building.

To address the structural digital dependency identified through Chaisse's analysis, the framework must incorporate specific safeguards and alternative pathways: First, FDI Safeguard Mechanisms that prevent the entrenchment of technological dependency through investment flows. These mechanisms would include mandatory technology transfer provisions for digital infrastructure investments, local capacity building requirements that ensure knowledge diffusion rather than mere service provision, and algorithmic transparency obligations that prevent opaque governance through technological means. States would retain the right to impose data localization requirements where necessary to prevent extractive data practices, provided such requirements are proportionate and do not constitute disguised protectionism.

Second, Alternative Digital Development Pathways that enable states to pursue technological modernization without replicating surveillance capitalism or authoritarian models. These pathways would emphasize commons-based digital infrastructure, including public investment in open-source technologies, support for platform cooperatives that distribute value creation more equitably, and development of interoperable standards that prevent vendor lock-in. International legal frameworks would recognize and protect these alternative models through adjusted intellectual property regimes, competition law adaptations that account for network effects, and public procurement preferences for sovereignty-enhancing technologies.

Third, Structural Dependency Mitigation Strategies that address the root causes of digital subordination rather than merely its symptoms. These strategies include establishing regional digital infrastructure funds that provide patient capital for sovereignty-enhancing projects, creating technology transfer obligations for dominant platforms operating in multiple jurisdictions, and developing 'digital sovereignty impact assessments' for major technology deployments. International financial institutions would be required to incorporate digital sovereignty considerations into their lending criteria, ensuring that development finance supports rather than undermines technological self-determination.

It could also strengthen existing Internet governance mechanisms, such as the IGF and the for-profit private entity known as the Internet Corporation for Assigned Names and Numbers (ICANN). These mechanisms are inadequate as they stand, and so the goal would also be to create new ones, such as a multilateral forum for data protection authorities, a cybersecurity ministerial forum for dialogue and cooperation where all states are sovereign, or even just a cybersecurity cooperation council for improved collaboration and cooperation. The existing frameworks could be fortified by inserting stronger guarantees for human rights and the multistakeholder model of governance.

Further, ensuring transparency and accountability in cyber policy-making – at the domestic and international levels – would have a significant impact and contribute to the circulation of best practices. Above all, though, such a framework would require significant political will and resources. It would need to address the different national contexts, priorities and capabilities of states and have flexibility and space for adaptation as technology and threats rapidly change [148]. The regional variations identified by Mishra and Valencia necessitate abandoning one-size-fits-all approaches to digital governance in favor of context-sensitive and developmentally oriented frameworks that preserve regulatory autonomy and reflect national priorities [140].

Balancing digital sovereignty and cooperation is complex and multidimensional. And what the IGF showed us is that it must also be principled and nuanced [94]. States can legitimately recognise and protect distinct national security and sovereignty interests, such as the development goals, political and social structures, and cultural values and identities that underpin national security. This stems from reasonable liberal cosmopolitan commitments to state sovereignty and self-determination. That said, these interests must be compatible with international law, including legal and normative requirements of human rights and the broader public good – in other words, what is positive and necessary for all to flourish.

In this complex landscape, there is no point trying to force a square peg through a round hole. What is needed instead is a pragmatic, aplomb-fuelled search for the common ground that exists among the many sub-blocs, ground that acknowledges (but does not bow simply to) the legitimate needs for security and independence, as well as political and cultural diversity, that preoccupy our allies and apparent adversaries. Sometimes, this will mean listening, even to those parts of the world that are wont to listen only to their own voices. And sometimes, it will mean talking and showing courage in devising solutions that might somehow straddle the chasms in this archipelago of incommunicability.

One possibility is to bolster the existing international architecture and associated institutions, such as the UN GGE and the OEWG, to provide a venue for inclusive and transparent dialogue on cyber norms and principles. These fora can be opportunities for states to come together to shape and implement fundamental norms while also inviting stakeholders other than states – especially civil society, academia and the private sector – to the conversation.

Parallel to this, there is a need to develop further regional and bilateral agreements that address particular cybersecurity problems and enable like-minded countries to cooperate on these issues. The US-EU Trade and Technology Council coordinates transatlantic cooperation on digital policy topics, including data governance, platform regulation and cybersecurity standards.

Ideally, this would lead to the development of a 'patchwork' of compatible and interoperable frameworks that could allow different stakeholders to address their particular interests and needs in a manner that will augment stability and security in cyberspace. The construction of this framework' will have to carefully strike a balance between national sovereignty and the realities of international cooperation and coordination.

Finally, an international legal framework must also address the de facto role of Big Tech as a foundational component of the international cybersecurity landscape, including their increasing dominance over global data flows and the maintenance or hosting of key pieces of critical infrastructure. Whether it's through Google's dominance of the internet and popular search engine rankings, Facebook's near-monopoly status for social media in the US and Europe, Amazon's hegemony over online retail in the West and China, or Microsoft's control over distribution of Windows operating systems and deployment of Office suites around the world, each company possesses foundational pieces of 'internet plumbing' [149] and collects massive amounts of state – and individually sensitive data. Their policies and decisions can have profound impacts across realms of cybersecurity, privacy and human rights, potentially without regard to national borders [150].

An effective international legal framework will, therefore, need to devise ways of regulating private actors, potentially including a mechanism for holding them accountable while simultaneously making use of their know-how and resources to help develop, promulgate, and enact cybersecurity norms and best practices. This could include mandating greater transparency and oversight of their activities, imposing liability authority for harms caused by products and services, or encouraging a reliance on public-private partnerships and multistakeholder initiatives [151].

6. Adapting international law for the digital age

It is an understatement to say that digital technologies have revolutionised virtually all aspects of contemporary society. Now that the global polity and economy increasingly depend on cyberspace for survival and prosperity, the need for a robust and nimble international legal order equipped to govern the conduct of states and promote human rights *vis-à-vis* digital technologies has arguably grown more urgent than ever. But here is the rub. The pre-existing international legal order that developed in the wake of the Second World War, by and large intended to mitigate the use of force among states and to uphold human rights, has not kept up with the sheer speed and complexities of the technological revolution [151]. For one, much of what we now call international law, including such core foundational principles and basic norms such as territoriality, inviolability, sovereignty, non-intervention and the prohibitions on the use of force, was developed in a world in which the principal threats to international peace and security still came in familiar physical and kinetic forms [152]. Today, the global threats to international peace and security still constitute that kind of anathema. Yet, in the digital age, these threats have acquired new kinetic and electronic forms in the nature of cyberattacks, disinformation campaigns and digital surveillance that have derived a life of their own, profoundly impacting virtually all areas of international, state and human life.

