Online ISSN 3007-3197 Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 5 (2025)

Digital Trade and Cyber Sovereignty: Reconciling WTO Obligations with National Security Priorities

[1]Maseeh Ullah, [2]Fatima Rida Suddle, [3]Sehar Shabbir

Article Details

Keywords: Cross-Border Data Flows, National Treatment Obligations, Security Exceptions, Data Localization Measures, Digital Service Regulations, Wto Dispute Settlement, Internet Governance Models

Maseeh Ullah
PhD Scholar, School of Law, Zhongnan University of Economics and Law, China
advmaseehullah@yahoo.com
Fatima Rida Suddle
Lecturer, Department of Law university of Sialkot Pakistan. suddlefatima@gmail.com
Sehar Shabbir
Bachelor of Science in International Relations (IR), Department of IR, Abbottabad University of Science & Technology, Havelian, Abbottabad.
Email: sardarseher36@gmail.com

ABSTRACT

The proliferation of digital trade has brought international commerce into new legal and geopolitical territories, where national security and cyber sovereignty increasingly shape regulatory frameworks. This study explores the tension between World Trade Organization (WTO) obligations—particularly under the General Agreement on Trade in Services (GATS) and the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)—and state measures justified on grounds of cybersecurity and national sovereignty. The research employs a doctrinal and comparative legal method, analyzing key WTO provisions, national digital trade policies, and dispute settlement jurisprudence, including the landmark Russia – Traffic in Transit case. The study finds that while WTO law permits certain exceptions for national security, the lack of precise boundaries opens the door to potential misuse and regulatory fragmentation. Cyber sovereignty strategies, such as data localization and digital censorship, increasingly challenge the WTO's foundational principles of non-discrimination and market access. The paper concludes that reconciling these competing priorities requires clarifying the scope of national security exceptions, fostering digital trade disciplines through plurilateral agreements, and promoting multilateral cooperation on cyber norms. These reforms are essential to sustaining an open yet secure global digital economy.

INTRODUCTION

The rise of the digital economy has transformed the global trade landscape, enabling the seamless exchange of goods, services, and data across borders. Yet, as digital interconnectivity deepens, so too do concerns over cybersecurity, surveillance, data protection, and national sovereignty. States are increasingly implementing digital regulations grounded in the principle of cyber sovereignty—asserting sovereign control over digital infrastructure, data flows, and online content. These measures, while often justified on security or public policy grounds, present new challenges to the multilateral trade system established by the WTO (Meltzer, 2020).

This article investigates the central research question: *To what extent can WTO members reconcile their international obligations on digital trade with domestic imperatives of cybersecurity and national control?* The study hypothesizes that existing WTO legal frameworks provide a limited but evolving space for such reconciliation, particularly through general and national security exceptions under the GATS and the Agreement on TRIPS.

Employing a doctrinal methodology supplemented by case studies, including key WTO jurisprudence and national regulatory practices, the article examines how WTO provisions apply to digital trade measures such as data localization, platform restrictions, and cybersecurity reviews. The paper highlights the legal ambiguity surrounding national security exceptions and the lack of harmonized norms governing digital trade.

The significance of this research lies in its attempt to clarify the legal balance between open digital markets and sovereign digital governance. As disputes over digital trade intensify—exemplified by U.S. actions against Chinese tech firms and China's cybersecurity regime—there is an urgent need to assess how WTO law can evolve to prevent normative fragmentation while safeguarding legitimate state interests.

The article is structured as follows: Part two explores conceptual foundations of digital trade and cyber sovereignty. Part three analyzes WTO obligations relevant to digital trade. Part four focuses on WTO exceptions that permit regulatory autonomy. Part five presents case studies of digital trade disputes. Part six proposes normative and institutional reforms to align WTO law with cybersecurity challenges. The conclusion summarizes findings and suggests pathways for cooperative digital trade governance in a securitized global environment.

