Summer, 2026
Vol. XVII, No. 2

Trade, Law *and* Development

EDITORIALS

Dr. Bipin Kumar, *Note from the Chief Editor's Desk*

Alka Nanda Mahapatra & Samiksha Lohia, *Foreword*

ARTICLES

Christian Delev, *No Small Fry? The Colombia — Frozen Fries Proceedings and the Long Road to WTO Dispute Settlement Reform*

I-Ju Chen, *Fishery Sustainability and the WTO Fisheries Subsidies Agreement: Its Causes, Consequences, and Prospects*

Jeremmy Okonjo, *Ideology Critique of Trade Liberalisation in the Digital Trade Era: The Economics-Law-Technology Ideology Nexus*

Jyotsna Manohar, *Security Exceptionalism and Developmental Asymmetry: National Security at the Trade-Technology Nexus*

Lorenzo Cotula, *Commodities and Sustainability in International Trade Treaties: Insights from the EU-Indonesia Comprehensive Economic Partnership Agreement*

Lukasz Gruszczyński & Marcin J. Menkes, *Memoranda of Understanding and Critical Minerals: Evolution of International Economic Law?*

Dr. Pralok Gupta & Dr. Shagufta Naaz, *The European Union Carbon Border Adjustment Mechanism: Compatibility with WTO Laws and Implications for FTAs*

Rafael Leal-Arcas et al., *Reconciling Trade and Environmental Protection in WTO Law: Adjudication, Fragmentation, and Regulatory Space*

Triplicane Damodaran Satish, *'Ex-Officio' Trade Remedy Investigations: Jurisprudence and Practice*

NOTES & COMMENTS

Carlos Lopes, *Navigating Turbulent Waters: Africa's Key Dilemmas and Challenges*

Trade, Law *and* Development

Vol. 17, No. 2 2026

ISSN: 0976 - 2329
eISSN: 0975 - 3346

Trade, Law *and* Development

Vol. 17, No. 2 2026

TABLE OF CONTENTS

ARTICLES, NOTES, AND COMMENTS

1. No Small Fry? The Colombia — Frozen Fries Proceedings and the Long Road to WTO Dispute Settlement Reform

   Christian Delev …248

2. Fishery Sustainability and the WTO Fisheries Subsidies Agreement: Its Causes, Consequences, and Prospects

   I-Ju Chen …276

3. Ideology Critique of Trade Liberalisation in the Digital Trade Era: The Economics-Law-Technology Ideology Nexus

   Jeremmy Okonjo …310

4. Security Exceptionalism and Developmental Asymmetry: National Security at the Trade-Technology Nexus

   Jyotsna Manohar …354

5. Commodities and Sustainability in International Trade Treaties: Insights from the EU-Indonesia Comprehensive Economic Partnership Agreement

   Lorenzo Cotula …390

6. Memoranda of Understanding and Critical Minerals: Evolution of International Economic Law?

   Lukasz Gruszczyński & Marcin J. Menkes …418

7. The European Union Carbon Border Adjustment Mechanism: Compatibility with WTO Laws and Implications for FTAs

Dr. Pralok Gupta & Dr. Shagufta Naaz …447

8. Reconciling Trade and Environmental Protection in WTO Law: Adjudication, Fragmentation, and Regulatory Space

Rafael Leal-Arcas et al. …478

9. 'Ex-Officio' Trade Remedy Investigations: Jurisprudence and Practice

Triplicane Damodaran Satish …519

10. Navigating Turbulent Waters: Africa's Key Dilemmas and Challenges

Carlos Lopes …562

Trade, Law *and* Development

Cite As: Jyotsna Manohar, *Security Exceptionalism and Developmental Asymmetry: National Security at the Trade-Technology Nexus*
17(2) TRADE L. & DEV. 354 (2026)

SECURITY EXCEPTIONALISM AND DEVELOPMENTAL ASYMMETRY: NATIONAL SECURITY AT THE TRADE-TECHNOLOGY NEXUS

JYOTSNA MANOHAR*

Traditional conceptions of national security have undergone various evolutions in recent decades, moving away from pure military aggression by a State to a new range of threats, which include cyber threats, climate change, and pandemics. In recent years, World Trade Organization (WTO) members have increasingly invoked national security justifications to defend national policies designed to address these threats, such as export controls, digital trade restrictions, sanctions regimes, and strategic industrial subsidies. Consequently, such measures increasingly clash with trade rules that remain firmly rooted in the post-war context of their drafting, and have not evolved at the same pace as the security threats themselves. Tracing the evolution of the national security exception since its inception to the most recent WTO panel rulings on its interpretation, this paper seeks to explore the relationship between national security, international trade, technology, and its impact on development. Given the sensitive nature of national security and the immense scope for misuse of national security carve-outs, it is vital to ensure a balance between trade, evolving national security considerations, and development. The second half of the paper seeks to explore this relationship and contend with how these different interests can be reconciled within the global trading system.

TABLE OF CONTENTS

I. INTRODUCTION
II. LEGAL FOUNDATIONS OF THE SECURITY EXCEPTION
  A. NEGOTIATING HISTORY OF THE SECURITY EXCEPTION
  B. OVERVIEW OF THE NATIONAL SECURITY EXCEPTION THROUGH WTO DISPUTE SETTLEMENT

* Jyotsna Manohar is an international trade lawyer and holds an LLM in transnational law from King's College London. The author may be contacted at jyotsna.manohar[at]gmail.com.

C. EVOLUTION OF THE NATIONAL SECURITY EXCEPTION THROUGH WTO DISPUTE SETTLEMENT
1. RUSSIA — MEASURES CONCERNING TRAFFIC IN TRANSIT
2. SAUDI ARABIA — MEASURES CONCERNING THE PROTECTION OF INTELLECTUAL PROPERTY RIGHTS
3. UNITED STATES — CERTAIN MEASURES ON STEEL AND ALUMINIUM
4. UNITED STATES — ORIGIN MARKING REQUIREMENT
5. KEY TAKEAWAYS
III. TECHNOLOGY RESTRICTIONS VIA SECURITY CLAIMS: AN ASSESSMENT OF POTENTIAL VIOLATIONS UNDER OTHER WTO AGREEMENTS/THE TBT AGREEMENT
A. LIKENESS
B. NO LESS FAVOURABLE TREATMENT
C. NO MORE TRADE RESTRICTIVE THAN NECESSARY
D. INTERNATIONAL STANDARDS
IV. THE EVOLVING NATIONAL SECURITY CHALLENGE: IS THE WTO FIT FOR PURPOSE?
A. NEW CENTURY, NEW SECURITY
B. IS THE WTO SECURITY EXCEPTION FIT FOR PURPOSE?
C. EMERGING TRENDS IN PTAS, RTAS, AND FTAS
V. IMPLICATIONS ON DEVELOPMENT AND INNOVATION
VI. POLICY RECOMMENDATIONS
VII. CONCLUDING REMARKS

I. INTRODUCTION

The interface between trade, security, and technology is an increasingly complex and relevant space in today's globalised world. Trade and security have existed in the same sphere since the very inception of the multilateral trading system, and indeed, global security was a fundamental rationale driving the establishment of the rules-based multilateral trading system that has now become the WTO.[1] In the years following the Great Wars, there was a growing consensus that a world that was more closely integrated through trade would create a sense of collective security and encourage nations to co-exist peacefully.[2] Similarly, technology and trade have also historically been inextricably linked, as it was only through trade that different technologies were able to be disseminated and innovation was able to advance on a

[1] CLAIR WILCOX, A CHARTER FOR WORLD TRADE (1949).
[2] *Id.* at 2.

global scale.[3] Technology and security considerations have also not been mutually exclusive, as both the Second World War and Cold War eras were characterised by a race between nations to develop and deploy superior technologies in pursuit of their national security interests. Indeed, even then, a response to threats from antagonistic nations' technological advancements included trade measures. Most notably, the United States (U.S.) response to the Soviet Union's development of nuclear weapons and other associated technologies was the 'offset strategy', which was an effort to use innovation and technology to offset the Soviet Union's perceived technological lead.[4]

A modernised multilateral trading system, combined with technological advancements in recent decades, has led to the creation of interlinked global value chains, thus gradually detaching production and distribution from domestic processes.[5] Simultaneously, nations are also faced with emerging threats to security, including those to international trade and development, primarily driven by technological advancements that did not exist at the time of drafting foundational international agreements. This has resulted in the lack of a common understanding of what could constitute 'security issues', as traditional notions of security that primarily involved inter-state conflicts, have now been expanded to include non-state actors, terrorism, cybersecurity, pandemics, and environmental concerns.[6]

In most cases, there is no intrinsic conflict between trade and economic liberalisation and the pursuit of other legitimate national objectives, such as the protection of public morals or human, animal, or plant life, or in the interests of national security through the use of one of the legitimate exceptions in WTO Agreements.[7] However, with the blurring of lines between trade and security, compounded in part due to technological advancements, States are forced to take a more nuanced and holistic approach in defining threats to national security, which in turn has significant

---

[3] WILLIAM J BERNSTEIN, A SPLENDID EXCHANGE: HOW TRADE SHAPED THE WORLD (2008).

[4] LINDA WEISS, AMERICA INC.?: INNOVATION AND ENTERPRISE IN THE NATIONAL SECURITY STATE (2018), https://www.degruyter.com/document/doi/10.7591/9780801471131/html.

[5] RICHARD E. BALDWIN, THE GREAT CONVERGENCE: INFORMATION TECHNOLOGY AND THE NEW GLOBALIZATION (2016).

[6] J. Benton Heath, *The New National Security Challenge to the Economic Order*, 129 YALE L. J. 1028 (2020).

[7] General Agreement on Tariffs and Trade art. XX, Oct. 30, 1947, 55 U.N.T.S. 194 [hereinafter GATT 1947]; General Agreement on Tariffs and Trade 1994, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1A, 1867 U.N.T.S. 187 [hereinafter GATT 1994]; General Agreement on Trade in Services, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1869 U.N.T.S. 183 [hereinafter GATS].

implications on the level of trade liberalisation they are willing to countenance. Higher levels of global economic integration have also raised concerns about 'weaponised' interdependence'.[8] As such, States have become more inclined to resort to trade and investment restrictions — as opposed to diplomatic measures, as the preferred tool to address novel security concerns, particularly in the context of technology and digital trade.[9] This includes import/export restrictions on foundational technologies and digital equipment, data localisation requirements, source code disclosures, and other technical regulations, as well as cybersecurity measures to address digital threats.

This paper seeks to explore the tripartite relationship between international trade, technology, and national security, and consider the implications that it may have on innovation and development. The article proceeds in the following manner: Part II provides a background of the national security exception in WTO Agreements, including the negotiating history of the security exception of the General Agreement on Tariffs and Trade, 1947 (GATT 1947), and the evolution of the interpretation of the article through dispute settlement. Part III covers another means through which national security objectives can be pursued by Members despite their trade-restrictive impacts: the Technical Barriers to Trade (TBT) Agreement. Part IV considers the evolution of security threats in recent years, including the rise of new challenges and how States are opting to combat them, including cybersecurity measures. This section will also look at agreements outside of the multilateral system, such as Preferential Trade Agreements, Regional Trade Agreements, and Free Trade Agreements, to assess how these relative contemporary agreements have sought to address emerging technology-related threats. Part V considers the impact of the national security-trade-technology nexus on development, assessing the importance of maintaining a balance between these interests. Part VI offers some policy recommendations for reconciling these various interests, and the final Part concludes.