Furthermore, the transnational and decentralised nature of cyberspace has complicated the lines separating domestic and international, international law and municipal law, public and private law, as well as states and non-states. Authoritarian regimes such as Putin's Russia and Xi's China have used this new terrain to seek power, influence, and control beyond their borders. And, as the reach of the state no longer seems to go as far as it once did, large technology companies such as Google, Facebook and Amazon present themselves and are empowered as the de facto global governors of the digital age.

6.1. The need for a dynamic and adaptable legal framework

Taken together, these concerns suggest the need for an open and flexible legal framework that evolves with cyberspace while addressing and anticipating the genuine security concerns and risks that are posed by an increasingly digital global economy and civilian society. Such a framework must be principled and rule-based but also adaptable and context-based, particularly when new and unforeseen problems and uncertainties arise.

The first and most fundamental principle that should drive it is the necessity of better balancing the legitimate security and regulatory interests of states on the one hand and the human rights and freedoms of individuals in cyberspace on the other. That is to say, international law recognises that states have the right in the digital age to maintain and safeguard national security and public order but that those states also have an obligation, under international human rights law, to respect, protect and fulfil the inherent human rights of citizens, including the rights to privacy, freedom of expression, due process and other non-derogable rights [153]. The digital age has made this balance harder to achieve, as many states increasingly invoke the pretext of national security to justify pervasive surveillance and censorship in the name of security at the expense of individual rights and freedoms online [97]. The response to this again lies in international law, through the development of a clear and binding human rights regime in the digital age based on existing international human rights law but adapted to the digital space [154]. This could include, for example, the global development of a new digital treaty that articulates states' obligations to respect the rights and freedoms of individuals in cyberspace and sets out effective remedies and enforcement mechanisms for situations where state parties fail to live up to their obligations. It could also include other institutional approaches, such as human rights-based changes to international law and policy for cybersecurity, including the BCC and the UN GGE.

The third core principle requires operationalizing the multistakeholder governance framework comprehensively analyzed in Section 3.2, which establishes the theoretical foundations and practical mechanisms for inclusive cyber governance.

To operationalise these principles and ensure the effectiveness of the proposed dynamic and adaptable legal framework, it is crucial to establish appropriate mechanisms and engage international organisations and multistakeholder initiatives.

6.2. Recommendations for mechanisms and potential role of international organisations and multistakeholder initiatives

The institutionalization of multistakeholder governance requires implementing the operational principles established in Section 3.2.4, which delineate differentiated participation mechanisms, capacity-building integration, accountability frameworks, and cultural adaptation modalities.

A second set of principles relates to the requirement of continuous improvement and updating of international cybersecurity law and norms. Given the rapid pace of technological evolution and the fluid nature of cyber threats, it is essential that international cybersecurity law and norms remain fit for purpose and are flexible and adaptable to new challenges and opportunities [155]. This requires a process of continuous improvement and updating. This component of the framework could take inspiration from competing or parallel achievements in other areas of international law, in particular with regard to the established practice of UPR in the human rights regime and the implementation review mechanism in relation to the United Nations Convention against Corruption.

A third principle of good international law relates to the need for continuous innovation and development in the domain of cyber governance. This could include the creation of a global network of research centres and think tanks interested in international law and policy for cyberspace. This could be a mechanism for continuous evidence-based analysis and recommendations for policymakers and practitioners. This could also include training and education programmes for diplomats, lawyers and other professionals on issues related to the development and implementation of international cybersecurity laws and norms.

A fourth principle relates to the operationalization of the graduated attribution framework developed through doctrinal analysis. International law must move beyond binary attribution determinations to embrace the complexity spectrum identified in our analysis. This requires establishing:

First, an International Cyber Attribution Mechanism that implements the three-tiered framework, with differentiated evidentiary standards and proportionate consequences for each attribution level. This mechanism would not replace national attribution processes but rather provide a multilateral validation framework that enhances legitimacy while respecting epistemic diversity. The mechanism would incorporate technical experts, legal scholars, and regional representatives, ensuring that attribution determinations reflect both forensic analysis and contextual understanding.

Second, a Cyber Haven Accountability Protocol that operationalizes the graduated responsibility framework for states whose territories are used for malicious cyber operations. This protocol would establish clear obligations differentiated by state capacity: enhanced due diligence requirements for developed states with sophisticated cyber capabilities; cooperative assistance obligations for states with moderate capabilities; and capacity-building entitlements for states lacking basic cybersecurity infrastructure. The protocol would include presumptive timelines for response to notification of malicious activities, with failure to engage constituting evidence of breach.

Third, Regional Attribution Variation Mechanisms that acknowledge the divergent epistemological approaches to attribution while maintaining accountability standards. These mechanisms would permit regional bodies to develop attribution methodologies consistent with their legal traditions and technical capabilities, provided they meet minimum reliability criteria established through inclusive multilateral processes. This approach recognizes that attribution is simultaneously technical and political, requiring frameworks that respect sovereignty while preventing impunity.

In light of the geopolitical challenges and the rapid pace of technological change, it is clear that international law must adapt to remain relevant and effective in the digital age. The development of a dynamic and adaptive legal framework that can respond to the evolving threat landscape and the competing interests of different actors is crucial.

Crucially, such a framework will require shared and precise definitions of important terms – such as sovereignty, jurisdiction and the use of force in cyberspace. The Tallinn Manual 2.0 is a helpful starting point for this endeavour, though its non-binding status and Western character mean it is unlikely to gain global traction. This work needs to be built upon, and we must seek the general participation of developing countries and non-state actors in the development of the required international consensus going forward.

Another is mechanisms for attribution, accountability and dispute resolution. The national approach, largely based on national capabilities and political will, has failed to cope with the nature of today’s challenges. Although national attribution is still unavoidable, international confidence-building norms and measures such as the ones that were discussed in the UN GGE and the OEWG reports can help reduce the risks of misperception and escalation. Nevertheless, they must be complemented by the establishment of stronger, more autonomous institutions and procedures for investigating and adjudicating cyber incidents, through either an international cyber attribution body along the lines suggested by Microsoft [156] or through strengthening of the existing mechanisms such as the International Criminal Court or International Court of Justice [157]. Ultimately, the objective should be the creation of an inclusive, unified and coherent international law that brings about legal certainty, predictability and accountability in the digital realm while ensuring openness and innovation. This would require long-term and concerted efforts by states, international organisations and non-state actors to overcome mistrust, do more together, and be more creative.