DEFINING THE TERRAIN: DIGITAL TRADE AND CYBER SOVEREIGNTY

UNDERSTANDING DIGITAL TRADE

Digital trade refers to commerce that is enabled or facilitated through digital technologies, encompassing a broad spectrum of cross-border activities including online services, digital goods, cloud computing, e-commerce transactions, digital payments, and the transmission of data. It covers both the sale of digital products—such as software, applications, and multimedia content—and the digital delivery of traditional services such as banking, education, legal consultancy, and healthcare (Khan, 2024). Although the WTO has not formally adopted a comprehensive definition of digital trade, the term is widely used in trade policy to denote both goods and services delivered or conducted digitally. The increasing reliance on cross-border data flows as a means of enabling digital transactions makes data governance a core element of modern trade regulation (Peng, 2015; Khan et al., 2020).

Several WTO agreements are directly or indirectly relevant to the governance of digital trade:

- The GATS regulates trade in services, including commitments made in sectors such as telecommunications, computer-related services, and online service platforms.
- The Agreement on TRIPS applies to the digital environment by mandating the protection and enforcement of intellectual property in cyberspace, including copyright, trademarks, and trade secrets.
- The Information Technology Agreement (ITA) facilitates tariff elimination on a wide range of IT products essential for digital trade, such as computers, semiconductors, and telecommunications equipment.
- The Joint Statement Initiative (JSI) on E-Commerce, launched during the Eleventh WTO Ministerial Conference (MC11) in 2017, represents an effort by a group of WTO members to negotiate multilateral rules on digital trade, focusing on issues such as data flows, paperless trading, consumer protection, and source code disclosure.

As digital trade expands and becomes more intertwined with national policy objectives—including data protection, digital taxation, and cybersecurity—its regulation poses novel challenges that existing WTO frameworks are only beginning to address (Dimitropoulos, 2023; Kahn & Wu, 2020).

THE DOCTRINE OF CYBER SOVEREIGNTY

Cyber sovereignty refers to the principle that a state possesses exclusive authority over its

cyberspace, including control over digital infrastructure, regulation of online content, and governance of data flows within its territorial boundaries. This doctrine positions the internet as a domain subject to traditional notions of state sovereignty, mirroring the principles of non-interference and territorial integrity that underpin international law. Prominently advocated by countries such as China and Russia, cyber sovereignty represents a strategic and ideological departure from the liberal model of a global, open, and interoperable internet. Instead, it emphasizes national control, regulatory autonomy, and the prioritization of domestic interests in cyberspace governance. The doctrine is increasingly institutionalized through domestic laws, such as China's Cybersecurity Law and Russia's Sovereign Internet Law, which assert expansive state authority over digital platforms and data infrastructure (Garibaldi & Deane, 2023).

Key components of cyber sovereignty typically include:

- Mandatory data localization, requiring data generated within a country to be stored and processed domestically;
- Content censorship and information control, enabling state oversight of digital speech and online platforms;
- Regulation and restriction of foreign digital firms, including security reviews, licensing regimes, and investment limitations;
- Strategic autonomy in cybersecurity policy, involving domestic development of technologies, network infrastructure, and surveillance capabilities.

While cyber sovereignty is often justified on the grounds of national security, cultural preservation, and economic independence, it has attracted criticism for enabling digital protectionism, curtailing freedom of expression, and contributing to the fragmentation—or "balkanization"—of the global internet. Moreover, such regulatory approaches challenge the multilateral rules and principles of the WTO, particularly those related to market access, non-discrimination, and the free flow of information. This evolving doctrine raises critical questions about the compatibility of national cybersecurity measures with international trade commitments, necessitating a deeper examination of the legal boundaries within which states may invoke sovereign rights in cyberspace (Qian, 2024).

WTO OBLIGATIONS AND THEIR DIGITAL REACH

GATS AND ITS APPLICATION TO DIGITAL SERVICES

The GATS is the foundational WTO framework governing international trade in services. It

applies to all service sectors, except those supplied in the exercise of governmental authority, and encompasses four distinct *modes of supply*:

1. Cross-border supply (Mode 1) – services supplied from the territory of one member into the territory of another (e.g., software downloads, cloud computing);
2. Consumption abroad (Mode 2) – services consumed by a member's nationals abroad (e.g., international use of streaming services);
3. Commercial presence (Mode 3) – services supplied via foreign investment or local subsidiaries;
4. Presence of natural persons (Mode 4) – services supplied by foreign nationals temporarily present in another member's territory.

