Forthcoming in *Cambridge Companion to World Trade Law*, edited by Chin Leng Lim & Joel Trachtman (CUP, 2024)

CHAPTER 21

SECURITY EXCEPTIONS (INCLUDING CYBERSECURITY)

Tania Voon and Mira Burri

1. INTRODUCTION

In recent years the precise nature and content of national security have gained in significance in international trade law. This development has arisen in part due to an increase in Members' invocations of 'security exceptions' in disputes within the World Trade Organization (WTO), and in part due to 'real-world' changes in what security means to individual States and groups of States. Cybersecurity in particular poses a relatively novel threat to States' interests that the drafters of the WTO Agreements may not have envisaged in the 1940s. Yet the practical (near) inability to alter WTO rules means that WTO Members must continue to resolve their disputes within the terms of these exceptions as drafted nearly a century ago.

In the context of international economic law, the meaning and nature of an 'exception' is contested.[1] However, the most common understanding of provisions constituting exceptions in WTO law is that a respondent may invoke such a provision as a defence to justify a measure that would otherwise violate a WTO obligation (commonly found in another provision in the same WTO Agreement). In general, therefore, a WTO Panel would not be expected to rule on a respondent's invocation of an exception until it has already found the challenged measure *prima facie* inconsistent with a WTO provision. Thus, for example, usually a Panel would not rule on whether a challenged measure falls within the general exceptions in Article XX of the General Agreement on Tariffs and Trade (GATT) 1994 without first having determined that the measure otherwise breaches, say, the national treatment obligation in Article III of the GATT.[2] The same general approach applies to

---

1 See, e.g., C. Henckels, 'Permission to Act: The Legal Character of General and Security Exceptions in International Trade and Investment Law' (2020) 69 *International and Comparative Law Quarterly* 557; K.J. Pelc, *Making and Bending International Rules: The Design of Exceptions and Escape Clauses in Trade Law* (Cambridge: CUP, 2016).

2 See, e.g., Appellate Body Report, *Thailand – Customs and Fiscal Measures on Cigarettes from the Philippines*, WT/DS371/AB/R, adopted 15 July 2011, para. 173; see also J. Pauwelyn, 'Defenses and the Burden of Proof In International Law' in L. Bartels and F. Paddeu (eds), *Exceptions in International Law* (Oxford University Press, 2020), 88.

security exceptions.[3] This chapter analyses those exceptions rather than the underlying (alleged) violations of WTO law.

The chapter focuses particularly on the security exceptions in WTO law,[4] while also considering corresponding exceptions in preferential trade agreements (PTAs), as identified in section 2. In four Panel Reports circulated since 2019 (only one of which has been adopted), WTO Panels have ruled on the security exceptions in more than one WTO agreement.[5] This development has shifted the previous pattern, over more than two decades since the WTO was established in 1995, of WTO Members refraining from invoking the security exceptions, presumably due to their wish to retain discretion without unwanted 'legal' oversight.

In the absence of a ruling by the WTO Appellate Body, these four Panel Reports (and particularly the sole adopted Panel Report in *Russia – Traffic in Transit*) provide extensive guidance on the interpretation and application of WTO security exceptions, as well as (potentially) PTA exceptions. We show in section 3 that although the WTO exceptions provide scope for WTO Members to define their own security interests and the measures necessary to protect those interests, WTO Panels have been unafraid to review such decisions and to require objectivity with respect to several elements. This approach aims for an appropriate balance to prevent Members from abusing the exceptions, which could otherwise involve improper circumvention of WTO obligations. However, it runs contrary to the United States (US) position[6] and therefore will do little to address US concerns about the WTO Appellate Body and the WTO dispute settlement system more broadly.[7]

---

3 In the only adopted Panel Report (*Russia – Traffic in Transit*), which is discussed in detail in this chapter, the Panel deviated from the normal order of review. The Panel started reviewing whether the Russian measures could be justified by GATT Article XXI without first establishing whether they had breached the Russian trade obligations under a primary rule, such as GATT Article V (freedom of transit). The Panel explained that the emergency in international relations involves a fundamental change of circumstances, which alters the factual matrix of the evaluation of consistency of the WTO measures. The Panel proceeded with substantive claims of violation only in the second part of its report. The Panel explained that should its findings on Russia's invocation of Article XXI (b)(iii) be reversed on appeal, it might be necessary for the Appellate Body to complete the analysis based on the Panel's other findings. The Panel Report was however not appealed.

4 For other analyses, see, e.g., T. Voon, 'The Security Exception in WTO Law: Entering a New Era' (2019) 113 *AJIL Unbound* 45; C. Wang, 'Invocation of National Security Exceptions under GATT Article XXI: Jurisdiction to Review and Standard of Review' (2019) 18 *Chinese Journal of International Law* 695; G. Vidigal, 'WTO Adjudication and the Security Exception: Something Old, Something New, Something Borrowed – Something Blue?' (2019) 46 *Legal Issues of Economic Integration* 203; V. Lapa, 'The WTO Panel Report in *Russia – Traffic in Transit*: Cutting the Gordian Knot of the GATT Security Exception?' (2020) 69 *Questions of International Law* 5.

5 Panel Report, Russia – Measures Concerning Traffic in Transit (Russia – Traffic in Transit), WT/DS512/R, circulated 5 April 2019, adopted 26 April 2019; Panel Report, Saudi Arabia – Measures Concerning the Protection of Intellectual Property Rights (Saudi Arabia – IPRs), WT/DS567/R, circulated 16 June 2020, dispute terminated while appeal pending; Panel Report, United States – Origin Marking Requirement (US – Origin Marking (Hong Kong, China), WT/DS597/R, circulated 21 December 2022, appealed 26 January 2023; Panel Reports, United States – Certain Measures on Steel and Aluminium Products, WT/DS544/R (China) / WT/DS552/R (Norway) / WT/DS556/R (Switzerland) / WT/DS564/R (Turkey), circulated 9 December 2022, appealed 26 January 2023. Mutually agreed solutions were reported in the Panel Reports in US – Steel and Aluminium Products, WT/DS550/R (Canada) / WT/DS551/R (Mexico), circulated 11 July 2019.