In addition to overarching principles, it is also crucial to address specific technological challenges driving the conversation around cybersecurity and digital sovereignty. The security of submarine communication cables, which carry over 95 % of international internet traffic, is vulnerable to various threats, including physical attacks, cyber-attacks, and espionage [158]. Disruption or destruction of these cables could have catastrophic consequences, necessitating international legal frameworks to protect these critical assets. A related issue is the fast-paced and largely uncontrolled development and deployment of AI systems in warfare. AI systems may dramatically transform the nature and conduct of armed conflict [159]. Large-scale deployment of AI weapons raises a host of ethical, legal and strategic questions, including the possible erosion or radical transformation of established norms of international humanitarian law, with the consequent risk of inadvertent escalation and other risks to human control. There is an urgent need for international legal regulation of AI systems in warfare to ensure meaningful human control over the development, testing and operation of AI systems and related technologies in armed conflict. Moreover, quantum computing and post-quantum cryptography could both have negative consequences for the security of digital communication and transactions. Quantum computers might be able to crack many of the cryptographic algorithms that presently secure our digital infrastructure [160]. International cooperation and standardisation of the development and deployment of post-quantum cryptographic solutions could help to secure digital information and assets against any disruption by quantum technologies, while there also needs to be legal frameworks in place to guarantee the security and privacy of digital assets in the quantum age.

The multistakeholder governance principles and institutional mechanisms detailed in Section 3.2 provide the foundational architecture for international organisations’ participation in developing and implementing cybersecurity norms.

7. Conclusion

Over the past three decades, digital technologies have transformed the world through unprecedented opportunities for economic growth, social development, and political transformation. However, the global rise of cyber-dependent activities also creates new sources of instability and insecurity with novel forms of interstate conflict and unprecedented threats to international peace and security arising in cyber and digital domains. As the world becomes more digital, the pressing need for an effective international legal framework that regulates state conduct and individual rights within cyberspace has never been greater. The interplay of geopolitical challenges and geopolitical determinations of and competition between visions of cybersecurity governance, as outlined in the above discussion, illustrate this fundamental point: the task of achieving an improved, more equitable and inclusive international-law-based cybersecurity framework is more challenging at this historical juncture than at any time before. The Balkanisation of the global order into not only patron-client blocs but new and competing modularised configurations is, at the very least, deeply unhelpful in forging a truly global, collectively endorsed, multi-stakeholder cybersecurity approach. So, the key will be to take a pragmatic, flexible and pluralistic approach that allows us to support the legitimate interests, concerns and needs of key stakeholders, including states and international organisations, while also embodying fundamental democratic values, like the rule of law and human rights. This will require states and international organisations to work together in order to build trust, compromise on priorities, and develop innovative ways to deal with the problems of the digital age. It will require a concerted, collective and cumulative effort.

In this article, I’ve attempted to articulate some of these challenges and suggest a set of recommendations for future work on this project of constructing international cybersecurity and digital sovereignty law. First, I’ve examined the applicability of existing international legal frameworks that may have relevance for cyber activities, in particular the UN Charter, as well as international humanitarian law and international human rights law, and I’ve identified the gaps and limits in the application of these legal regimes to the digital domain. Second, I’ve highlighted the urgent need for legal definitions and categories of crime for the purposes of building high-level concepts for the regulation of cybercrimes under international law, as well as for the differentiation between cyber warfare and cybercrimes under international law, with a view to drawing appropriate ethical and legal boundaries between different levels of severity and impact of malicious cyber activities. Put together; these approaches provide a basis for specifying the framework of legal responses and punitive measures that may appropriately apply to the given activity or incident.

Third, I’ve stressed the need for some balance between competing claims of state digital sovereignty and human rights, especially the individual rights and freedoms that anchor and safeguard democratic society in cyberspace. I've proposed a framework for finding the equitable balance between dual and competing imperatives of digital sovereignty and human-centric global connectivity in cyberspace by prioritising the principles of international cooperation, multistakeholder collaboration, the rule of law and human rights.

Fourth, I've stressed the priority of an open-ended, evolving, and dynamic architecture of international cybersecurity and digital sovereignty law able to keep up with the pace of digital technologies and the evolving threats and problems in the cyberspace order. With this in mind, I've proposed that state and non-state parties be dedicated and empowered to monitor and evaluate the efficacy of existing international cybersecurity laws and norms and periodically refine the rules to address emerging challenges and challenges of emerging digital technologies. Fifth, I've highlighted the critical need for dedicated international organisations, multistakeholder processes and capacity-building initiatives to develop and implement international cybersecurity and digital sovereignty law. Here, I call for more investment in the research, education and training programmes required to equip more policymakers, lawyers and other stakeholders with the expertise needed to navigate the complex landscape of this project.

The takeaway from these findings and recommendations includes the sense of immediacy and complexity of the challenges and problems facing the international community in the digital age: the exponentially increasing pace, scale and frequency of nation-state and criminal cyberattacks; the mounting competition between states for control and jurisdiction over cyberspace in the digital age; and the exponential pace of technological change. Failure to address these challenges may imperil international peace, security, and human security. Malicious cyber operations against critical state infrastructures – including power grids, transport infrastructure, financial services and other vulnerable sectors – might be able to trigger cascading failures, resulting in the disruption of vital services to large numbers of populations for days, months or longer. Whoever controls the Internet controls the world. Operationalising cyberspace for espionage, sabotage and information warfare, apart from inflaming mutual mistrust, could inflame mutual suspicion between states and lead to reduced cooperation and heightened risks of conflict and retaliation [161].

Moreover, the erosion of digital sovereignty and the concentration of power in the hands of a few dominant technology companies could threaten the autonomy and self-determination of states and limit their ability to protect the rights and interests of their citizens [114]. The mass surveillance and data exploitation practices of these companies, often in collaboration with state actors, could infringe on the privacy and freedom of expression of individuals and undermine the foundations of democratic societies [162].