Digital trade predominantly falls under Mode 1 and Mode 2, though complex digital business models increasingly blur these distinctions. The application of GATS to digital services depends significantly on whether a WTO member has made commitments in relevant sectors, such as telecommunications, computer and related services, or online content delivery (Peng, 2023).

Two core GATS obligations are particularly relevant to digital trade:

- Market Access (Article XVI): This provision prohibits WTO members from imposing quantitative or qualitative restrictions on the number of service suppliers, total service operations, or the types of legal entities permitted to operate—unless such restrictions are clearly specified in their schedules of commitments. Thus, measures such as blanket bans on foreign cloud service providers or limits on foreign investment in digital platforms may violate Article XVI if not explicitly reserved.
- National Treatment (Article XVII): This clause requires that foreign services and service suppliers receive treatment no less favorable than that accorded to domestic counterparts. Regulatory measures that impose discriminatory licensing requirements, content controls, or operational standards on foreign digital firms—but not on domestic equivalents—can potentially breach this obligation.

For instance, requiring foreign social media platforms to undergo special security reviews, while exempting local providers, could be inconsistent with national treatment obligations if the affected services fall within a committed sector. However, a major interpretive challenge lies in the technological evolution since GATS's adoption in 1995. At that time, the digital economy was in its infancy, and the agreement does not specifically refer to digital services or

e-commerce. This legal ambiguity has prompted debates over whether unscheduled or novel digital services—such as AI-as-a-service or blockchain platforms—fall under existing classifications, and how emerging regulatory practices can be reconciled with GATS disciplines. As digital trade continues to expand, the effective application of GATS to new services remains contingent on both the scope of members' commitments and evolving WTO jurisprudence (Wu, 2021).

MFN AND NON-DISCRIMINATION IN DIGITAL TRADE

The principle of Most-Favored-Nation (MFN) treatment is a cornerstone of the multilateral trading system, enshrined in Article II of the GATS and Article I of the General Agreement on Tariffs and Trade (GATT). Under these provisions, WTO members are obligated to accord equal treatment to "like" services and service suppliers from all other members, thereby preventing discriminatory advantages or disadvantages based on nationality. In the context of digital trade, this means that measures regulating cross-border data flows, digital platforms, or cloud services must not arbitrarily favor or disadvantage service providers from countries. For example, a member imposing restriction on foreign digital services or suppliers that selectively target firms from specific countries—such as through trade sanctions, geo-blocking, or targeted licensing regimes—risks breaching the MFN obligation (Wang, 2023).

Nevertheless, the application of MFN in digital trade is complex due to the technical and regulatory diversity of digital products and services, as well as the strategic nature of some cybersecurity and data governance measures. WTO law allows for limited exceptions to MFN treatment under specific conditions, such as pursuant to security exceptions under Article XIV bis of GATS or Article XXI of GATT, which can justify otherwise discriminatory measures on grounds of national security or public order. Absent such exceptions, discriminatory digital trade policies undermine the predictability and fairness expected in the multilateral system and may provoke retaliatory actions, fragmenting the digital economy into competing national spheres. This principle reinforces the need for transparent, non-discriminatory regulatory approaches that reconcile legitimate national interests with the WTO's commitment to open and fair digital trade (Bogdanova, 2021).

TRIPS AND DIGITAL IP RIGHTS

The Agreement on TRIPS establishes comprehensive standards for the protection and enforcement of intellectual property (IP) rights within the WTO framework. In the digital environment, TRIPS plays a pivotal role in regulating the use, distribution, and protection of

IP assets, including software, digital media, patents related to digital technologies, trade secrets, and domain names. Digital trade has heightened the challenges of IP enforcement, particularly concerning online copyright infringement, unauthorized data replication, and the protection of confidential business information in cyberspace. TRIPS mandates members to provide effective legal remedies against IP violations, including in digital contexts, while balancing enforcement with fair use exceptions and public interest considerations (Khan et al., 2025).