II. LEGAL FOUNDATIONS OF THE SECURITY EXCEPTION

The security exception was included for the first time in a trade agreement in the GATT 1947;[10] It was constructed to be virtually a complete escape clause from all

---

[8] Henry Farrell & Abraham L Newman, *Weaponized Interdependence: How Global Economic Networks Shape State Coercion*, 44 INT'L. SEC. (2019).
[9] Joshua P. Meltzer, *Cybersecurity, Digital Trade, and Data Flows: Re-thinking a Role for International Trade Rules* (Global Econ. & Dev. Working Paper No. 132, 2020), https://www.brookings.edu/wp-content/uploads/2019/11/Cybersecurity-digital-trade-data-flows.pdf [hereinafter Meltzer].
[10] GATT 1947, *supra* note 7, art. XXI.

trade commitments.[11] This is the foundational document that informed later agreements under the WTO system, including the General Agreement on Tariffs and Trade 1994 (GATT 1994).[12] The language of the security exception, found in Article XXI of the GATT 1994, which formed the blueprint for security exceptions in other WTO agreements, is an exact copy of the original provision in the GATT 1947. Given the importance of the GATT 1947 in shaping the modern multilateral trading system under the WTO, an analysis of the intentions of the Contracting Parties at the time of drafting the security exception in this agreement would prove useful in order to better understand the scope and limits of Article XXI and its sister provisions in other WTO Agreements.

A. *Negotiating History of the Security Exception*

Following the end of the Second World War, members of the international community came together to negotiate the establishment of the International Trade Organization (ITO). Envisaged to be an international organisation comprising United Nations (UN) Member States, such as the U.S. and the United Kingdom (U.K.), negotiations began at the United Nations Conference on Trade and Employment (UNCTAD) between 1946 and 1948, and were meant to legally consolidate negotiations on tariff reductions.[13] Post-war multilateral institution-building was largely predicated on the notion that a world that was more closely integrated through trade and an interconnected global economy would be a more secure and peaceful place for nations to co-exist.[14] Such co-dependence and cooperation would reduce the likelihood of future conflicts.[15]

The GATT 1947 was originally envisaged as a provisional agreement to be in place whilst States negotiated the ITO Charter, and it eventually became the main text for international trade when the ITO ultimately failed to receive approval from the U.S.[16]

The drafting history of the GATT 1947 highlights that the security exception under Article XXI was essentially envisaged as a balancing act between two divergent and

[11] Jacob Gladysz, *The National Security Exception in WTO Law: Emerging Jurisprudence and Future Direction*, 52 GEO. J. INT'L. L. 387 (2021).
[12] GATT 1994, *supra* note 7.
[13] Memorandum by the Deputy Director, Office of Int'l. Trade Policy (Nitze) to the Under Secretary of State for Econ. Affairs (Clayton) (Dec. 5, 1946), https://history.state.gov/historicaldocuments/frus1946v01/d703.
[14] Simon Lacey, *Trade, Technology and Security: Exploring the Linkages*, 6 (Inst. Int'l. Trade, Univ. Adel., Working Paper No. 06, 2022), https://ssrn.com/abstract=4217251.
[15] Anne-Marie Slaughter & Gordon LaForge, *Opening Up the Order: A More Inclusive International System*, 100 FOREIGN AFF. 154, 154–55 (2021).
[16] William Diebold Jr., *The End of the I.T.O*, *in* ESSAYS IN INTERNATIONAL FINANCE, No. 16, at 24 (1975).

potentially conflicting interests, namely: permitting Members to have some latitude for measures taken in pursuance of their legitimate security interests, whilst ensuring that the exception is not so broad so as to allow Members to use restrictive measures for commercial or protectionist purposes under the guise of security.[17] Even the U.S., which played perhaps the largest role in the framing of the language of the security exception, was keen to ensure that national security and trade liberalisation co-exist in a balanced fashion and never intended for such an exception to be construed in a purely self-judging manner.[18] During the Geneva Round of negotiations for the ITO, the U.S. delegation, in response to a question regarding what would constitute an 'essential security interest', stated:

> We recognized that there was a great danger of having too wide an exception and we could not put it into the Charter, simply by saying: 'by any Member of measures relating to a Member's security interests,' because that would permit anything under the sun. Therefore, we thought it well to draft provisions which would take care of really essential security interests and, at the same time, so far as we could, to limit the exceptions and to adopt that protection for maintaining industries under every conceivable circumstance…
>
> I think there must be some latitude here for security measures. It is really a question of balance. We have got to have some exceptions. We cannot make it too tight, because we cannot prohibit measures which are needed purely for security reasons. On the other hand, we cannot make it so broad that, under the guise of security, countries will put on measure which really have a commercial purpose. We have given considerable thought to it and this is the best we could produce to preserve that proper balance.[19]

Thus, despite the U.S.' current position on the self-judging nature of the security exception, it is clear from the negotiating history that Members intended to strike a balance between two competing interests and not open the gates to misuse under the guise of national security.[20]

---

[17] WORLD TRADE. ORG., WTO ANALYTICAL INDEX, ART. XXI 600 (2012); *see also* U.N. Conference on Trade and Employment, *Report of the Second Session of the Preparatory Committee*, U.N. Doc. E/PC/T/186 (Sep. 10, 1947) [hereinafter UNCTAD Report].

[18] Daria Boklan & Amrita Bahri, *The First WTO's Ruling on National Security Exception: Balancing Interests or Opening Pandora's Box?*, 19 WORLD TRADE REV. 123, 132 (2020).

[19] UNCTAD report, *supra* note 18.

[20] For a full analysis of the negotiating history of the ITO and GATT 1947 security exception provision, *see* Stephen Kho et al., *The Conundrum of the Essential Security Exception: Can the WTO Resolve the GATT Article XXI Crisis and Save the Dispute Settlement Mechanism?* (Geneva Graduate Inst., Working Paper, Nov. 2023), https://repository.graduateinstitute.ch/record/301872.

The U.S.' underlying reason for the inclusion of such a provision is also clear from the language, which contains specific references to 'traffic in arms', 'war', and 'military establishment', reflecting the predominant security threat at the time: the Soviet Union. States negotiating the ITO were largely comprised of UN Member States and other allied countries that identified the Soviet Union as posing an ideological, economic, and existential threat.[21] These threats were also rooted in more traditional forms of warfare and notions of national security, as reflected in the conventional language of the text of the GATT 1947 security exception. It is clear from this language that the negotiating parties never intended to stretch the exception to cover more unconventional security challenges that have emerged in the years since, or to cover unconventional aggressors, such as non-state actors.

Despite these political issues being deeply entrenched in the original negotiating context of the GATT 1947, it is vital to note that the ITO was originally designed to share power and responsibilities with the UN. During the Havana Conference between 1947–1949, the final draft of the ITO Charter split the security exception into two parts, each meant to be regulated differently: Part I contained essentially the text of the security exception found in GATT 1947, and articulated the circumstances in which Members can suspend their normal trade obligations; Part II clarifies that the ITO cannot override the obligations of other UN Peace Treaties.[22] What this essentially did was split security interests into their economic and political components, and limit the mandate of the ITO to one that was purely economic in nature, while the UN would bear responsibility for political matters concerning peace and security.[23] However, given that the ITO ultimately failed to materialise, and the security exceptions clause of the GATT was never amended, what remains is a provision that was never intended to address the full breadth of security issues but now exists with sufficient ambiguity to give Members the potential to abuse it.

The security exception was a necessary compromise, without which the great powers may never have joined the organisation. However, scholars have warned that in an increasingly interconnected world, such an exception tends to favour more powerful nations and reinforce their superior position.[24] The nearly eighty-year-old provision

---

[21] Abe Yoshinori, *Security Exception Clauses in Post-Globalization - A Study of the GATT/WTO Regime in Historical Perspective*, 20 PUB. POL'Y REV. 4 (2024).

[22] 'For the text of the Havana Charter, *see* United Nations Conference on Trade and Employment, Final Act and Related Documents*, E/CONF.2/78,* https://treaties.un.org/doc/source/docs/E_CONF.2_78-E.pdf'.

[23] Ji Yeong Yoo & Dukgeun Ahn, *Security Exceptions in the WTO System: Bridge or Bottle-Neck for Trade and Security?*, 19 J. INT'L. ECON. L. 417, 423 (2016) [hereinafter Yoo & Ahn].

[24] Chao Wang, *Invocation of National Security Exceptions under GATT Article XXI: Jurisdiction to Review and Standard of Review*, 18 CHIN. J. INT'L. L. 695, 697 (2019); *see also* Wesley A. Cann Jr.,

is also faced with the challenge of assimilating new and unconventional national security threats, such as cybersecurity and protecting the integrity of telecommunications and other critical infrastructures. It is also tasked with navigating the increasingly blurred lines between traditional notions of security and its economic and political components.

B. *Overview of the National Security Exception in WTO Agreements*

For nearly eighty years, States have, for the most part, exercised self-restraint in invoking security exceptions in international trade, recognising the importance of the delicate balance between their right to pursue legitimate security interests and their obligation to promote trade liberalisation and reduce barriers to trade. However, this seven-decade stint of discipline has recently come to an end due to the increasing number of invocations of national security exceptions by Members at the WTO. This is not to say that Members have not made use of exceptions on national security grounds thus far, but rather that they have done so by way of Member notifications or Trade Policy Reviews, and not in such a way as to significantly restrict trade and give rise to a dispute between Member States. Members have also sought to exercise restraint in engaging in dispute settlement to avoid creating future obstacles to their use of such exceptions by subjecting them to interpretation by the Dispute Settlement Body (DSB) of the WTO. Accordingly, until recently, the security exception has not been subject to interpretation or clarification by the WTO DSBs — the Panel and Appellate Body (AB).

An exception to trade rules on the grounds of national security first arose in the GATT 1947. Once the WTO was created in 1995, this exception was incorporated into various WTO Agreements, including Article XXI of the GATT 1994, Article XIV *bis* of the General Agreement on Trade in Services (GATS), Article 73 of the Agreement on Trade Related Aspects of Intellectual Property (TRIPS), and Article III of the Agreement on Government Procurement (GPA).

Article XXI of the GATT 1994 states:

> Nothing in this Agreement shall be construed:
> (a) to require any contracting party to furnish any information the disclosure of which it considers contrary to its essential security interests; or
> (b) to prevent any contracting party from taking any action which it considers necessary for the protection of its essential security

---

Creating Standards and Accountability for the Use of the WTO Security Exception: Reducing the Role of Power-Based Relations and Establishing a New Balance Between Sovereignty and Multilateralism, 26 YALE J. INT'L. L. 414 (2001).