In light of these urgent and complex challenges, it is essential that the international community takes decisive and coordinated action to develop a comprehensive and effective international legal framework for cybersecurity and digital sovereignty. This framework must be founded on a deep appreciation and shared commitment to the core tenets of international law, including the primacy of respect for state sovereignty, territorial integrity, non-interference, and peaceful resolution of disputes as enshrined in the UN Charter. The framework must be based on a tripartite recognition of:

i. the protection of fundamental human rights and freedoms – including but not limited to the right to privacy, the right to freedom of expression, and the right to due process of law as articulated in international conventions and human rights law – that must be ensured in cyberspace;
ii. the clear and enforceable norms and standards that define responsible state behaviour in cyberspace in conformity with these fundamental rights and freedoms; and
iii. the accountability, by means of effective attribution and the credibility of attribution, of behaviour in cyberspace that exceeds the bounds of responsible behaviour.

Finally, universal solutions can never be found to these challenges without a multistakeholder approach that is precise, comprehensive, and inclusive, based on the principles of shared intervention, cooperation, and transparency that have long been the hallmarks of good governance – and on substantive innovative research and analysis carried out by an interdisciplinary group of scientists from various fields, including international law, computer science, political science, and economics.

Some critical areas for future research and action could include:

1. Developing consensual and internationally agreed upon definitions and categories of, and laws and legal frameworks for, cybercrimes and cyberwarfare, accompanied by appropriate and proportionate criminal penalties.
2. Exploring the opportunities for new international legal instruments, such as a treaty on cyberspace with binding obligations, which could offer a complete and well-rounded regime for states to adhere to in developing a governance framework for the digital domain that respects human rights.
3. Strengthening the capacity and effectiveness of international organisations and multistakeholder initiatives for developing and implementing norms and standards for responsible state behaviour in cyberspace and promoting international cooperation and dialogue on the same.
4. Developing education, training and awareness-raising programmes for policymakers, lawyers, judges, and other relevant actors to master the technical aspects of cyber issues and participate in meaningful efforts to develop international cyber law and norms.
5. Increasing the transparency, accountability, and oversight of private actors such as technology companies and their practices when conducting business in the digital domain, and thus ensure that their conduct in cyberspace adheres to international human rights law and other relevant legal norms and standards.
6. Establishing institutional mechanisms for epistemic dialogue between different conceptualizations of cyber sovereignty, including formal recognition of alternative theoretical frameworks in international legal discourse and creation of translation mechanisms that facilitate mutual understanding across divergent governance philosophies.
7. Developing South-South solidarity frameworks that enable collective resistance to digital hegemony while constructing alternative pathways for technological development that prioritize human flourishing over surveillance capitalism or authoritarian control.

The imperative for sustainable cyber governance frameworks extends beyond immediate security and economic concerns to encompass what Chaisse and Lam describe as a broadened vision of sustainability in international economic law – one that integrates environmental stewardship, social inclusivity, and institutional adaptability [163]. Their editorial outlines a shift toward governance models that are responsive to long-term challenges such as climate change, digital inequality, and systemic reform. This sustainability lens highlights how short-term assertions of digital sovereignty may jeopardize the viability of global digital ecosystems, calling for a temporal expansion of governance horizons and more inclusive legal frameworks.

With urgent, coordinated action, the international community can help pave the way toward more stable, secure and equitable digital spaces that serve humanity. This will require sustained political will, resources, engagement from relevant stakeholders, and commitments to international law and human rights. It will also necessitate a recognition that cybersecurity and digital sovereignty challenges are neither static nor one-dimensional but are constantly evolving and will require interplay with broader global governance challenges, economic development and social progress. As such, efforts toward an effective, international legal framework for cyberspace should be treated as an iterative process rather than as a static, one-off solution. The imperative for a global, international legal framework for cybersecurity and digital sovereignty is simple: the global stakes are high, and failure to take the necessary measures to keep pace with accelerating threats and challenges to global cybersecurity, digital economies, and digital public goods could be severe.

The imperative for structural transformation extends beyond immediate governance challenges to encompass the fundamental architecture of global digital relations. As the analysis has demonstrated, current patterns of digital dependency replicate and intensify historical patterns of subordination, requiring international law to evolve beyond neutral facilitation toward active redistribution of technological capabilities. The recommendations advanced (from regional governance laboratories to structural dependency mitigation) represent not merely technical adjustments but fundamental reimagining of how international law can serve emancipatory rather than subordinating functions in the digital age. Only through such transformation can the promise of digital technologies for human flourishing be realized on a truly global scale.

Declaration of competing interest

The author declares that there is no conflict of interest regarding the publication of this article. The research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest. The author has not received any funding or support from organizations that could influence the findings or conclusions presented in this work. The views and opinions expressed in this article are those of the author and do not necessarily reflect the official policy or position of any affiliated institution or organization.

Data availability

No data was used for the research described in the article.

References

[1] International Telecommunication Union. Overview of cybersecurity. ITU; 2008 [Available from: https://www.itu.int/rec/T-REC-X.1205-200804-I.

[2] Greenberg A. The untold story of NotPetya, the most devastating cyberattack in history: WIRED. 2018 [Available from: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[3] Finlay L, Payne C. The attribution problem and cyber armed attacks. AJIL Unbound 2019;113:202–6.

[4] Blue Goat Cyber. The challenge of attribution in cyber attacks: Blue Goat Cyber; [Available from: https://bluegoatcyber.com/blog/the-challenge-of-attribution-in-cyber-attacks/.

[5] Tsagourias N, Farrell M. Cyber attribution: technical and legal approaches and challenges. Eur J Int Law 2020;31(3):941–67.

[6] Karlstad W. Digital Sovereignty: adapting to a challenging digital landscape. Tietoevry; 2023 [Available from: https://www.tietoevry.com/siteassets/files/tech-services/tech-services-digital-sovereignty-whitepaper-v1-2023.pdf.

[7] Musoni M, Karkare P, Teevan C, Domingo E. Global approaches to digital sovereignty: competing definitions and contrasting policy. 2023. Ecdpm: the Centre for Africa-Europe relations.

[8] Internet Society. Navigating digital sovereignty and its impact on the internet. 2022.

[9] PEN America. Splintered speech: digital sovereignty and the future of the internet. 2021.

[10] Pohle J, Thiel T. Digital Sovereignty. Internet Policy Rev 2020;9(4).

[11] BizNews. Big tech's dominance in ai sparks regulatory scrutiny as startups lean on giants for lifelines. BizNews; 2023 [Available from: https://www.biznews.com/tech/2023/12/19/big-techs-dominance-ai-sparks-regulatory-scrutiny-startups-lean-giants-lifelines.