However, the intersection of national security concerns with IP protection raises complex legal tensions. States may invoke national security or public order grounds to restrict foreign access to digital IP assets, particularly in sensitive sectors such as cybersecurity technologies, encryption software, or critical infrastructure technologies. Such restrictions can include export controls, licensing requirements, or outright bans on foreign involvement in IP-rich digital domains. These measures, while potentially justified under WTO security exceptions, may conflict with TRIPS obligations if they amount to arbitrary or unjustifiable discrimination or unnecessary barriers to legitimate trade. The lack of explicit TRIPS provisions addressing national security complicates the legal analysis, often requiring interpretation considering the broader WTO legal framework. Consequently, reconciling national security imperatives with the TRIPS mandate to protect digital IP rights remains a key challenge for WTO members navigating the evolving landscape of digital trade governance (Khan & Ullah, 2024).

NATIONAL SECURITY AND PUBLIC POLICY EXCEPTIONS IN WTO LAW

GENERAL EXCEPTIONS: GATS ARTICLE XIV

Article XIV of the GATS sets out important general exceptions permitting WTO members to adopt measures that would otherwise be inconsistent with their commitments, provided these measures satisfy strict criteria. Specifically, Article XIV allows exceptions for measures necessary to:

- Protect public morals or maintain public order;
- Protect human, animal, or plant life or health; and
- Secure compliance with domestic laws and regulations, including those related to the prevention of fraud or the protection of privacy.

In the context of digital trade and cybersecurity, these provisions offer critical legal space for states to enact policies aimed at safeguarding information infrastructure, protecting personal data, and mitigating cyber threats. Cybersecurity measures—such as data localization,

mandatory encryption standards, or restrictions on foreign digital service providers—may fall within Article XIV's scope if they can be convincingly demonstrated to be "necessary" to achieve legitimate public policy objectives (Khan, 2024).

However, the exception is narrowly construed. Members invoking Article XIV must satisfy a necessity test, showing that the measure is the least trade-restrictive means reasonably available to achieve the stated goal. Moreover, the "chapeau" (introductory clause) of Article XIV requires that such measures be applied in a manner that is non-discriminatory and not a disguised restriction on trade. This means cybersecurity regulations cannot be used as a pretext for protectionism or arbitrary discrimination against foreign services or suppliers (Khan, 2024).

The burden of proof rests with the defending member to establish that the challenged measure meets both the necessity requirement and the chapeau conditions. WTO dispute settlement panels have underscored the rigorous nature of this assessment, emphasizing objective evaluation and proportionality. Therefore, while Article XIV provides a vital legal foundation for reconciling national security and public interest concerns with WTO obligations, its application to digital trade requires careful legal and factual analysis to avoid undermining the principle of open and fair markets (Khan & Jiliani, 2023).

SECURITY EXCEPTIONS: GATS ARTICLE XIV BIS AND GATT ARTICLE XXI

The WTO framework explicitly recognizes the primacy of essential security interests by providing robust exceptions under GATS Article XIV bis and GATT Article XXI. These provisions permit WTO members to take any measures they consider necessary to protect their essential security interests, thereby carving out a legal space for sovereign action in circumstances implicating national security.

The scope of security exceptions under these articles encompasses:

- The protection of critical infrastructure, including digital networks, telecommunications systems, and information technology platforms vital to national security;
- Measures taken in time of war or other emergency in international relations, reflecting heightened security concerns during conflicts or geopolitical crises;
- Actions related to the trade in arms, ammunition, and fissionable materials, which are traditionally sensitive areas linked to defense and international peace.

The 2019 WTO dispute panel ruling in Russia – Traffic in Transit provided critical clarification on the nature and application of these security exceptions. The panel confirmed

that while members have considerable discretion in determining what constitutes essential security interests and the necessity of measures taken, this discretion is not entirely self-judging. The WTO retains authority to review whether the invocation of the security exceptions is bona fide or an abuse of the provision. This implies that measures that are disguised protectionism or economic retaliation may be subject to legal challenge (Khan & Usman, 2023).