> interests
> (i) relating to fissionable materials or the materials from which they are derived;
> (ii) relating to the traffic in arms, ammunition and implements of war and to such traffic in other goods and materials as is carried on directly or indirectly for the purpose of supplying a military establishment;
> (iii) taken in time of war or other emergency in international relations; or
> (c) to prevent any contracting party from taking any action in pursuance of its obligations under the United Nations Charter for the maintenance of international peace and security.[25]

The language of this exception is largely mirrored in its counterpart provisions in the GATS and TRIPS in relation to services and intellectual property, respectively. The security exception can be broken down into its constituent parts as follows: section (a) permits Members to not disclose any information which "it considers" contrary to its "essential security interests"; clause (b) provides three circumstances wherein a Member state may take "any action", this can be understood as any action that restricts trade, contrary to its obligations under the WTO, which "it considers necessary" to protect its "essential security interests". These instances include measures relating to (i) "fissionable materials", (ii) "arms, ammunition … and other materials …. for the purpose of supplying a military establishment", and (iii) "taken in time of war or other emergency in international relations"; clause (c) enables States to take action in pursuance of their obligations under the UN Charter to maintain international peace and security. Article XXI, and indeed the rest of the GATT, is silent on the definition of ambiguous terms such as 'necessary', 'essential security interests', and 'other emergency in international relations'.

As discussed above, jurisprudence on this provision has been scarce, and even recent disputes have only scratched the surface by addressing only paragraphs (b)(ii) and (b)(iii). In addition to a lack of interpretation and clarification through dispute settlement, modern debates over the scope and extent of security exceptions in WTO Agreements are further complicated by new and emerging security threats that were not envisaged at the time when these carve-outs were drafted. As a result, the security exception is faced with two crucial ambiguities: firstly, the substantive scope of the exception, and secondly, questions surrounding who gets to decide the substantive scope of the exception.
The following part traces the evolution of WTO jurisprudence in attempting to address some of these ambiguities.

---

[25] GATT 1994, *supra* note 7, art. XXI.

C. *Evolution of the National Security Exception Through WTO Dispute Settlement*

As discussed above, the security exception has rarely been invoked or subject to WTO dispute settlement during its long history. This is due, in part, to the fact that, at least, during the Cold War years, trade restrictions were generally targeted towards non-Members — most notably the Soviet Nations — and accordingly there was no need for such measures to be justified under the GATT or be subject to adjudication. Following the Cold War years, this exception continued to remain dormant as Members were cautious about opening up Pandora's Box and setting precedents that might be used against them and that could potentially undermine the WTO system as a whole.[26]

The long refrain from adjudicating on the security exception came to an end in 2019 with the Panel in *Russia — Measures Concerning Traffic in Transit* handing down a decision which interpreted Article XXI for the very first time.[27] The second case, dealing with the security exception, followed shortly after with *Saudi Arabia — Measures Concerning the Protection of Intellectual Property Rights* in 2020.[28]

Before venturing into the cases themselves, it is pertinent to note that no discussion on the dispute settlement system of the WTO would be complete without reference to the current state of affairs at the DSB. Since 2019, the U.S. has been blocking appointments to the AB, effectively crippling the appellate mechanism of the WTO's dispute settlement system and resulting in panel decisions being 'appealed into the void'. This has significant implications for the dispute settlement system, as well as for the likelihood of any authoritative ruling on the national security exception. All the disputes discussed below are Panel decisions, and none have been subject to Appellate review due to this ongoing crisis.

1. Russia — Measures Concerning Traffic in Transit

This case represented the first time the security exception was comprehensively analysed and interpreted by a WTO Panel. The questions before the Panel were to determine: (1) whether the chapeau of Article XXI(b) is self-judging in nature, and (2) the scope of Article XXI(b) and XXI(b)(iii).

---

[26] Stephen Kho & Thor Petersen, *Turning the Tables: The United States, China, and the WTO National Security Exception*, CHINA BUS. REV. (Aug. 16, 2019), https://www.uschina.org/articles/turning-the-tables-the-united-states-china-and-the-wto-national-security-exception/.

[27] Panel Report, *Russia — Measures Concerning Traffic in Transit*, WTO Doc. WT/DS512/R (adopted Apr. 26, 2019) [hereinafter *Russia — Traffic in Transit*].

[28] Panel Report, *Saudi Arabia — Measures Concerning the Protection of Intellectual Property Rights*, WTO Doc. WT/DS567/8 (adopted June 16, 2020) [hereinafter *Saudi Arabia — Intellectual Property*].

The dispute arose due to Russia's imposition of restrictions on the transit of Ukrainian goods through Russian territory towards their end markets in Central Asia. These restrictions were in place amid the broader tensions between Russia and Ukraine due to a number of events, including Russia's annexation of Crimea, protest movements in Ukraine, and ongoing struggles between the two countries in the Donetsk and Luhansk regions.[29]
Ukraine claimed that such a restriction was a violation of the 'freedom of transit' through the territories of other Members, as guaranteed by Article V(2) of the GATT 1994.[30] Russia, in response, invoked the security exception under Article XXI(b)(iii), claiming that the measure was taken in time of war or other emergency in international relations and, accordingly, the panel did not have jurisdiction to review such invocation,[31] as Article XXI was self-judging.[32] The U.S. was also involved in this dispute as a third party, and put forward the argument that Article XXI was a non-justiciable matter, akin to a 'political question'.[33] In so arguing, the U.S. claimed that the text, context, object and purpose, negotiating history, and state practice all supported a wholly self-judging interpretation of Article XXI.[34]

The Panel, upon examining the text, context, object and purpose, negotiating history, and state practice concerning the security exception, rejected these arguments. The panel instead made the following findings: firstly, it found that the *chapeau* of Article XXI(b) was self-contained and does not apply to the circumstances specified in subparagraphs (i)–(iii).[35] This means that the non-justiciability afforded by the language of the *chapeau* — "which it considers" — does not extend to the subparagraphs of Article XXI(b), which would require an objective determination.[36] A subjective interpretation of these paragraphs would be contrary to the object and purpose of the GATT, as reflected in the negotiating history and *travaux préparatoiress*, which indicate that the contracting parties did not intend for the security exception to be a blanket unilateral escape clause from their WTO obligations.[37]

Once the Panel established the justiciability of the invocation of Article XXI(b), it then evaluated the substantive merits of Russia's claim, which was an objective assessment of the existence of "war or other emergency in international relations" under subparagraph (iii). The Panel began by defining "war or other emergency" as

---

[29] *Russia — Traffic in Transit*, *supra* note 28, ¶¶ 7.5–7.19.
[30] *Id.* ¶ 7.2 (referencing GATT 1994 art. V(2)).
[31] *Id.* ¶ 7.4
[32] *Id.* ¶ 7.57.
[33] *Id.* ¶ 7.103.
[34] *Id.* ¶ 7.52.
[35] *Id.* ¶ 7.82.
[36] *Id.* ¶¶ 7.69, 7.70, 7.77, 7.79.
[37] *Id.* ¶¶ 7.83-7.100.

"a situation of armed conflict, or of latent armed conflict, or of heightened tension or crisis, or of general instability engulfing or surrounding a state."[38] With regard to the *chapeau* of Article XXI(b), invoking Members were given deference to determine what they considered to be their "essential security interests", with the caveat that such determinations should be made in good faith.[39] This good faith requirement stems from Article 3.2 of the Dispute Settlement Understanding (DSU), read with Article 31(1) and 26 of the Vienna Convention on the Law of Treaties.[40] The invoking Member is further required to establish a plausible nexus between the essential security interest in question and the chosen means to address it.[41]

The panel ultimately found that a situation of 'emergency' existed in the case at hand, and given the heightened tensions and the mutual sanctions between Russia and Ukraine at the time, the Panel concluded that the measures at issue were not so "remote from or unrelated to" the protection of Russia's essential security interests arising out of such emergency.[42] Although in this case Russia did not articulate the specific "essential security interests" that warranted the measures at issue to protect, the Panel was satisfied that the mere existence of a state of armed conflict was sufficient to render Russia's security interests cognisable.[43]

The relevance/importance of this decision is two-fold: firstly, it established that the security exception is not entirely self-judging, and secondly, it clarified that although the *chapeau* of Article XXI(b) permits a subjective determination of the "essential security interests" by the invoking Member, the subsequent subparagraphs require an objective assessment by the Panel to determine whether they can be maintained. The ruling also reflects the balanced approach of the Panel in permitting States with limited discretion on sensitive political considerations, whilst maintaining the authority to review the objective elements of the exception.

2. Saudi Arabia — Measures Concerning the Protection of Intellectual Property Rights

This dispute arose from Saudi Arabia's decision, alongside some other Gulf countries, to sever all diplomatic, economic, and political ties with Qatar in June 2017 during a period of deteriorating international relations in the region.[44] Saudi Arabia

---

[38] *Id.* ¶¶ 7.76, 7.111.
[39] *Id.* ¶¶ 7.131-7.132.
[40] *Id.* ¶ 7.59.
[41] *Id.* ¶¶7.134, 7.138.
[42] *Id.* ¶ 7.145.
[43] *Id.* ¶ 7.136-1.137.
[44] Government Communications Office, *GCC Crisis*, GOV'T. COMMUNICATIONS OFFICE (STATE OF QATAR), https://www.gco.gov.qa/en/media-centre/in-focus/gcc-crisis/; Patrick Wintour, *Qatar Diplomatic Crisis - What You Need to Know*, THE GUARDIAN, (Jun. 5, 2017),

also adopted a number of measures, including blocking access within its territory to a Qatari sports broadcaster, beIN. Qatar challenged this measure under the TRIPS Agreement, while Saudi Arabia countered by invoking the security exception under Article 73 TRIPS and argued that such measures were necessary to protect its "essential security interests" in light of Qatar's alleged support of terrorist organisations.[45] The U.S. once again joined as a third party in this case, offering the same arguments that it had in *Russia — Traffic in Transit.*

Noting that the text of TRIPS Article 73(b) was identical to that of GATT Article XXI(b), the Panel in this case was guided by the Panel in *Russia — Traffic in Transit*, and applied the same analytical framework and found that the severance of all diplomatic and economic ties constituted "the ultimate State expression of the existence of an emergency in international relations",[46] and accordingly, (b)(iii) was satisfied. With regard to the assessment of whether a nexus was established between the essential security interests and the state of emergency, the panel here went a step ahead of the panel in *Russia — Traffic in Transit* and, stated that panels had limited jurisdiction to review whether or not Members had 'sufficiently' articulated their "essential security interests" and whether, measures taken in pursuance of the same were plausibly related to the war or other emergency.[47]

3. United States — Certain Measures on Steel and Aluminium

Several WTO Members, including China, Norway, Switzerland, and Turkey, challenged the legality of additional tariffs and related measures on imports of steel and aluminium on the ground that they threatened U.S. national security, and were imposed pursuant to Section 232 of the Trade Expansion Act, 1962.[48] As these measures were challenged on different grounds and were not "substantively identical

---

https://www.theguardian.com/world/2017/jun/05/qatar-diplomatic-crisis-what-you-need-to-know.