[12] Kak A, West SM, Whittaker M. Make no mistake—AI is owned by Big Tech: MIT Technology Review. 2023 [Available from: https://www.technologyreview.com/2023/12/05/1084393/make-no-mistake-ai-is-owned-by-big-tech/.

[13] Larsen BC. The geopolitics of AI and the rise of digital sovereignty. Brookings; 2022 [Available from: https://www.brookings.edu/articles/the-geopolitics-of-ai-and-the-rise-of-digital-sovereignty/.

[14] Peltola M. Negotiating Africa's digital partnerships: interview series. In: Soule F, Negotiating Africa's digital partnerships policy research project: global economic governance programme: Blavatnik School of Government, University of Oxford.

[15] Jiang M. Authoritarian informationalism: China's approach to internet sovereignty. SAIS Rev Int Aff 2010;30(3):71–89.

[16] Hobbs C, editor. Europe's digital sovereignty: from rulemaker to superpower in the age of US-China rivalry. European Council on Foreign Relations; 2020 [Available from: www.ecfr.eu/publication/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry/.

[17] Komaitis K. Sovereignty strikes the internet: when two don't become one. 2020 [Available from: https://www.komaitis.org/personal-blog/category/sovereignty.

[18] Moynihan H. The application of international law to cyberspace: sovereignty and non-intervention: Just Security. 2019 [Available from: https://www.justsecurity.org/67723/the-application-of-international-law-to-cyberspace-sovereignty-and-non-intervention/.

[19] Tsagourias N. The legal Status of Cyberspace: sovereignty redux? In: Tsagourias N, Buchan R, editors. Research handbook on international law and cyberspace. Edward Elger Publishing; 2021. p. 9–31.

[20] Schmitt M. The Sixth United Nations GGE and international law in cyberspace: Just Security. 2021 [Available from: https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/.

[21] MaCAK K. From cyber norms to cyber rules: re-engaging states as law-makers. Leiden J Int Law 2017;30(4):877–99.

[22] Finnemore M, Hollis DB. Beyond naming and shaming: accusations and international law in cybersecurity. European J Int Law 2020;31(3):969–1003.

[23] The EU's cybersecurity strategy for the digital decade. 2020.

[24] Drake WJ, Cerf VG, Kleinwächter W. Internet fragmentation: an overview. World Economic Forum; 2016 [Available from: https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf.

[25] Ponta A. Responsible State behavior in cyberspace: two new reports from parallel UN processes. ASIL Insights 2021;25(14).

[26] United Nations. Report of the Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security. 2015. UN Doc A/70/174. United Nations.

[27] Efrony D. The UN cyber groups, GGE and OEWG – A consensus is optimal, But Time is of the Essence: Just Security. 2021 [Available from: https://www.justsecurity.org/77480/the-un-cyber-groups-gge-and-oewg-a-consensus-is-optimal-but-time-is-of-the-essence/.

[28] Cyber Peace Institute. The OEWG final report: new milestone in global cyber diplomacy, collective efforts still needed to close the accountability gap and achieve cyberpeace. Cyber Peace Institute; 2021 [Available from: https://cyberpeaceinstitute.org/news/the-oewg-final-report-new-milestone-in-global-cyber-diplomacy-collective-efforts-still-needed-to-close-the-accountability-gap-and-achieve-cyberpeace.

[29] Lewis JA. Creating accountability for global cyber norms. 2022.

[30] Council of Europe. The Budapest Convention on Cybercrime: benefits and impact in practice. Council of Europe; 2020.

[31] EuroJust. Budapest convention on cybercrime and cross-border access to electronic evidence. EuroJust; 2024 [Available from: https://www.eurojust.europa.eu/sites/default/files/assets/the-budapest-convention-on-cybercrime-and-cross-border-access-to-electronic-evidence-23-01-2024.pdf#:~:text=URL%3A%20https%3A%2F%2Fwww.eurojust.europa.eu%2Fsites%2Fdefault%2Ffiles%2Fassets%2Fthe.

[32] Clough J. A world of difference: the budapest convention on cybercrime and the challenges of harmonisation. Monash Univ Law Rev 2014;40(3):697.

[33] Rodriguez K. The proposed Cybercrime Treaty's approach to cross-border spying. EFF; 2023 [Available from: https://www.eff.org/deeplinks/2023/08/proposed-cybercrime-treatys-international-cooperation-provisions-could-let-tyrants.

[34] Rodriguez K. First draft of UN cybercrime convention drops troubling provisions, but dangerous and open-ended cross border surveillance powers are still on the table. EFF; 2023 [Available from: https://www.eff.org/deeplinks/2023/07/first-draft-un-cybercrime-treaty-drops-troubling-provisions-dangerous-and-open.

[35] US Department of States. Joint statement on the united states-european union 9th cyber dialogue in Brussels. US Department of States; 2023 [Available from: https://www.state.gov/joint-statement-on-the-united-states-european-union-9th-cyber-dialogue-in-brussels/.

[36] Jones C. US and EU infosec authorities pen intel-sharing pact: as Cyber Solidarity Act edges closer to full adoption in Europe. 2023. the Register[Available from: https://www.theregister.com/2023/12/07/cisa_enisa_intel_sharing/.

[37] Kelly R. US and EU cyber agencies strike agreement to boost global threat response. IT Pro; 2023 [Available from: https://www.itpro.com/security/us-and-eu-cyber-agencies-strike-agreement-to-boost-global-threat-response.

[38] Schuetze J. EU-US cybersecurity policy coming together: recommendations for instruments to accomplish joint strategic goals. European Union; 2020 [Available from: https://eucyberdirect.eu/research/eu-us-cybersecurity-policy-coming-together-recommendations-for-instruments-to-accomplish-joint-strategic-goals.

[39] European Commission. Digital trade agreements. 2023 [Available from: https://policy.trade.ec.europa.eu/help-exporters-and-importers/accessing-markets/goods-and-services/digital-trade_en.

[40] Nye JS. The regime Complex for managing global cyber activities. 2014. Global Commission on Internet Governance Paper Series No 1.

[41] Schmitt MN, Watts S. Beyond State-centrism: international law and non-state actors in cyberspace. J Confli SecurLaw 2016;21(3):595–611.

[42] Hurwitz R. The play of states: norms and security in cyberspace. Am Foreign Policy Inter 2014;36(5):322–31.

[43] Shackelford S, Craig A. Beyond the new ‘digital divide’: analyzing the evolving role of national governments in internet governance and enhancing cybersecurity. Stanford J Int Law 2014;50:119–84.