In the context of digital trade, these provisions allow states to justify restrictive cybersecurity measures, data localization requirements, or restrictions on foreign digital firms on national security grounds. However, the broad wording and high threshold for adjudication create a complex balance between respecting sovereign security prerogatives and maintaining a rules-based trading system. Thus, GATS Article XIV bis and GATT Article XXI serve as critical legal instruments for reconciling WTO commitments with sovereign security priorities in an increasingly securitized digital trade environment, while also imposing a duty on members to exercise these exceptions responsibly and transparently (Khan et al., 2023).

CASE STUDIES: CONFLICTS AND PRECEDENTS

CHINA'S CYBERSECURITY LAW AND WTO COMPATIBILITY

China's Cybersecurity Law (CSL), enacted in 2017, represents one of the most comprehensive regulatory frameworks addressing data governance, cybersecurity, and digital trade within a sovereign context. The law mandates data localization, requiring that personal and important data collected or generated within China's borders be stored domestically. It also imposes security review requirements on foreign digital service providers and technology products deemed critical to national security (Khan, 2023).

These provisions have attracted significant international scrutiny and criticism. Opponents argue that China's data localization and security review mandates are inconsistent with its WTO commitments, particularly under the GATS in the telecommunications and computer-related services sectors. The restrictions are seen as creating market access barriers by limiting foreign digital firms' ability to provide cross-border cloud services and operate freely in the Chinese market. Additionally, they potentially breach the national treatment obligation by imposing onerous compliance burdens selectively on foreign entities (Liu et al., 2023).

China, however, defends these measures on grounds of national security, invoking the general exceptions under GATS Article XIV and the security exceptions under Article XIV bis. It

asserts that the law is essential for protecting critical information infrastructure, safeguarding personal data, and ensuring cybersecurity in an era marked by rising cyber threats and geopolitical tensions. From this perspective, the CSL is a legitimate exercise of cyber sovereignty, aimed at balancing the demands of digital openness with the imperatives of state security (Khan & Ximei, 2022).

The legal tension between China's national cybersecurity priorities and its multilateral trade obligations exemplifies the broader challenge of reconciling WTO rules with evolving state practices in cyberspace. It raises fundamental questions about the scope of national security exceptions, the limits of regulatory discretion, and the potential need for WTO disciplines tailored specifically to digital trade and cybersecurity governance (Khan et al., 2022).

U.S. RESTRICTIONS ON TIKTOK AND HUAWEI

In recent years, the United States has enacted a series of bans and restrictions targeting Chinese technology firms, notably TikTok and Huawei, citing national security risks related to data privacy, espionage, and critical infrastructure vulnerabilities. These measures include prohibitions on government use of Huawei equipment, efforts to limit Huawei's participation in 5G networks, and attempts to restrict TikTok's operations and data handling within the U.S. market. From a WTO law perspective, such unilateral actions raise significant questions about their compatibility with multilateral trade rules, particularly the security exception under Article XXI of the GATT. Article XXI allows members to take any measures they consider necessary for the protection of their essential security interests, but the breadth and limits of this exception remain subjects of debate and have only recently been scrutinized through WTO dispute settlement panels (Khan, 2022).

If challenged before the WTO, the U.S. would need to demonstrate that its restrictions on TikTok and Huawei are bona fide measures genuinely motivated by essential security interests, such as protecting critical information infrastructure or national defense systems. The 2019 panel ruling in Russia – Traffic in Transit provided some guidance, confirming that the security exception is not wholly self-judging and that WTO adjudicators retain the authority to assess claims of abuse or bad faith invocation (Khan & Wu, 2021).

The outcome of any potential WTO dispute would have profound implications for the balance between legitimate national security concerns and the prohibition of disguised economic protectionism. A ruling against the U.S. could constrain the scope of permissible security measures under WTO law, compelling greater transparency and proportionality in the

regulation of foreign digital firms. Conversely, upholding the U.S. measures could reinforce states' sovereign discretion to regulate digital trade in the name of security, potentially accelerating fragmentation of the global digital economy. These dynamic underscores the ongoing tension between maintaining an open, rules-based digital trade regime and addressing rapidly evolving cybersecurity threats in a geopolitically charged environment (Abdelrehim Hammad et al., 2021).