[45] *Saudi Arabia — Intellectual Property*, *supra* note 29, ¶¶ 3.3–3.4.

[46] *Id.* ¶ 7.259.

[47] *Id.* ¶¶ 7.280–7.282.

[48] Trade Expansion Act of 1962, Pub. L. No. 87–794, § 232, 76 Stat. 877 (1962); Panel Report, *United States — Certain Measures on Steel and Aluminium Products (China)*, WTO Doc. WT/DS544/R (adopted Dec. 9, 2022) [hereinafter *US — Steel and Aluminium Products (China)*]; Panel Report, *United States — Certain Measures on Steel and Aluminium Products (Norway)*, WTO Doc. WT/DS552/R (adopted Dec. 9, 2022) [hereinafter *US — Steel and Aluminium Products (Norway)*]; Panel Report, *United States — Certain Measures on Steel and Aluminium Products (Switzerland)*, WTO Doc. WT/DS556/R (adopted Dec. 9, 2022) [hereinafter *US — Steel and Aluminium Products (Switzerland)*]; Panel Report, *United States — Certain Measures on Steel and Aluminium Products (Turkey)*, WTO Doc. WT/DS564/R (adopted Dec. 9, 2022) [hereinafter *US — Steel and Aluminium Products (Turkey)*].

in all respects",[49] the DSB established several Panels to adjudicate on the issues, although they did attempt to maintain harmonised timetables and provide identical analyses on the justification of the measures under WTO security exceptions.

Following a similar approach taken by previous panels, the panel in *US — Steel and Aluminium Products (China)* acknowledged the deference accorded to a Member's judgment for "any action which it considers necessary for the protection of its essential security interests" under the chapeau, while also holding that the subparagraphs under Article XXI(b) were subject to an "objective assessment of factors".[50]

The panel found that the situation in this case had not escalated to the "gravity or severity of tensions on the international plane" to meet the requirements of Article XXI(b)(iii).[51] The panel did not, however, elaborate on the other components of Article XXI(b) or provide any clarification regarding the chapeau, the standard of review, or the standard of proof required under the preconditions of Article XXI(b). The panels were also not convinced by the U.S.' attempts to argue that the text, context, object and purpose, negotiating history, and state practice regarding Article XXI indicated that it should be "self-judging", and instead held in each case that there was insufficient evidence to conclusively demonstrate that the negotiating parties considered the security exception to be non-justiciable.[52]The panels made

[49] *US — Steel Aluminium Products (China)*, *supra* note 49, ¶ 1.21.
[50] *Id.* ¶¶ 7.114, 7.145.
[51] *Id.* ¶ 7.148.
[52] First Written Submission of the United States, *US — Steel and Aluminium Products (China)*, ¶ 82, WT/DS544 (June 12, 2019), https://ustr.gov/sites/default/files/enforcement/DS/US.Sub1.%28DS544%29.fin.%28public%29.pdf; *US — Steel and Aluminium Products (China)*, *supra* note 49, ¶ 7.128; First Written Submission of the United States, *US — Steel and Aluminium Products (Norway)*, ¶ 88, WT/DS552 (June 12, 2019), https://ustr.gov/sites/default/files/enforcement/DS/US.Sub1.%28DS552%29.fin.%28public%29.pdf; *US — Steel and Aluminium Products (Norway)*, *supra* note 49, ¶ 7.116; First Written Submission of the United States, *US — Steel and Aluminium Products (Switzerland)*, ¶ 82, WT/DS556 (June 12, 2019), https://ustr.gov/sites/default/files/enforcement/DS/US.Sub1.%28DS556%29.fin.%28public%29.pdf; *US — Steel and Aluminium Products (Switzerland)*, *supra* note 49, ¶ 7.146; First Written Submission of the United States, *US — Steel and Aluminium Products (Turkey)*, ¶ 82, WT/DS564 (June 12, 2019), https://ustr.gov/sites/default/files/enforcement/DS/US.Sub1.%28DS564%29.fin.%28public%29.pdf; *US — Steel and Aluminium Products (Turkey)*, *supra* note 49, ¶ 7.143.

identical findings in other cases regarding *US — Steel and Aluminium Products* disputes.[53]

4. United States — Origin Marking Requirement

In August 2020, the U.S. mandated that imported goods produced in Hong Kong could no longer be marked to indicate Hong Kong as their origin, but instead must be labelled as 'China' as their place of origin.[54] Citing that Hong Kong was no longer sufficiently autonomous to justify differential treatment in relation to the People's Republic of China.[55] The new US policy in determining the country of origin for duty and customs purposes would require that products originating in Hong Kong be labelled as originating in China as the actual country of origin.[56] The U.S.' argument was that such a measure was meant to prevent consumers from being misled or deceived as to the actual country of origin of the products,[57] and that this was a response to 'a threat to the essential security of the United States'.[58]

The U.S. once again raised the defence that GATT Article XXI is self-judging, and therefore a panel would only have the authority to find that the U.S. had invoked Article XXI(b) and report it as such to the Dispute Settlement Body.[59]

Following the lead of panels before it, the Panel in this case rejected the U.S.' argument and held that Article XXI(b) is not a wholly self-judging provision; rather, the applicability of the exceptions in the subparagraphs are subject to panel review,[60] unlike the freedom for unilateral determination that is granted to the invoking Member in deciding the actions "which it considers necessary" under the *chapeau* of the provision.

---

53 *US — Certain Measures on Steel and Aluminium Products (Norway)*, *supra* note 49, ¶ 7.136; *US — Certain Measures on Steel and Aluminium Products (Switzerland)*, *supra* note 49, ¶ 7.166; *US – Certain Measures on Steel and Aluminium Products (Turkey)*, *supra* note 49, ¶ 7.163.

54 Panel Report, *United States — Origin Marking Requirement*, ¶ 2.1, WTO Doc. WT/DS597/R (Dec. 21, 2022) [hereinafter *US — Origin Marking (Hong Kong, China)*].

55 *Id.* ¶¶ 7.327–7.331.

56 First Written Submission of Hong Kong, China, *US — Origin Marking (Hong Kong, China)*, ¶ 16, WT/DS597 (May 28, 2021), https://www.tid.gov.hk/en/our_work/trade_relations/americas/us/files/first_written_submission.pdf.

57 *US — Origin Marking (Hong Kong, China)*, *supra* note 55, ¶ 7.222.

58 First Written Submission of the United States of America, *US — Origin Marking (Hong Kong, China)*, ¶ 2, WT/DS597 (July 2, 2021), https://ustr.gov/sites/default/files/enforcement/DS/DS597/US.Sub1.fin.pdf.

59 *US — Origin Marking (Hong Kong, China)*, *supra* note 55, ¶¶ 7.17–7.18.

60 *Id.* ¶7.17–7.18.

The Panel, in determining whether the requirements under Article XXI(b)(iii) were met, took a narrower view of "emergency in international relations" than previous panels, and highlighted that such emergency would have to constitute "a state of affairs, of the utmost gravity, which represents a breakdown or near-breakdown in the relations between states or other participants in international relations."[61] Though the panel acknowledged that there was a situation in Hong Kong/China that affected the international relations between Hong Kong/China and other WTO Members, including the U.S., this did not rise to the level of an "emergency in international relations" within the meaning of Article XXI(b)(iii) GATT.[62] Like panels before it, this panel therefore did not proceed to assess/evaluate the U.S. measures under the remaining elements of Article XXI(b).

Interestingly, in response to the U.S.' claim that the application of the National Security Law to Hong Kong violated Hong Kong's democracy and human rights and that this, in turn, was a threat to U.S. security, the panel did not deny the possibility that protecting values such as human rights and democracy could be of essential security interest.[63] While this leaves the door ajar for future invocations of the security exception on grounds of protecting human rights and democracy, the panel seems to set a high bar for such invocation.

5. Key Takeaways

The key takeaways from these disputes, particularly for the purposes of this article, are as follows: firstly, all the cases resolved a long-standing interpretive question regarding the provision by making it definitively clear that invocations of national security exceptions under WTO covered Agreements are justiciable and not entirely self-judging in nature. Secondly, the panels have also clarified that although the *chapeau* of Article XXI(b) defers to the subjective determination by States as to what constitutes "essential security interests", the requirements under subparagraphs (i)-(iii) are subject to objective review and analysis by panels. Thirdly, although the panels required that invoking Members articulate sufficient nexus between the trade restrictive measure and the essential security interest that is pursued via such measure, this standard need only meet a "minimum requirement of plausibility".[64] Furthermore, the panels have found that in order to meet the requirements of Article XXI(b)(iii), a situation of emergency in international relations must constitute a state of affairs of the "utmost gravity, which represents a breakdown or near-breakdown in the relations between states or other participants in international

[61] *Id.* ¶ 7.315.
[62] *Id.* ¶ 7.358.
[63] *Id.* ¶¶ 7.17–7.18.
[64] *Saudi Arabia — Intellectual Property*, *supra* note 29, ¶ 7.288 (quoting *Russia — Traffic in Transit*, *supra* note 28, ¶ 7.138).

relations".[65] This represents a high bar to clear, particularly in the context of emerging threats to national security that do not mimic traditional breakdowns of inter-state relationships.

6. TECHNOLOGY RESTRICTIONS VIA SECURITY CLAIMS: AN ASSESSMENT OF POTENTIAL VIOLATIONS UNDER OTHER WTO AGREEMENTS/THE TBT AGREEMENT

This paper has so far dealt with the security exceptions found in the GATT, GATS, and TRIPS Agreements. However, it would be incorrect to say that these are the only instances where national security can be used as a justification to adopt trade-restrictive measures. The Agreement on Technical Barriers to Trade (TBT) applies if Members implement mandatory technical regulations that deviate from internationally recognised standards and impose additional burdens on goods from another Member as compared to 'like' products from other Member states or 'like' domestic products.[66]

Cybersecurity measures, which will be discussed in more detail in the part below, generally tend to constitute technical regulations or standards and would accordingly be governed by the TBT Agreement. According to the TBT Agreement, technical regulations "lay down product characteristics or their related process and production methods, including applicable administrative procedures with which compliance in mandatory".[67] However, unlike the GATT and other WTO Covered Agreements, the TBT Agreement does not contain a concurrent security exception clause. Instead, any reference to national security must be addressed within the confines of Article 2.1. In contrast to an explicit security exception carve-out in the GATT, the TBT Agreement instead recognises national security as a 'legitimate objective' of a TBT measure, and lays down the procedures that a Member must follow when adopting a trade restrictive measure on the grounds of national security.[68] Notably, the provision lacks the deferential language found in GATT Article XXI (a) and (b) "which it considers necessary", thus ensuring a balance between Members' freedom to determine their "national security requirements" and limiting such measures to be no more restrictive than necessary. Although this creates an alternative structural framework for members invoking national security, the TBT Agreement does have some similarities to the GATT security exception framework, in that the language

[65] *US — Origin Marking (Hong Kong, China), supra* note 55, ¶ 7.135.
[66] Agreement on Technical Barriers to Trade art. 2.1, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1A, 1868 U.N.T.S. 120 [hereinafter TBT Agreement].
[67] *Id.* annex 1.1.
[68] *Id.* arts. 2.2, 2.9, and 5.6.

of the Preamble defers to Members' "essential security interest"[69] and also maintains the GATT-like non-disclosure clause wherein 'nothing in this Agreement' required any Member 'to furnish any information which they consider contrary to their essential security interests'.[70] In spite of these similarities, however, given that security occupies a different position in the TBT Agreement as compared to other Agreements in the form of a legitimate objective rather than an exception, it would be interesting to see whether Panels attempt to read in "good faith" and "plausible nexus" standards by analogy when interpreting the text of the TBT Agreement.