[44] Pawlak P. Capacity building in cyberspace as an instrument of foreign policy. Glob Policy 2016;7(1):83–92.

[45] Carr M. Power plays in global internet governance. Millennium 2015;43(2):640–59.

[46] Schmitt MN, Vihul L. The nature of international law cyber norms. In: Tallinn Papers No 5 (NATO Cooperative Cyber Defence Centre of Excellence; 2014.

[47] Waxman M. Cyber-attacks and the use of force: back to the future of article 2(4). Yale J Int Law 2011;36:421.

[48] Roscini M. Cyber operations and the use of force in international law. Oxford: Oxford University Press; 2014.

[49] Schmitt MN. Tallinn manual 2.0 on the international law applicable to cyber operations. 2 ed. Cambridge: Cambridge University Press; 2017.

[50] International Law Commission. Draft articles on responsibility of states for internationally wrongful acts. 2001. United Nations[Available from: https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf.

[51] Banks W. State responsibility and attribution of cyber intrusions after Tallinn 2.0. Tex Law Rev 2017;95(7):1487–513.

[52] Qian X. Redefining international law paradigms: charting cybersecurity, trade, and investment trajectories within global legal boundaries. J World Invest Trade 2024;25(3):295–333.

[53] Schmitt MN. Tallinn manual on the international law applicable to cyber warfare. Cambridge: Cambridge University Press; 2013.

[54] Hakmeh J, Peters A. A new UN cybercrime treaty? The way forward for supporters of an open, free, and secure internet: council on Foreign Relations. 2020 [Available from: https://www.cfr.org/blog/new-un-cybercrime-treaty-way-forward-supporters-open-free-and-secure-internet#:~:text=With%20this%20passage%2C%20supporters%20of,bring%20more%20countries%20to%20their.

[55] United Nations General Assembly. Resolution 74/247. Countering the use of information and communications technologies for criminal purposes: United Nations. 2019 [UN Doc A/RES/74/247: [Available from: https://documents.un.org/doc/undoc/gen/n19/440/28/pdf/n1944028.pdf?token=jbosvSphZg4Na0STZi&fe=true.

[56] Douek E. The rise of content cartels. SSRN Electron J 2020.

[57] Council of Europe. Second additional protocol to the convention on cybercrime on enhanced co-operation and disclosure of electronic evidence. Council of Europe; 2022. Treaty Series No 224.

[58] EDRi. New cybercrime protocol will undermine our privacy to compensate for the rising powers of law enforcement authorities. eDRi; 2022 [Available from: https://edri.org/our-work/new-cybercrime-protocol-will-undermine-our-privacy-to-compensate-for-the-rising-powers-of-law-enforcement-authorities/.

[59] Mulligan SP. Cross-border data sharing under the CLOUD Act 2018. Congressional Research Service, R45173.

[60] Daskal J. Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0. Stanf Law Rev Online 2018;71:9.

[61] ACLU. Coalition letter opposing the CLOUD Act: American Civil Liberties Union. 2018 [Available from: https://www.aclu.org/wp-content/uploads/document/Cloud_Act_Coalition_letter_3-8_clean.pdf.

[62] Borghard ED, Lonergan SW. The Logic of Coercion in cyberspace. Secur Stud 2017;26(3):452–81.

[63] Ruhl C, Hollis DB, Hoffman W, Maurer T. Cyberspace and geopolitics: assessing global cybersecurity norm processes at a crossroads. Carnegie Endowment for International Peace; 2020 [Available from: https://carnegieendowment.org/research/2020/02/cyberspace-and-geopolitics-assessing-global-cybersecurity-norm-processes-at-a-crossroads?lang=en.

[64] Weber RH. Cybersecurity governance – International law as policy driver?. Jusletter IT. 2021.

[65] Liaropoulos AN. Cyberspace governance and State sovereignty. In: Bitros GC, Kyriazis NC, editors. Democracy and an open-economy world order. Cham: Springer International Publishing; 2017. p. 25–35.

[66] Bannelier-Christakis K, Roscini M. Cyber operations and the use of force in international law. J Confl Secur Law 2016;21(2):367–8.

[67] Eichensehr KE. Ukraine, cyberattacks, and the lessons for international law. AJIL Unbound 2022;116:145–9.

[68] Weber RH. Digital Sovereignty revisited. Jusletter IT; 2023.

[69] Crawford J. State responsibility: the general part. Cambridge: Cambridge University Press; 2013.

[70] Articles on responsibility of states for internationally wrongful acts’ UN doc A/56/10. 2001.

[71] Corn GP, Taylor R. Sovereignty in the age of cyber. AJIL Unbound 2017;111:207–12.

[72] Maurer T. Cyber mercenaries: the state, hackers, and power. Cambridge: Cambridge University Press; 2018.

[73] United States v Netyksho, No. 1:18-cr-00215. (DDC 2018).

[74] Milanović M. State responsibility for acts of non-state actors: a comment on Griebel and Plücken. Leiden J Int Law 2009;22(2):307–24.

[75] Military and paramilitary Activities in and against Nicaragua (Nicaragua v United States) [1986]ICJ Rep 14.

[76] Schmitt MN. Cyber Operations and the Jus Ad Bellum revisited. Villanova Law Rev 2011;56:569.

[77] Prosecutor v Tadić (Appeal Judgment) IT-94-1-A (15 July 1999) para 120.

[78] Rid T, Buchanan B. Attributing cyber attacks. J Strat Stud 2014;38(1–2):4.

[79] Kilovaty I. Doxfare: politically motivated leaks and the future of the norm on non-intervention. Harvard Natl Secur J 2018;9:146.

[80] Trail smelter Case (United States v Canada) (1941) 3 RIAA 1905.

[81] Corfu Channel Case (United Kingdom v Albania) [1949]ICJ Rep 4.

[82] Bannelier-Christakis K. Cyber diligence: a low-intensity due diligence principle for low-intensity Cyber operations? Baltic Yearb Int Law 2014;14:23.

[83] Goldsmith JL. The internet and the legitimacy of remote cross-border searches. Univ Chicago Legal Forum 2001;(1):103.

[84] Couzigou I. Securing cyber space: the obligation of states to prevent harmful international cyber operations. Int Rev Law Comput Technol 2018;32(1):37.

[85] Shackelford SJ, Russell S, Kuehn A. Unpacking the international law on cybersecurity due diligence: lessons from the public and private sectors. Chic J Int Law 2016;17(1):1.