BRIDGING THE DIVIDE: TOWARDS RECONCILIATION

ENHANCING CLARITY IN WTO SECURITY EXCEPTIONS

The ambiguous language and broad scope of the WTO security exceptions under GATS Article XIV bis and GATT Article XXI have led to uncertainty and divergent interpretations among members. This lack of clarity risks undermining the predictability and stability of the multilateral trading system, especially as digital trade and cybersecurity concerns increasingly intersect.

To address these challenges, there is a pressing need for the WTO to enhance guidance and transparency around the invocation of security exceptions. Potential reforms could include:

- Establishing a peer review mechanism: A structured process whereby WTO members review and assess the legitimacy and necessity of security-related trade measures. Such a mechanism would promote accountability, build mutual trust, and reduce the risk of abuse or disguised protectionism.
- Developing a checklist or indicators for legitimate security concerns: Creating clear criteria or benchmarks to help distinguish bona fide security measures from unjustified trade restrictions. These indicators could cover aspects such as proportionality, evidence of threat, consistency with international security norms, and non-discrimination.

These reforms would help reconcile the competing demands of national security and trade openness by fostering a more transparent, rules-based framework. They would also support members in navigating the complex and evolving challenges of regulating digital trade while safeguarding essential security interests. By clarifying the parameters of security exceptions, the WTO can strengthen its role as a forum for cooperation and dispute resolution in the digital age, preventing fragmentation and ensuring that security measures are applied responsibly and proportionately (Usman, 2021).

INCORPORATING DIGITAL TRADE DISCIPLINES IN FTAS AND PLURILATERAL AGREEMENTS

In response to the slow pace of multilateral negotiations on digital trade, bilateral and regional trade agreements (FTAs) have become key platforms for advancing digital trade disciplines. Prominent agreements such as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), the Digital Economy Partnership Agreement (DEPA), and the Regional Comprehensive Economic Partnership (RCEP) increasingly include provisions that address the unique challenges and opportunities posed by digital trade (Khan & Wu, 2021).

These agreements typically incorporate norms such as:

- Prohibitions on data localization requirements, promoting the free flow of information across borders;
- Commitments to interoperability and harmonization of digital regulations, enabling seamless cross-border digital transactions and reducing compliance costs for businesses;
- Protection of source code and algorithms, limiting forced disclosure requirements;
- Rules on digital payments, consumer protection, and cybersecurity cooperation, fostering trust and stability in digital markets.

Such provisions often go beyond the current WTO framework, reflecting the priorities and policy innovations of the participating states. These FTAs act as experimental laboratories where new rules and standards for digital trade governance can be tested and refined. Over time, successful elements from these plurilateral arrangements may inform and catalyze broader WTO reforms aimed at establishing more comprehensive and harmonized global disciplines on digital trade. Consequently, while the WTO remains the principal venue for global trade governance, the increasing prominence of FTAs and plurilateral agreements underscores a multi-layered approach to reconciling trade liberalization with digital sovereignty and security concerns (Khan et al., 2021).

PROMOTING MULTILATERAL COOPERATION ON CYBER NORMS

Given the inherently transnational nature of cyberspace, effective governance of digital trade and cybersecurity demands robust multilateral cooperation beyond the trade domain. Key international bodies such as the United Nations Group of Governmental Experts (UN GGE), the Organisation for Economic Co-operation and Development (OECD), and the G20 possess valuable expertise and convening power to complement the WTO's trade mandate.

These institutions should collaborate with the WTO to build consensus on critical issues,

including:

- Shared definitions of cybersecurity threats, establishing a common understanding of risks such as cyber espionage, sabotage, and data breaches;
- Best practices for balancing digital openness with national resilience, ensuring that states can protect critical infrastructure without unnecessary trade restrictions;
- Mechanisms for cross-border data governance that respect national sovereignty while facilitating the free flow of data essential for global commerce.