The TBT Agreement normally requires interested parties to become acquainted with it,[71] and producers in exporting Member states have time to adapt their products or methods of production to meet the requirements of such technical regulation.[72] If the technical regulation is not in accordance with international standards and may have a "significant effect on trade of other Members",[73] then such Member is required to notify the Secretariat "at an early appropriate stage",[74] of the products to be covered by the technical regulation, and provide a brief indication of its objective and rationale.[75] Other Members are also to be permitted "reasonable time", and "without discrimination", to make comments in writing and discuss the same, the results of which should be "taken into account".[76]

This *ex-ante* notification obligation may be suspended in situations of "urgent problems", including those of "national security";[77] Members are instead required to notify the Secretariat "immediately" (i.e., following the adoption of the measure) of the particular technical regulation and products covered, a brief indication of the objective and rationale of the technical regulation, including the nature of the urgent problems,[78] and also permit Members, without discrimination, to present and discuss their comments, the results of which are to be taken into account.[79]

Members are also afforded the same protection against disclosure of sensitive information as in the GATT, wherein 'nothing in this Agreement' requires any Member to furnish "any information which they consider contrary to their essential

---

[69] *Id.* at 7.
[70] *Id.* art. 10.8.3.
[71] *Id.* art. 2.11; *see also* art. 5.8 (in the context of conformity assessment procedures).
[72] *Id.* art. 2.12; *see also* art. 5.9 (in the context of conformity assessment procedures).
[73] *Id.* art. 2.9; *see also* art. 5.6 (in the context of conformity assessment procedures).
[74] *Id.* art. 2.9.1; *see also* art. 5.6.1 (in the context of conformity assessment procedures).
[75] *Id.* art. 2.9.2; *see also* art. 5.6.2 (in the context of conformity assessment procedures).
[76] *Id.* art. 2.9.4; *see also* art. 5.6.4 (in the context of conformity assessment procedures).
[77] *Id.* art. 2.10; *see also* art. 5.7 (in the context of conformity assessment procedures).
[78] *Id.* art. 2.10.1; *see also* art. 5.7.1 (in the context of conformity assessment procedures).
[79] *Id.* art. 2.10.3; *see also* art. 5.7.3 (in the context of conformity assessment procedures).

security interests".[80] The Preamble to the Agreement further defers to Members' views by recognising that no country should be prevented from taking measures necessary for the protection of its "essential security interest".[81]

This flexibility accorded to Members is reflected in the number of notifications made to the WTO regarding TBT measures on the grounds of national security, which as of March 2026 stands at 672.[82] Although most of these notifications do not concern digital trade, a number of them cover regulations relating to ICT, particularly in recent years.

In the context of cybersecurity measures, although some of them may not be notified on national security grounds, they may nonetheless be adopted in the interests of the security of domestic critical infrastructure. In this case, they would need to meet the requirements under Article 2 of the TBT. Article 2.1 requires that Members shall be accorded treatment "no less favourable" than that accorded to "like products of national origin" and to "like products originating in any other country". Article 2.2 requires that regulations are not more trade restrictive than necessary to fulfil a legitimate regulatory objective. Finally, Article 2.4 is also relevant for our analysis, as it requires Members to use international standards, where they exist, as a basis for their technical regulations, unless such international standards would be an ineffective or inappropriate means for the fulfilment of the legitimate objectives pursued.

A. *Likeness*

The first requirement is to establish that the two products targeted by the technical regulation are "like". WTO jurisprudence has focused on the existence of a competitive relationship between the products to determine likeness,[83] and has also stated that a Panel should "discount any distortive effects that the measure at issue may itself have on the competitive relationship".[84] The AB has also rejected an approach based on the regulatory objectives of a technical regulation.[85] This is particularly pertinent in the context of cybersecurity measures that may seek to treat

---

[80] *Id.* art. 10.8.3.
[81] *Id.* recital 7.
[82] Please see search results in *Search notifications*, EPING SPS AND TBT PLATFORM, https://eping.wto.org/en/Search/Index?objectiveIds=6&distributionDateFrom=1995-01-01&distributionDateTo=2026-03-25.
[83] Appellate Body Report, *United States — Measures Affecting the Production and Sale of Clove Cigarettes*, WTO Doc. WT/DS406/AB/R, ¶ 112 (adopted Apr. 24, 2012) [hereinafter *US — Clove Cigarettes*].
[84] *Id.* ¶111.
[85] *Id.* ¶¶1071–20.

products as not "like" based on national security grounds, such as concerns surrounding origin, technology, or production methods.

The AB has also not objected to reliance on the likeness criteria developed in the jurisprudence under Article III of the GATT 1994, which includes a consideration of the product's physical characteristics, and consumer tastes and preferences.[86]

B. *No less favourable treatment*

Once likeness has been established, the assessment then turns to a two-step analysis of whether the measure accords "treatment no less favourable" to imported products: the first step is to determine whether the technical regulation modified the conditions of competition to the detriment of imported products *vis-à-vis* like products of domestic origin and/or like products originating from any other country; and the second step requires a determination of whether such detrimental impact "stems exclusively from a legitimate regulatory distinction".[87] According to the AB, there is no less favourable treatment where the detrimental impact stems directly from a legitimate regulatory distinction.[88] A challenge in applying this in the cybersecurity regulation context is that such measures are often risk-based, and the panel will need to make an assessment of whether the regulation appropriately calibrates the discriminatory aspects of the measure with the cybersecurity risk at hand.[89] Furthermore, as greater risk entails greater deference to the invoking Member regarding how they choose to address the risk, this may pose additional challenges in making objective determinations.

C. *No more trade restrictive than necessary*

The AB in *Brazil — Retreaded Tyres* clarified that "necessary" means that there is no less trade restrictive alternative means for achieving the government's regulatory

---

[86] *Id.* ¶¶ 107, 112, and 121–160.

[87] Appellate Body Report, *United States — Measures Concerning the Importation, Marketing and Sale of Tuna and Tuna Products*, ¶ 215, WTO Doc. WT/DS381/AB/R (adopted June 13, 2012) [hereinafter *US — Tuna II (Mexico)*]; Appellate Body Report, *United States — Certain Country of Origin Labelling (COOL) Requirements*, ¶ 271 , WTO Doc. WT/DS384/AB/R (adopted July 23, 2012) [hereinafter *US — COOL*]; Appellate Body Report, *US — Tuna II (Mexico) (Article 21.5 — Mexico)*, ¶ 7.26, WTO Doc. WT/DS381/RW2 (adopted Dec. 14, 2018); *see also* Panel Report, *US — Tuna II (Mexico) (Article 21.5)*, ¶ 7.73, WTO Doc. WT/DS381/RW (adopted Dec. 3, 2015); Panel Report, *US — COOL (Article 21.5 — Canada and Mexico)*, ¶ 7.60–7.62, WTO Doc. WT/DS384/RW (adopted May 29, 2015).

[88] *US — Tuna II (Mexico,) supra* note 87, ¶¶ 174, 175; Appellate Body Report, *Dominican Republic — Measures Affecting the Importation and Internal Sale of Cigarettes,* ¶ 96, WTO Doc. WT/DS302/AB/R (adopted May 19, 2005).

[89] Meltzer, *supra* note 9, at 19.

goal.[90] This would be particularly challenging for Members to prove due to the high evidentiary demands, classified information surrounding cybersecurity measures, and the fact that these regulations may often be part of a broader cybersecurity policy.

D. *International standards*

Through Article 2.4, the TBT Agreement seeks to promote the adoption of international standards in the interests of harmonisation and trade liberalisation.[91] The AB in *US — Tuna II (Mexico)* found that in order to constitute an 'international standard' for the purposes of the TBT Agreement, a standard has to be adopted by an 'international standardizing body'.[92] The AB further explained that an international standardising body is one that has 'recognised activities in standardisation and whose membership is open to the relevant bodies of at least all Members'.[93] This poses a significant challenge due to a number of reasons. Firstly, there are a large number of different cybersecurity standards worldwide, and no uniform or harmonized approach to cybersecurity, including best practices, to guide the creation of these standards. Secondly, although there are arguably *some* standards that could be considered to be a "relevant international standard", such as the ISO standards, for example, Members are not obliged to adopt such standards if they are an "ineffective or inappropriate means for the fulfilment of the legitimate objectives pursued".[94] Any complaining Member would struggle to prove that the ISO standard, for example, would be both effective and appropriate to meet the national security goal of the party, imposing alternative standards given the sensitive nature of cybersecurity and national security policies and lack of publicly available information to make a strong evidence-based claim.

This part has highlighted an alternative context in which WTO Members may invoke national security as a ground to deviate from their WTO obligations. The positioning of national security as a legitimate objective rather than an exception provision could be an important distinction in how future Panels adjudicate on cases involving a TBT measure justified on national security grounds, potentially creating two separate structural frameworks for assessing national security measures, with different standards of review. This may in turn affect how States choose to adopt and frame measures taken in pursuance of their security interests. This is not to say that such

---

[90] Appellate Body Report, *Brazil — Measures Affecting Imports of Retreaded Tyres*, WTO Doc. WT/DS332/AB/R, ¶ 210 (adopted Dec. 17, 2007).

[91] Shin-yi Peng, *Cybersecurity and Trade Governance*, *in* THE ELGAR COMPANION TO THE WORLD TRADE ORGANIZATION 35, 40–41 (Julien Chaisse & Cristián Rodríguez-Chiffelle eds., 2023).

[92] Appellate Body Report, *US — Tuna II (Mexico)*, *supra* note 87, ¶¶ 354–356.

[93] *Id.* ¶¶ 357–359.

[94] Peng, *supra* note 91, at 40–41.

measures would be easier to justify or maintain under the TBT framework, as there are likely to be obstacles for both the invoking Member and the Members contesting such measures. In practice, although likeness of the products may arguably be established through tariff classification, physical characteristics, and similar end uses, consumer preferences might be a strong sticking point on which to argue that products with different security risks are not like, particularly in the context of technology and cybersecurity. Secondly, as cybersecurity measures are often risk-based, Panels are likely to afford more deference to the invoking Member to determine how to address such risks where the risks are higher. Furthermore, given the relatively nascent nature of the field of cybersecurity, there are little to no uniform international standards that have been established to guide State practice in adopting cybersecurity measures. This permits States to develop their own unique standards to meet their security requirements. Complaining States may provide alternative measures, but these must by WTO-consistent whilst affording an equivalent level of contribution to achieve the objective pursued by the challenged measure. This is no easy feat due to the fact that such cybersecurity measures often form part of larger national security policies that contain classified information, which a Member is not required to share. Rapidly evolving security risks and slower regulatory advancements also compound the difficulties in offering viable alternative measures that are less trade restrictive. Thus, although the TBT Agreement provides an important framework for pursuing national security objectives at the nexus of international trade and technology, the doctrinal indeterminacy surrounding these provisions becomes significant when attempting to balance these competing interests in practice.