[86] Healey J. The Spectrum of National Responsibility for cyberattacks. Brown J World Aff 2011;18(1):57–70.

[87] Clark DD, Landau S. Untangling attribution. Harvard Natl Secur J 2011;2:1.

[88] Bendiek A, Schulze M. Attribution: a major challenge for EU cyber sanctions. 2021. SWP Research Paper 2021/RP 11.

[89] Council of the European Union. EU Cyber Defence Policy Framework. Doc 13177/22 (21 October 2022). (2022 update).

[90] Creemers R. China’s conception of cyber sovereignty: rhetoric and realization. In: Broeders D, Berg BVD, editors. Governing cyberspace: behavior, power, and diplomacy. Rowman & Littlefield Pub Inc; 2020. p. 107–42.

[91] Giles K. Russia’s ‘new’ Tools for confronting the West: continuity and innovation in Moscow’s exercise of power. 2016. Chatham House Research Paper, March 2016.

[92] United Nations General Assembly. Open-Ended working group on developments in the field of information and telecommunications in the context of international security. United Nations; 2021.

[93] Human Rights Council. Resolution 32/13, ’The Promotion, Protection and Enjoyment of Human Rights on the Internet’ (1 July 2016) UN Doc A/HRC/RES/32/13, operative para 1.

[94] Sukumar AM. The UN GGE failed. Is international law in cyberspace doomed As well? 2017 [Available from: https://www.lawfaremedia.org/article/un-gge-failed-international-law-cyberspace-doomed-well#:~:text=The%20GGE%20even%20came%20close,of%20international%20law%20to%20cyberspace.

[95] Okafor OC. Critical third world approaches to international law (TWAIL): theory, methodology, or both? Int Commun Law Rev 2008;10:371–8.

[96] Hill J. The growth of data localization Post-Snowden: analysis and recommendations for U.S. Policymakers and business leaders. SSRN Electron J 2014.

[97] Shahbaz A, Funk A. Freedom on the net 2021: the global drive to control big tech: freedom House. 2021 [Available from: https://freedomhouse.org/report/freedom-net/2021/global-drive-control-big-tech#:~:text=Freedom%20on%20the%20Net%20is,June%202020%20and%20May%202021.

[98] Jiang M. The coevolution of the internet, (Un)civil society, and authoritarianism in China. In: Jacques d, Avery G, Guobin Y, editors. The internet, social media, and a changing China. Philadelphia: University of Pennsylvania Press; 2016. p. 28–48.

[99] Creemers R. Cyber-Leninism: the political culture of the Chinese internet. In: Price M, Stremlau N, editors. Speech and society in turbulent times: freedom of expression in comparative perspective Cambridge. Cambridge University Press; 2017. p. 255–73.

[100] Creemers R. The Chinese Conception of cybersecurity: a conceptual, institutional, and regulatory genealogy. J Contemp China 2024;33(146):173–88.

[101] Kostka G. China’s social credit systems and public opinion: explaining high levels of approval. New Media Soc 2019;21(7):1565–93.

[102] Shen H. China and global internet governance: toward an alternative analytical framework. Chin J Commun 2016;9(3):304–24.

[103] Hariharan G. Centre for Internet & Society – CIS-India. 2014 [5 July 2025]. Available from: https://cis-india.org/internet-governance/blog/marco-civil-da-internet.

[104] Souza CA, Viola M, Lemos R, editors. Brazil’s internet Bill of Rights: a closer look. ITS Rio; 2017.

[105] Couldry N, Mejias UA. Data colonialism: rethinking big Data’s relation to the contemporary subject. Telev New Media 2019;20(4):336–49.

[106] Arun CAI, the Global South. Designing for other Worlds. In: Dubber MD, Pasquale F, Das S, editors. The oxford handbook of ethics of AI. Oxford University Press; 2020. p. 588–606.

[107] African Union. The digital transformation strategy for Africa (2020-2030). African Union; 2020.

[108] Abebe R, Aruleba K, Birhane A, Kingsley S, Obaido G, Remy SL, et al. Narratives and counternarratives on data sharing in Africa. In: Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency; Virtual Event. Association for Computing Machinery; 2021. p. 329–41.

[109] Bastion Gd, Mukku S. Data and the Global South: key issues for inclusive digital development. 2020. Washington, DC.

[110] Heeks R, Ospina AV, Foster C, Gao P, Han X, Jepson N, et al. China’s digital expansion in the Global South: systematic literature review and Future research agenda. 2023. Manchester Centre for Digital Development Working Paper 95.

[111] He A. The digital Silk Road and China’s influence on standard setting. 2022. CIGI Papers No 264.

[112] Schjolberg S, Ghernaouti-Helie SA. Global treaty on cybersecurity and cybercrime. 2nd ed. Stein Schjølberg and Solange Ghernaouti-Hélie; 2011.

[113] Pawlak P, Barmpaliou P-N. Politics of cybersecurity capacity building: conundrum and opportunity. Journal of Cyber Policy 2017;2(1):123–44.

[114] Couture S, Toupin S. What does the notion of "sovereignty" mean when referring to the digital? New Media Soc 2019;21(10):2305–22.

[115] Floridi L. The fight for digital sovereignty: what it is, and why it matters, especially for the EU. Philos Technol 2020;33(3):369–78.

[116] Mueller ML. Against sovereignty in cyberspace. Int Stud Rev 2019;22(4): 779–801.

[117] Liaropoulos A. Exploring the complexity of cyberspace governance State sovereignty, multi-stakeholderism, and power politics. J Inf Warfare 2016;15(4): 14–26.

[118] Liberty and Others v United Kingdom app no 58243/00 (ECtHR, 1 July 2008).

[119] Big Brother Watch and Others v United Kingdom apps nos 58170/13, 62322/14 and 24960/15 (ECtHR, 25 May 2021).

[120] Digital Rights Ireland Ltd v minister for Communications joined cases C-293/12 and C-594/12 [2014]ECR I-238.

[121] Granger M-P, Irion K. The court of justice and the data retention directive in digital rights Ireland: telling off the EU legislator and teaching a lesson in privacy and data protection. Eur Law Rev 2014;39(6):834–50.

[122] Svantesson DJB. Solving the internet jurisdiction puzzle. Oxford University Press; 2017.

[123] Swire P, Hemmings J. Mutual legal assistance in an era of globalized communications: the analogy to the visa waiver program, 71. NYU Annual Survey of American Law; 2017. p. 687.