Such cooperation can enhance policy coherence, reduce regulatory fragmentation, and foster trust among WTO members. Integrating cyber norms developed in broader international forums into the trade framework can strengthen the legitimacy and effectiveness of WTO rules, thereby advancing a secure and inclusive digital trading system (Khan et al., 2021).

CONCLUSION

This study highlights the complex and evolving interplay between WTO obligations on digital trade and the assertion of national security priorities through cyber sovereignty. As digital commerce grows exponentially and cyber threats intensify, states face the difficult task of balancing open, rules-based trade with the legitimate need to protect critical infrastructure, data privacy, and national security interests. Key findings reveal that while WTO provisions such as GATS, TRIPS, and GATT provide a foundational framework for regulating digital trade, their application to cybersecurity and data governance raises significant challenges. The general and security exceptions under Articles XIV, XIV bis, and XXI offer important legal space for sovereign measures but require clearer interpretation and oversight to prevent abuse and ensure proportionality.

At the same time, national laws like China's Cybersecurity Law and unilateral actions such as the U.S. restrictions on TikTok and Huawei demonstrate the growing tensions between multilateral trade commitments and sovereign security imperatives. These developments underscore the urgent need for WTO reform and enhanced multilateral cooperation on cyber norms. Looking ahead, the integration of digital trade disciplines in FTAs and plurilateral agreements and stronger collaboration with international bodies such as the UN GGE, OECD, and G20 can provide practical pathways toward greater coherence and predictability in this domain. Future research should focus on developing robust mechanisms for transparency, accountability, and peer review of security measures, as well as exploring innovative models for cross-border data governance that respect both sovereignty and trade

facilitation. Ultimately, bridging the divide between digital trade liberalization and cyber sovereignty is critical not only for the stability of the global trading system but also for fostering trust, innovation, and sustainable economic development in the digital era. This research invites policymakers, scholars, and practitioners to engage collaboratively in shaping a balanced and forward-looking governance framework that reconciles these competing imperatives.

REFERENCES

Abdelrehim Hammad, A. A., Khan, A., & Soomro, N. E. (2021). Digital Economy Barriers to Trade Regulation Status, Challenges, and China's Response. *International Journal of Social Sciences Perspectives*, *8*(2), 41-49.

Bogdanova, I. (2021). Targeted economic sanctions and WTO law: Examining the adequacy of the national security exception. *Legal Issues of Economic Integration*, *48*(2).

Dimitropoulos, G. (2023). The WTO new national security challenge. In *The Elgar Companion to the World Trade Organization* (pp. 619-637). Edward Elgar Publishing.

Garibaldi, S., & Deane, F. (2023). Cyberspace as a fifth dimension of national security: trade measure exceptions. *Journal of International Trade Law and Policy*, *22*(2), 67-88.

Kahn, A., & Wu, X. (2020). Impact of digital economy on intellectual property law. *J. Pol. & L.*, *13*, 117.

Khan, A. (2022). E-commerce Regulations in Emerging Era: The Role of WTO for Resolving the Complexities of Electronic Trade. *ASR Chiang Mai University Journal Of Social Sciences And Humanities.*

Khan, A. (2023). Rules on Digital Trade in the Light of WTO Agreements. *PhD Law Dissertation, School of Law, Zhengzhou University China.*

Khan, A. (2024). The Emergence of the Fourth Industrial Revolution and its Impact on International Trade. *ASR: CMU Journal of Social Sciences and Humanities (2024) Vol, 11.*

Khan, A. (2024). The Intersection Of Artificial Intelligence And International Trade Laws: Challenges And Opportunities. *IIUMLJ*, *32*, 103.

Khan, A., & Jiliani, M. A. H. S. (2023). Expanding The Boundaries Of Jurisprudence In The Era Of Technological Advancements. *IIUMLJ*, *31*, 393.

Khan, A., & Ullah, M. (2024). The Pakistan-China FTA: legal challenges and solutions for marine environmental protection. *Frontiers in Marine Science*, *11*, 1478669.