7. THE EVOLVING NATIONAL SECURITY CHALLENGE: IS THE WTO FIT FOR PURPOSE?

A. *New Century, New Security*

From an international trade law perspective, the security threats and vulnerabilities that exist in the 21st century are fundamentally different from those that informed the creation of the security exception in the GATT 1947. Unlike the conflicts that were familiar to the drafters, which were largely confined to traditional military conflict between States through the use of conventional weapons — extended to include nuclear weapons and fissionable materials — modern security issues involve non-state actors, are often difficult to attribute, and can be carried out at relatively low cost to target non-military targets. The rules of the security exception were framed too narrowly to address cybersecurity concerns, and the true limits of the exception are now coming to light. A comprehensive study of the new national security challenges to the economic order has been carried out by J. Benton Heath, which provides an overview of the different challenges faced by States today.[95] This includes cybersecurity threats, pandemics, climate change, and terrorism, to name a few. For the purposes of this article, the focus will remain on cybersecurity threats and associated threats to digital trade.

Cybersecurity has become one of the most often cited rationales behind trade and investment protectionist measures, such as information and communications technology (ICT) product standards, data location and protection requirements, and investment screening.[96] Although there is no one singular internationally recognised definition of 'cybersecurity', the International Telecommunications Union (ITU) broadly defines it as a "collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and users' assets."[97] The National Institute of Standards and Technology (NIST) provides a slightly more focused definition: "the prevention of damage to, unauthorised use of, exploitation of, and, if needed, the restoration of electronic information and communications systems, and the information they contain, in order to strengthen the confidentiality, integrity and availability of these systems."[98] Cybersecurity measures are thus primarily in place to protect the integrity of information and information systems, as well as the critical infrastructure of States. Critical infrastructure can be understood to be the physical and cyber systems and assets that are so vital that their incapacity or destruction would have a debilitating impact on physical and economic security or public health.[99] Threats to critical infrastructure could be in the form of a direct attack that damages critical infrastructure, such as power plants, water distribution systems, and electricity grids, or it could be in the form of disruption to the supply chains of critical industries, which in turn threaten the integrity of a State's critical infrastructure.[100]

Other forms of cyberattacks could be through cyber espionage or spying to hack into commercial enterprises for a variety of purposes, ranging from stealing trade

---

[95] Heath, *supra* note 6.

[96] Peng, *supra* note 91, at 35–36.

[97] *Definition of Cybersecurity*, INT'L. TELECOMM. UNION, https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx#:~:text=Cybersecurity%20is%20the%20collection%20of,and%20organization%20and%20user's%20assets.

[98] Computer Security Resource Centre*, Glossary term Cybersecurity*, NAT'L INST. STANDARDS & TECH., https://csrc.nist.gov/glossary/term/cybersecurity.

[99] TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 564 (Michael N. Schmitt ed., 2017); *Critical Infrastructure Security and Resilience*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience.

[100] Shin-yi Peng, *Digital Economy and National Security: Contextualizing Cybersecurity-Related Exceptions*, 117 AJIL UNBOUND 122, 122–123 (2023).

secrets and intellectual property to the collection of sensitive personal information and other personal data. These have been cited as pertinent threats to national security by numerous countries, including the U.S. and China. For instance, the U.S.'s earlier proposed ban on the social media application TikTok was based on claims that China was using artificial intelligence (AI) for censorship and surveillance.[101]

Some examples of recent trade-restrictive measures adopted by States on grounds of national security include: Australia's prohibition on its telecommunications carriers to purchase 5G equipment or services from the Chinese firm Huawei due to risks of espionage and sabotage brought on by foreign involvement in national 5G networks;[102] The U.S.' 5G Clean Network Program that prevents Huawei from pre-installing untrusted applications,[103] and also requires American telecommunications companies to remove Huawei equipment, such as cell towers, and services, such as cloud services, from their networks;[104] the EU's recent policies, including the 5G Toolbox of Risk Mitigation Measures, which delineates potential risk areas and remedial measures connected with suppliers of 5G infrastructure and aims to diversify its supply chain so as to reduce reliance on Chinese companies' (particularly Huawei) participation in the 5G rollout;[105] The U.S.' ban on the U.S. Department of Defence using software platforms developed by Kaspersky Lab is based on reports that the Russian company may have been vulnerable to Russian government influence.[106] China's Great Firewall is an internet filtering system used by the Chinese government to block access to content hosted in other countries,

---

[101] Robert D. Williams, *Beyond Huawei and TikTok: Untangling U.S. Concerns over Chinese Tech Companies and Digital Security* (Penn Project on the Future of U.S.-China Relations, Working Paper, 2020), https://www.brookings.edu/wp-content/uploads/2020/10/FP_20201030_huawei_tiktok_williams.pdf; Kelly K. Shang & Rachel R. Du, *Disciplining Artificial Intelligence Policies: World Trade Organization Law as a Sword and a Shield*, *in* ARTIFICIAL INTELLIGENCE AND INTERNATIONAL ECONOMIC LAW 274, 277 (Shin-yi Peng, Ching-Fu Lin, & Thomas Streinz eds., 2021).

[102] *Huawei and ZTE handed 5G Network ban in Australia,* BBC(Aug. 23, 2018), https://www.bbc.com/news/technology-45281495; *Australia, Huawei and 5G*, ISSS, (Oct. 2019), https://www.iiss.org/publications/strategic-comments/2019/australia-huawei-and-5g/.

[103] *The Clean Network,* U.S. DEP'T. STATE, https://2017-2021.state.gov/the-clean-network/index.html.

[104] David Shepardson, *U.S. FCC Set to Ban Approvals of New Huawei, ZTE Equipment*, REUTERS, (Oct. 13, 2022), https://www.reuters.com/technology/us-fcc-set-ban-all-us-sales-huawei-zte-equipment-axios-2022-10-13/.

[105] *Cybersecurity of 5G Networks – EU Toolbox of Risk Mitigating Measures*, EUR. COMM'N (Jan. 23, 2020), https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

[106] Press release, Bureau Indus. & Sec (U.S. Dep't. Com.), Commerce Department Prohibits Russian Kaspersky Software for U.S. Customers (June 20, 2024), https://www.bis.gov/press-release/commerce-department-prohibits-russian-kaspersky-software-u.s.-customers.

which it deems harmful to the nation,[107] and India's ban on Chinese telecom equipment on grounds of national security.[108]

In response to these emerging threats, most States have adopted comprehensive cybersecurity measures, often as part of a larger national cybersecurity strategy.[109] Some of these measures include data localisation requirements, import and investment restrictions on data and ICT products, particularly from countries, or countries along supply chains, where cyber risks are high, and also high tariffs on goods from such countries.[110] As discussed above, States have also begun to take unilateral measures to address some of these concerns.

Such cybersecurity-based trade restrictions have the potential to clash with international trade rules. As discussed in earlier parts, and given that national security objectives are central to these trade-restrictive measures, the question now concerns how these established principles can be applied to modern security issues. Do the provisions enumerated in earlier parts afford Members sufficient flexibility to make use of the exceptions to address modern threats?

B. *Is the WTO Security Exception Fit for Purpose?*

Applying the jurisprudence from the disputes before the WTO panels, it is clear that there are certain issues that need to be overcome when attempting to apply the security exception from the GATT and other WTO Agreements to cybersecurity measures.

The first hurdle to be overcome is to establish a plausible link between a State's "essential security interests" and the measure adopted. Given the dynamic nature of both technologies used in critical infrastructures as well as the techniques of cyberattacks, it may be difficult for States to be certain of the entire extent of vulnerabilities of their digital systems and accordingly craft a satisfactory link between the measure and the essential security interest. Panels may also not be in a position to determine if the threat is grave enough to justify the measure adopted by the State.

---

[107] Jyh-An Lee, *Great Firewall*, 406 SSRN 408, (2018), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=3192725.

[108] Aarti Ramachandran, *India Restricts Chinese Telecom Firms Citing Security Concerns*, FOREIGN POL'Y. ASS'N., https://fpa.org/india-restricts-chinese-telecom-firms-citing-security-concerns/.

[109] *National Cybersecurity Strategies Repository*, INT'L. TELECOMM. UNION, https://www.itu.int/en/ITU-D/Cybersecurity/pages/national-strategies-repository.aspx.

[110] Meltzer, *supra* note 9 at 2.

Secondly, and with regard to the subparagraphs (i)–(iii) of Article XXI(b), which exhaustively enumerate the circumstances in which a State may take the action which "it considers necessary" for the protection of its "essential security interests".[111] States may be able to justify the measure under subparagraphs (i) and (ii) by attempting to argue that, given the digitisation of their militaries as well as their nuclear facilities, they would be vulnerable to cyberattacks and, accordingly, trade-restrictive measures may be necessary in light of these contemporary security concerns.[112] However, given that cyberattacks have numerous other non-military targets, particularly targets such as critical state infrastructures, or even private companies to access sensitive personal data, trade secrets, or other intellectual property, these provisions may not be very useful in most cases. A better-suited option, therefore, would be to try to justify the measure under subparagraph (iii).

The "emergency in international relations" within the meaning of GATT XXI(b)(iii) requires that the situation must be "at least comparable it its gravity or severity to a war" in terms of its impact on international relations.[113] This may prove difficult to establish as cybersecurity risks are comparatively more routine and ubiquitous, and can occur even without an outright escalation in international relations more generally. Moreover, given that there is no clearly delineated 'beginning' or 'end' in the context of cybersecurity threats, the temporal link that requires the measure to be "taken in time of" the "emergency in international relations" will be problematic to establish when addressing a long-lasting cybersecurity matter,[114] which as Heath argues, is of a permanent nature and must be systematically addressed over time.[115] Furthermore, is it unclear whether cyberattacks on government websites, banks, or private actors, could constitute an 'armed attack' in international law, adding to the difficulty for a panel to make an objective determination on the existence of an "emergency in international relations".[116] Similarly, it is also uncertain whether commercial and economic threats, such as theft of data or intellectual property, though capable of significant detrimental impact, would reach the threshold of "war or emergency in international relations".

Should a dispute in this regard ever be brought before a Panel, it is sure to bring about interesting legal analysis on the application of a nearly eight-decade-old provision to contemporary threats. However, any analysis is bound to stretch the

---

[111] *See, e.g., US — Steel and Aluminium Products (China)*, *supra* note 49, ¶¶ 6.14-6.16 and 7.113-7.114.

[112] Kartikeya Garg, *The National Security Exception in International Trade and Cybersecurity*, COMMONWEALTH CYBER J. 117, (2025).