[124] United Nations. Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye (22 May 2015) UN Doc A/HRC/29/32, para 32.

[125] Abelson H, Anderson R, Bellovin SM, Benaloh J, Blaze M, Diffie W, et al. Keys under doormats: mandating insecurity by requiring government access to all data and communications ‡. J Cybersecur 2015;1(1):69–79.

[126] Human Rights Committee. General comment No. 34: article 19: freedoms of opinion and Expression' (12 September 2011) UN doc CCPR/C/GC/34.

[127] United Nations. Report of the Special Rapporteur on the promotion and Protection of the right to freedom of opinion and Expression, Frank La Rue (16 May 2011) UN Doc A/HRC/17/27.

[128] Centrum för rättvisa v Sweden [GC] app no 35252/08 (ECtHR, 25 May 2021).

[129] Escher et al. v Brazil Series C No 200 (Inter-American Court of Human Rights, 6 July 2009).

[130] African Commission on Human and Peoples' Rights, Declaration of Principles on Freedom of Expression and Access to Information in Africa (adopted 10 November 2019, entered into force 17 April 2020).

[131] Barak A. Proportionality: constitutional rights and their limitations. Cambridge University Press; 2012.

[132] Budnitsky S, Jia L. Branding internet sovereignty: digital media and the Chinese–Russian cyberalliance. Eur J Cult Stud 2018;21(5):594–613.

[133] Zeng J, Stevens T, Chen Y. China's solution to global cyber governance: unpacking the domestic discourse of "internet sovereignty. Polit Policy 2017;45 (3):432–64.

[134] Cuihong C. Global Cyber governance: china's contribution and approach. China Quart Int Strategic Stud 2018;4(1):55–76.

[135] Zeng J, Stevens T, Chen Y. China's solution to global cyber governance: unpacking the domestic discourse of "internet sovereignty. Polit Policy 2017;45.

[136] Sherman J. China's war for control of global internet governance. SSRN Electron J 2022.

[137] Jindal D. Shifting cyber agenda in Shanghai Cooperation Organisation: modern diplomacy. 2022 [Available from: https://moderndiplomacy.eu/2022/08/29/shifting-cyber-agenda-in-shanghai-cooperation-organisation/.

[138] International Trade Centre. BRICS Digital Economy Report 2022. 2022.

[139] BRICS. XII BRICS Summit Moscow declaration: BRICS. 2020 [Available from: https://eng.brics-russia2020.ru/images/114/81/1148126.pdf.

[140] Mishra N, Valencia AMP. Digital services and digital trade in the Asia pacific: an alternative model for digital integration? Asia Pacific Law Rev 2023;31(2): 489–513.

[141] Rehman A. India's Foreign policy. Perspective of quad and sco. Global Strategic & Defence News; 2023 [Available from: https://gsdn.live/indias-foreign-policy-in-perspective-of-quad-and-sco/.

[142] Hofmann J, Katzenbach C, Gollatz K. Between coordination and regulation: finding the governance in internet governance. New Media Soc 2016;19(9).

[143] Raymond M, DeNardis L. Multistakeholderism: anatomy of an inchoate global institution. Int Theory 2015;7(3):572–616.

[144] Väljataga A. Back to square one? The fifth UN GGE fails to submit a conclusive report at the UN General Assembly. NATO Cooperative Cyber Defence Centre of Excellence; 2017 [Available from: https://ccdcoe.org/incyder-articles/back-to-square-one-the-fifth-un-gge-fails-to-submit-a-conclusive-report-at-the-un-general-assembly/.

[145] Chaisse J'. The black pit:' Power and pitfalls of digital FDI and cross-border data flows. World Trade Rev 2023;22(1):73–89.

[146] Nocetti J. Contest and conquest: russia and Global internet governance. Int Aff 2015;91(1):111–30.

[147] Tikk E, Kerttunen M. Parabasis: cyber-diplomacy in stalemate. Oslo: Norwegian Institute of International Affairs; 2018.

[148] Kettemann MC. The normative order of the internet: a theory of rule and regulation online. Oxford University Press; 2020.

[149] Kak A, West SM, Whittaker M. Make No mistake—AI is owned by big tech: MIT Technology Review. 2023 [Available from: https://www.technologyreview.com/2023/12/05/1084393/make-no-mistake-ai-is-owned-by-big-tech/#:~:text=Put%20simply%2C%20in%20the%20context,is%20dependent%20on%20these%20firms.

[150] BizNews. Big tech's dominance in ai sparks regulatory scrutiny as startups lean on giants for lifelines 2023.

[151] Koh HH. International law in cyberspace. Harvard Int'l L J Online 2012;54.

[152] Schmitt MN, Vihul L. Sovereignty in cyberspace: lex lata vel non?, 111. AJIL Unbound; 2017. p. 213–8.

[153] Milanovic M. Human Rights treaties and foreign surveillance: privacy in the digital age. Harvard Int Law J 2015;56:81–146.

[154] Land MK, Aronson JD. New technologies for human rights law and practice. Cambridge: Cambridge University Press; 2018.

[155] Finnemore M, Hollis DB. Constructing norms for global cybersecurity. Am J Int Law 2016;110(3):425–79.

[156] Charney S, English E, Kleiner A, Malisevic N, McKay A, Neutze J, et al. From articulation to implementation: enabling progress on cybersecurity norms: microsoft. 2016 [Available from: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmc8.

[157] Eilstrup-Sangiovanni M. Why the world needs an international cyberwar convention. Philos Technol 2018;31(3):379–407.

[158] Sunak R. Undersea cables: indispensable, insecure: policy exchange. 2017 [Available from: https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf.

[159] Scharre P. Army of none: autonomous weapons and the future of war. W. W. Norton & Company; 2018.

[160] National Academies of Sciences Engineering and Medicine. Quantum computing: progress and prospects. The National Academies Press; 2018.

[161] Lewis JA. Cognitive effect and State conflict in cyberspace. Center for Strategic and International Studies; 2018 [Available from: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/180924_Cognitive_Effect_Cyberspace.pdf.

[162] Zuboff S. The age of surveillance capitalism: the fight for a human future at the new frontier of power. 1st ed. New York: PublicAffairs; 2019. x, 691 pages p.

[163] Chaisse J, Lam J. World Investment & Trade: shaping the narrative for a sustainable future. J World Invest Trade 2024;25(1):1.