Khan, A., & Usman, M. (2023). THE EFFECTIVENESS OF INTERNATIONAL LAW: A COMPARATIVE ANALYSIS. *International Journal of Contemporary Issues in Social Sciences*, *2*(3), 780-786.

Khan, A., & Wu, X. (2021). Bridging the Digital Divide in the Digital Economy with Reference to Intellectual Property. *Journal of Law and Political Sciences*, *28*(03), 256-263.

Khan, A., & Wu, X. (2021). Reforms for culmination of the deadlock in appellate body of WTO: An agenda of saving the multilateral trading system. *Journal of Humanities, Social and Management Sciences (JHSMS)*, *2*(1), 50-62.

Khan, A., & Ximei, W. (2022). Digital economy and environmental sustainability: Do Information Communication and Technology (ICT) and economic complexity matter?. *International journal of environmental research and public health*, *19*(19), 12301.

Khan, A., Abd Elrhim, A. A., & Soomro, N. E. (2021). China Perspective in Reforming of the World Trade Organization. *J. Pol. & L.*, *14*, 104.

Khan, A., Amjad, S., & Usman, M. (2020). The Role of Customary International Law in Contemporary International Relations. *International Review of Social Sciences*, *8*(08), 259-265.

Khan, A., Jillani, M. A. H. S., Abdelrehim Hammad, A. A., & Soomro, N. E. H. (2021). Plurilateral negotiation of WTO E-commerce in the context of digital economy: Recent issues and developments. *Journal of Law and Political Sciences*.

Khan, A., Jillani, M. A. H. S., Ullah, M., & Khan, M. (2025). Regulatory strategies for combatting money laundering in the era of digital trade. *Journal of Money Laundering Control*, *28*(2), 408-423.

Khan, A., Usman, M., & Amjad, S. (2023). The digital age legal revolution: taped's trailblazing influence. *International journal of contemporary issues in social sciences*, *2*(4), 524-535.

KHAN, M. I., Usman, M., KANWEL, S., & Khan, A. (2022). Digital Renaissance: Navigating the Intersection of the Digital Economy and WTO in the 21st Century Global Trade Landscape. *Asian Social Studies and Applied Research (ASSAR)*, *3*(2), 496-505.

Khan, U. (2024). The World Trade Organization and International Law: Balancing Trade, Sovereignty, and Global Governance. *Journal of Law, Society and Policy Review*, *1*(02), 01-17.

Liu, X., Khan, M., & Khan, A. (2023). The Law and Practice of Global ICT Standardization by

Olia Kanevskaia [CUP, Cambridge, 2023, xxvi+ 361pp, ISBN: 978-1-0093-00575, £ 95.00 (h/bk)]. *International & Comparative Law Quarterly*, *72*(4), 1094-1097.

Meltzer, J. P. (2020). Cybersecurity, digital trade, and data flows: Re-thinking a role for international trade rules. *Global Economy & Development WP*, *132*.

Peng, S. Y. (2015). Cybersecurity threats and the WTO national security exceptions. *Journal of International Economic Law*, *18*(2), 449-478.

Peng, S. Y. (2023). Cybersecurity and trade governance. In *The Elgar Companion to the World Trade Organization* (pp. 35-50). Edward Elgar Publishing.

Qian, X. (2024). Redefining International Law Paradigms: Charting Cybersecurity, Trade, and Investment Trajectories within Global Legal Boundaries. *The Journal of World Investment & Trade*, *25*(3), 295-333.

Usman, M. U. H. A. M. M. A. D., Khan, A. S. I. F., & Amjad, S. O. H. A. I. L. (2021). State Responsibility and International Law: Bridging the Gap.

Wang, X. (2023). Decoupling Trade and Cybersecurity: A Way to Recalibration?. *Asian J. WTO & Int'l Health L & Pol'y*, *18*, 39.

Wu, C. H. (2021). Sovereignty fever: The territorial turn of global cyber order. *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht/Heidelberg Journal of International Law*, *81*(3), 651-676.