[113] *US — Steel and Aluminium Products (China)*, *supra* note 49, ¶ 7.139.

[114] *Id.* ¶¶ 7.112, 7.139-7.149.

[115] Heath, *supra* note 6.

[116] Neha Mishra, *The Trade: (Cyber)Security Dilemma and Its Impact on Global Cybersecurity Governance*, 54 J. WORLD TRADE 567, 14 (2020).

limits of the law as well as of the intent of the drafters, which was explicitly to limit the scope of the exception and not permit 'everything under the sun'. In light of this reality, states have decided to take matters into their own hands and enter into other agreements with each other that contain updated provisions on national security in order to better address contemporary threats.

C. *Emerging Trends in PTAs, RTAs, And FTAs*

As the previous parts have highlighted, the security exceptions in WTO Covered Agreements are quite narrowly framed and have also been interpreted in a way so as to limit their scope to the original context of their drafting during the post-war years. Accordingly, they may not be best suited to address new and emerging security threats, such as cybersecurity. In an attempt to counter this, modern trade agreements, in the form of Preferential Trade Agreements (PTAs), Regional Trade Agreements (RTAs), or bilateral Free Trade Agreements (FTAs), have begun to adopt more expansive and innovative security exceptions to take into account these emerging threats in the context of digital trade and cybersecurity, and restore the trade-national security balance that was originally envisaged under the original security exceptions provisions. Countries have approached this issue in two ways: firstly, some agreements have amended the scope of the security exception to account for evolving threats to national security. Secondly, states have also increasingly begun to adopt sector-specific provisions on cybersecurity to address these threats.

With regard to the first category, the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) contains a very broad security exception that draws from GATT language to a certain extent, but does not include a closed list of circumstances in which such exceptions could be triggered.[117] This gives Parties broad discretion to determine when and how they implement such a security exception, and appears to be self-judging in nature. This language is mirrored in other agreements as well, such as the U.S.–Mexico–Canada Agreement (USMCA),[118] and the Digital Economy Partnership Agreement (DEPA) between New Zealand, Chile, and Singapore.[119]

---

[117] Comprehensive and Progressive Agreement for Trans-Pacific Partnership art. 29.2, Mar. 8, 2018, U.N.T.S 3337 [hereinafter CPTPP].

[118] United States–Mexico–Canada Agreement art.32.2, Nov. 30, 2018, 58 I.L.M 1292 [hereinafter USMCA].

[119] Digital Economy Partnership Agreement art. 15.2, June 12, 2020, [2020] N.Z.T.S. 2 [hereinafter DEPA].

Other examples of agreements that alter the scope of the original security exception are the Canada–Israel FTA,[120] and the Carribean Community (CARICOM)–Costa Rica FTA,[121] both of which omit the term "it" in the *chapeau*, "it considers necessary" to remove any doubt regarding the self-judging nature of the provision. Similarly, the CARICOM–Dominican FTA also mandates a necessity test as a precondition that any measure must first overcome.[122] The EU–Canada Comprehensive Economic and Trade Agreement also broadens the scope of the exception by permitting measures to be taken in relation to the maintenance of international peace and security, including the protection of human rights.[123]

The Regional Comprehensive Economic Partnership (RCEP), having taken into account the vital importance of critical infrastructure to national security, has also expanded the scope of its security exception to include measures taken so as to protect critical infrastructure, whether privately or publicly owned, including communications, power, and water infrastructures.[124]

The second category consists of PTAs that contain specific clauses addressing cybersecurity. Couched in soft, aspirational language, such as "shall endeavour" and "recognise", this set of provisions focuses largely on voluntary international cooperation frameworks for cybersecurity and governance and cyber-capacity building. Additionally, these agreements also contain sector-specific clauses. For instance, the RCEP contains a provision on data localisation that allows the parties to take any data localisation measure they consider necessary for the protection of essential security interests.[125] The self-judging element has been further reinforced by a subparagraph stating that such measures shall not be disputed by other parties,[126] effectively opening the doors for parties to restrict data flows to achieve a range of regulatory objectives. Similar provisions on data localisation and restrictions on cross-border data flows can also be found in the CPTPP[127] and the EU–Singapore Digital Trade Agreement.[128]

---

120 Free Trade Agreement, Can.–Isr., art. 10.2, July 31, 1996, 3122 U.N.T.S. 99.
121 The Caribbean Community (CARICOM)–Cost Rica Free Trade Agreement art. XVI.02, Mar. 9, 2004, https://edit.wti.org/document/show/97bfbf30-3d45-4ae9-b1d5-b5ead4fb79f1.
122 CARICOM — Dominican Republic Free Trade Agreement art. VII, Aug. 22, 1998, https://edit.wti.org/document/show/0455cc20-3745-46cd-a8af-48b04fc063b0.
123 Comprehensive Economic and Trade Agreement, Can.–EU, art. 28.6, Oct. 30, 2016, 2017 O.J. (L 11) 23.
124 Regional Comprehensive Economic Partnership art. 17.13(b)(iii), Nov. 15, 2020, [2022] A.T.S. 1 [hereinafter RCEP].
125 *Id.* art. 12.14.(3)(b).
126 *Id.*
127 CPTPP, *supra* note 119, art. 14.13.
128 Digital Trade Agreement, EU–Sing. art. 5, n. 1, May 7, 2025, 2026 O.J. (L 126) 1.

These trends indicate that recent trade agreements are taking on open-ended and digital sector-specific security exceptions to address the policy needs of the digital economy. Whilst this addresses some of the gaps left by the inadequacy of the traditional WTO framework, these types of security exceptions risk being over-broad and may potentially tip the balance between trade and national security towards the latter and open the doors for protectionist measures, particularly if they cannot be subject to review.

V. IMPLICATIONS ON DEVELOPMENT AND INNOVATION

Trade is considered to be essential in the international transfer of technology, which in turn lends to the development of economies. Through trade with technologically advanced nations, developing countries can gain access to more open channels of communication about production methods, product design, and technological know-how. Additionally, such technology transfer enables developing countries to adapt foreign technologies for their use, often at lower costs than what innovation from scratch would require.[129] Digital trade also has the effect of making global markets more inclusive by allowing more countries and smaller players to participate in international trade.[130]

It is also important to remember that development occupies a central position in the normative architecture of the WTO, reflecting its close and reciprocal relationship with international trade. The Preamble to the Marrakesh Agreement Establishing the World Trade Organization explicitly situates trade liberalisation within the broader objective of sustainable development, thus accounting for both the diversity of Members' economies and the need for 'positive efforts' to ensure that developing countries and least developed countries (LDCs) secure a share in global trade commensurate with their developmental needs. The language of the Preamble also underscores that development is not merely an ancillary concern of international trade, but a foundational principle of the rules-based multilateral trading system that shapes its objectives, informs its legal framework, and offers a basis for differential treatment for its developed and least-developed Members. In this way, international trade can be conceived not as an end in and of itself, but rather a means through

---

[129] Dalia Hakura & Florence Jaumotte, *The Role of Inter- and Intraindustry Trade in Technology Diffusion* 3 (Int'l Monetary Fund, Working Paper No. 99/58, 1999), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=880585.

[130] James Manykia, et. al., *Digital Globalization: The New Era of Global Flows*, MCKINSEY GLOBAL INSTITUTE 76-77 (2016), https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/digital%20globalization%20the%20new%20era%20of%20global%20flows/mgi-digital-globalization-full-report.pdf.

which developmental goals can be realised and gains from the same can be more equitably distributed among WTO Members.

It is also important to highlight here that development occupies a central position in the normative architecture of the WTO, reflecting its close and reciprocal relationship with international trade. The Preamble to the Marrakesh Agreement Establishing the World Trade Organization explicitly situates trade liberalisation within the broader objective of sustainable development, thus accounting for both the diversity of Members' economies and the need for 'positive efforts' to ensure that developing countries and LDCs secure a share in global trade commensurate with their developmental needs. The language of the Preamble also underscores that development is not merely an ancillary concern of international trade, but a foundational principle of the rules-based multilateral trading system that shapes its objectives, informs its legal framework, and offers a basis for differential treatment for its developed and least-developed Members. In this way, international trade can be conceived not as an end in and of itself, but rather a means through which developmental goals can be realised and gains from the same can be more equitably distributed among WTO Members. Despite this central positioning in the WTO framework, security exceptions in WTO Agreements, which lack explicit development-sensitive carve-outs or impact assessment requirements, risk undermining the development mandate of the WTO. This tension is further exacerbated in the context of technology-related trade measures, such as export controls, investment screening measures, and restrictions on access to critical technologies, which may impede technological advancements and participation in global supply chains for developing economies. This reveals a structural contradiction within the WTO framework itself: whilst development is recognised as a foundational objective of the post-war multilateral trading system, the legal architecture of its security exceptions contains no mechanisms or carve-outs to protect, or even account for, developmental interests. This risks undermining the WTO's mandate and transforming development from a constitutive principle to one that can be displaced *carte blanche* to further geopolitical security interests.

International trade is also essential in achieving Sustainable Development Goals (SDGs), especially in reducing poverty (SDG 1), promoting gender equality (SDG 5), decent work and economic growth (SDG 8), as well as reducing inequalities within and among countries (SDG 10).[131] This is also supported by the Organisation

[131] G.A. Res. 70/1, Transforming Our World: the 2030 Agenda for Sustainable Development, U.N. Doc. A/RES/70/1 (Sept. 25, 2015); *The 17 Goals*, UNITED NATIONS, https://sdgs.un.org/goals#; *see also* Mira Burri & Kholofelo Kugler, *Digitization, Regulatory Barriers and Sustainable Development* (University of Lucerne, Trade Law 4.0 Working Paper

for Economic Cooperation and Development's (OECD) finding that information and communication technology (ICT) has a major role to play in the reduction of poverty.[132] There have also been other studies that aim to analyse the impact of new digital trade barriers on hindering innovation and sustainable development.[133]

Trade has also always been linked to innovation. Tracing back to the Silk Road, trade has been a means to disseminate new ideas and technologies and foster innovation and development. International trade and innovation can be seen to be cyclical and mutually reinforcing. Open and liberal trade regimes have the effect of facilitating the diffusion of technology, technical know-how, and access to foundational and intermediate goods, which are all critical inputs for innovation. Participating in global markets also encourages competition and facilitates greater economic integration. It therefore becomes important that developing and least-developed countries do not fall too far behind technologically, so that they can continue to compete in the international marketplace.

Certain barriers to trade in the context of ICT goods and digital trade, such as cybersecurity measures, data localisation requirements, data protection measures, as well as restrictions on the import/export of goods, are some examples that could have harmful effects on developing countries and LDCs. Localisation measures that compel businesses to conduct certain digital trade-related activities within a country's borders limit market access and generally tend to result in higher costs and sub-optimal processes for foreign firms, particularly if they are from developing countries and LDCs.[134] Similarly, strict regulations on data flows stemming from data protection laws could also potentially qualify as a trade barrier that imposes burdensome requirements on foreign firms, who may have to incur substantial costs to comply with these standards. While low levels of data protection can also be a

---

Series, Working Paper No. 03, 2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4424470.

[132] *ICTs for Development: Improving Policy Coherence*, ORG. ECON. COOP. & DEV. (2010), https://www.oecd.org/content/dam/oecd/en/publications/reports/2010/01/icts-for-development_g1ghbddc/9789264077409-en.pdf.

[133] *See e.g.,* Digital Trade in the U.S. and Global Economies (Part 1), Inv. No. 332-531, USITC Pub. 4415 (July 2013); Digital Trade in the U.S. and Global Economies (Part 2) Inv. No. 332-540, USITC Pub. 4485 (August 2014); Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64(3) EMORY L.J. 677 (2015); Simon Evenett & Johannes Fritz, *Emergent Digital Fragmentation: The Perils of Unilateralism: A Joint Report of the Digital Policy Alert and Global Trade Alert,* GLOBAL TRADE ALERT (2022), https://globaltradealert.org/reports/a-joint-report.

[134] For a more detailed study on this topic, *see* Susan Stone, James Messent & Dorothee Flaig, *Emerging Policy Issues: Localisation Barriers to Trade*, 180 ORG. ECON. COOP. & DEV. TRADE POL'Y. PAPERS (2015), https://www.oecd.org/content/dam/oecd/en/publications/reports/2015/05/emerging-policy-issues_g17a264f/5js1m6v5qd5j-en.pdf.

trade barrier by reducing consumer trust in a good or service, this is a delicate area that requires an assessment that considers the impact of these different, sometimes contrary, factors. Strict cybersecurity measures, whilst essential for national security, also have the potential to limit market access to smaller businesses and enterprises that may not be able to comply with such regulations.

Most developing countries and LDCs consistently rank lower on cybersecurity indicators, such as the ITU's Global Cybersecurity Index.[135] Accordingly, stringent cybersecurity regulations primarily impact enterprises from these countries. Limited regulatory and technical expertise in these nations also contributes to their inability to effectively trade with more technologically advanced nations and integrate into the global digital economy.[136] Furthermore, and more troublingly, in the absence of harmonised international standards or norms on cybersecurity, developing countries and LDCs may be pressured by digital powers to adopt their specific regulatory approach to cybersecurity or data protection, and prioritise this over their own developmental needs.[137]

Given these considerations, barriers to digital trade, particularly on obscure, vague, and overbroad considerations such as national security, have the capacity not only to hinder global trade but also to impact development and innovation. However, current debates and negotiations surrounding digital trade or national security do not address the development aspect or account for sustainable development considerations and SDGs. Even at the PTA/FTA level, although numerous agreements have provisions on cooperation on cybersecurity, nearly all remain silent on facilitating cyber capacity building and technical assistance in developing countries and LDCs. However, a few PTAs have attempted to reference sustainable development through digital inclusion, such as the DEPA,[138] Singapore-UK DEA,[139] the UK-New Zealand FTA,[140] and the Chile Paraguay FTA.[141]

---

135 *Global Cybersecurity Index 2024*, INT'L. TELECOMM. UNION 6 (2024), https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf.

136 Neha Mishra, *Cybersecurity and International Trade: Understanding the Policy Landscape*, INT'L INST. FOR SUSTAINABLE DEV. 19-20 (2025), https://www.iisd.org/system/files/2025-08/cybersecurity-international-trade-policy.pdf. [hereinafter Mishra].

137 Susan Ariel Aaronson & Patrick Leblond, *Another Digital Divide: The Rise of Data Realms and Its Implications for the WTO*, 21 J. INT'L. ECON. L. 245 (2018).

138 DEPA, *supra* note 121, art. 11.1(3)(b).

139 Digital Economy Agreement, Sing.–U.K., art. 8.61-P, Feb. 25, 2022, U.K.T.S. 22 (2023).

140 Free Trade Agreement, N.Z.–U.K., art. 15.20, Feb. 28, 2022, U.K.T.S. 36 (2023).

141 Free Trade Agreement, Chile–Para., art. 7.22, Dec. 1, 2021, https://edit.wti.org/document/show/6c1d59c5-a57f-42b6-baec-4ffea1a7c7d6.

It is therefore all the more important that an assessment of national security is also weighed against its impact on development, particularly in developing countries and LDCs.

VI. POLICY RECOMMENDATIONS

Debates surrounding the national security exception and its interpretation and applicability to evolving challenges have existed in academic spaces long before the first dispute even made it to a panel. Some scholars have suggested a proposal to constitute a WTO Committee on National Security to address growing challenges posed by security measures and their implications on international trade.[142] This suggestion faces the same issues as any proposal that advocates WTO reform: consensus from the entire membership. An alternative proposal has been to make use of non-violation complaints under Article XXIII(1)(b) of the GATT, thereby prioritising the solution of the tension between parties rather than directly addressing the legality of the measure.[143]

Another suggestion would be to revisit the original intention of the negotiators of the ITO Charter to divide the economic and political responsibility between the ITO and the UN, respectively. Although the WTO was concluded outside of the UN umbrella, and is intended to be a wholly independent organisation, the Arrangements for Effective Cooperation with Other Intergovernmental Organizations granted both organisations mutual observer status.[144] The arrangement encourages reciprocal participation of the WTO and the UN in each other's meetings and promotes cooperation, which could assist in the smooth and efficient functioning of both organisations in areas where such interaction could be beneficial.[145] Given the increasingly political nature of national security exceptions, trade disputes that contain both trade-related and political concerns may benefit from consultations with the UN. Although the strict delineation of authority and how this can be maintained requires significant inquiry and debate to prevent conflict, a mutually cooperative relationship between the two organisations may prove to prevent the WTO from overstepping its mandate and adjudicating on the political aspects of Members' security measures.

---

[142] Simon Lester & Inu Manak, *A Proposal for a Committee on National Security at the WTO*, 30 (2) DUKE J. COMP. INT'L. L. (2020).
[143] Nicolas Lamp, *At the Vanishing Point of Law: Rebalancing, Non-Violation Claims, and the Role of the Multilateral Trade Regime in the Trade Wars*, 22 J. INT'L. ECON. L. 721, 723, 738 (2019).
[144] Yoo and Ahn, *supra* note 24 at 440; WTO Gen. Council, *Arrangements for Effective Cooperation with Other Intergovernmental Organizations, Relations Between the WTO and the United Nations*, WTO Doc. WT/GC/W/10 (Nov. 3, 1995).
[145] *Id.*

One of the difficulties posed by invoking national security in the context of cybersecurity and digital trade is the sensitive nature of the information that would have to be shared in order to meet the requirements of successfully maintaining such a measure under Article XXI GATT or its sister provisions in other agreements: establishing a nexus between the essential security interest and the measure used to pursue the same. This requires a delicate balance between preserving States' interest not to disclose sensitive information, and ensuring that States do not abuse the provision by adopting arbitrary measures to pursue trade protectionism under the guise of national security. A way in which these competing interests can be balanced is by mandating *translucency,* where complete *transparency* cannot be achieved.[146] This is to say that States should at the very least be mandated to disclose some information regarding the security measure, such as the types of activities taken, for how long the measure is to be in place, even if a full justification of the measure is not provided.[147] In this way, States may retain sensitive information while still maintaining some amount of accountability to their trading partners. Alternatively, scholars have also suggested expanding the mandate of the Secretariat to establish a 'confidentiality system', which would have the authority to vet the credibility of the information provided by invoking Members whilst ensuring that such information is not disclosed to the public.[148] This would ensure a reasonable trade-off for members between maintaining national security, preventing access to sensitive information to antagonistic states, and upholding the integrity of the multilateral trading system and the obligations taken under it. Questions would remain on how this disclosed information should be assessed, and the types of decisions such a body can take based on such disclosures. Given the complex nature of technology and cyber-related risks, it may not be possible to assign a scale value to different types of threats to determine whether they would meet the threshold for invoking the security exception. As such, they would need to be assessed on a case-by-case basis.

Having noted the importance of the developmental element in digital trade, there is also a need to take these considerations into account in assessing the viability of any of these recommendations. Advancements in digital trade governance would also benefit from recognising the importance of development and affording technical assistance to developing countries and LDCs, as this would enable such countries to build their cyber capabilities and be effective and active participants in global trade. The international community can have a positive influence in this regard in two ways: firstly, through the regulatory harmonisation of standards. The prevalence of numerous disharmonised regulations presents significant challenges across various

---

[146] Mona Pinchis-Paulsen, *Let's Agree to Disagree: A Strategy for Trade-Security*, 25 J. INT'L. ECON. L. 527, 544 (2022).
[147] *Id.*
[148] *Id.* at 545.

sectors, from data privacy to product specifications.[149] The development of uniform international standards, or at least region-specific standards combined with Mutual Recognition Agreements (MRA) would aid in creating a level playing field for all businesses to participate in global markets and would also prevent developing countries and LDCs from having to make a difficult trade-off between their economic and developmental goals. Secondly, the WTO can also play an integral role in promoting transparency on cybersecurity measures, through discussions at WTO forums, and initiatives to map cybersecurity measures so as to afford more clarity on such measures.[150]

VII. CONCLUDING REMARKS

The foregoing analysis has sought to situate the security exception within its historical and doctrinal contexts, tracing its origins in the GATT 1947 and its subsequent incorporation into the architecture of the rules-based multilateral trading system of the WTO. What emerges is a provision that was carefully crafted to meet the demands of the time, and limited by its language to prevent abuse, but now is being required to bear interpretive weight far beyond its initial mandate. While recent jurisprudence has tried to articulate its limits and provide clarity on its interpretation and scope of application, questions still remain on whether such limits can be stretched to cover contemporary issues of national security.

Simultaneously, the landscape in which the security exception operates has also shifted considerably in the last eighty years. As such, security is no longer confined to traditional means of warfare or armed conflict between state parties, but rather has now expanded into critical digital infrastructures, artificial intelligence, and other new and emerging technologies and involves non-state actors. The multilateral framework of the WTO has struggled to effectively grapple with the nuances that this new landscape brings, and risks stretching the security exception beyond its plausible interpretive limits.

Despite these limitations, States continue to invoke national security in the context of digital trade, raising broader systemic concerns on the downstream effects of such restrictions on innovation, technology diffusion, and market access, particularly in developing and least developed nations. Therefore, indiscriminate use and abuse of the security exception to restrict trade in this manner risks entrenching asymmetries between States, particularly where access to critical digital infrastructure, technologies, and technical know-how is uneven.

---

[149] Asif Khan, *The Intersection of Artificial Intelligence and International Trade Laws: Challenges and Opportunities*, 32 IIUM L. J. 103, 117–118 (2024).

[150] Mishra, *supra* note 138, at 22.

If the security exception is to remain a legitimate and credible component of the multilateral trading system, then any future reform, interpretation, or application of this provision cannot be insulated from such developmental considerations. A more nuanced approach that acknowledges both the evolving nature of security and takes account of developmental needs is both necessary and overdue. Absent such progress, there is a real risk that the security exception, rather than operating as a narrowly tailored safeguard, becomes a vehicle to perpetuate measures that undermine the very objectives that the WTO system was designed to promote.