6 See, e.g., Statement by the US at the Meeting of the WTO Dispute Settlement Body (Geneva, 27 January 2023).

7 See, e.g., United States Trade Representative, *Report on the Appellate Body of the World Trade Organization* (February 2020).

At the same time, the significance of the WTO security exceptions is growing, as the concept of national security continues to evolve, as elaborated in section 4. This expansion is particularly evident in the area of cybersecurity, as States face cyberattacks, as well as develop distinct cybersecurity strategies to address them. The chapter explores the interface between cybersecurity and the security exceptions in section 5, pointing out shortcomings of the existing WTO approach to these exceptions in the context of cybersecurity, as well as the limitations of alternative PTA approaches.

2. SECURITY EXCEPTIONS IN THE WTO AND IN PREFERENTIAL TRADE AGREEMENTS

2.1 GATT Article XXI and Corresponding WTO Exceptions

The classic 'security exceptions' in international trade law are found in the General Agreement on Tariffs and Trade 1947 (GATT 1947), as now incorporated in Article XXI of the GATT 1994.[8] This provision encompasses a range of exceptions in the following terms (emphasis added):

Nothing in this Agreement shall be construed

(a) to require any Member to furnish any information the disclosure of which *it considers* contrary to its *essential security interests*; or

(b) to prevent any Member from taking any action which *it considers* necessary for the protection of its *essential security 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 Member from taking any action in pursuance of its obligations under the United Nations Charter for the maintenance of *international peace and security*.

Article 73 of the WTO Agreement on Trade-Related Aspects of Intellectual Property (TRIPS) contains the same exceptions. Article XIV*bis* of the General Agreement on Trade in Services (GATS) contains corresponding exceptions, although Article XIV*bis*(b)(ii) (corresponding to GATT

---

8 On the history of the security exceptions, see, e.g., Negotiating Group on GATT Articles, Article XXI: Note by the Secretariat para. 14, GATT Doc. MTN.GNG/NG7/W/16 (18 August 1987); J.Y. Yoo and D. Ahn, 'Security Exceptions in the WTO System: Bridge or Bottle-Neck for Trade and Security?' (2016) 19 *Journal of International Economic Law* 417; M. Pinchis-Paulsen, 'Trade Multilateralism and U.S. National Security: The Making of the GATT Security Exceptions' (2020) 41 *Michigan Journal of International Law* 109.

Article XXI(b)(i)) refers to 'fissionable *and fusionable* materials or the materials from which they are derived', and Article XIV*bis*(b)(i) (corresponding to GATT Article XXI(b)(ii)) refers to 'the *supply of services* as carried out directly or indirectly for the purpose of *provisioning* a military establishment' (emphasis added).

Some WTO Members (typically respondents in WTO disputes) have identified the words 'which it considers' in both GATT Article XXI(a) and (especially) Article XXI(b) as evidence that these security exceptions are non-justiciable, in the sense that Members have full discretion in making this assessment and that WTO Panels cannot override them, as discussed further in section **Fehler! Verweisquelle konnte nicht gefunden werden.** below. The words 'essential security interests' in the same two provisions, which are undefined, raise significant questions about the types of security concerns covered by the exceptions, as elaborated in section **Fehler! Verweisquelle konnte nicht gefunden werden.** below. The words 'other emergency in international relations' in GATT Article XXI(b)(iii) have the potential to broaden the range of relevant circumstances far beyond the traditional understanding of 'war' in that provision, as addressed in section **Fehler! Verweisquelle konnte nicht gefunden werden.** below.

2.2 Security Exceptions in Preferential Trade Agreements

Like many WTO provisions, the security exceptions have played an important role in influencing the drafting of many PTAs, as well as of some bilateral investment treaties. Sometimes the WTO exceptions are incorporated by reference; in other agreements the WTO exceptions are essentially replicated or adopted with modifications. As security exceptions have grown in significance in the last several years, this pattern has continued with more recently concluded treaties.

For example, Article 201 of the PTA between China and New Zealand (both in the original 2008 treaty and as 'upgraded' in 2022) contains wording very similar to that in GATT Article XXI. Article 16.3 of the 2015 PTA between China and Australia states that 'Article XXI of GATT 1994 and Article XIV*bis* of GATS are incorporated into and made part of this Agreement, *mutatis mutandis*'. Similarly, Article 14.62 of the 2022 PTA between Japan and the United Kingdom (UK) provides, for the purposes of the intellectual property chapter, that 'Article 73 of the TRIPS Agreement is hereby incorporated into and made part of this Agreement, *mutatis mutandis*'.

Several larger regional PTAs also include security exceptions broadly modelled on the WTO security exceptions. For instance, Article 28.6 of the Comprehensive Economic and Trade Agreement between Canada and the European Union (CETA) is fairly similar to GATT Article XXI, although it is somewhat broader (e.g. referring to 'international obligations' rather than those under the UN Charter) in Article 28.6(c)).

Article 29.2 of the Trans-Pacific Partnership Agreement (TPP), as incorporated in the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), which entered

into force on 30 December 2018 and has 11 States parties as of 12 July 2023,[9] contains a simplified version of the GATT security exceptions, possibly granting greater flexibility to parties wishing to invoke them. Article 29.2(a) corresponds to GATT Article XXI(a) but uses the words 'which it determines' (similar to some other treaties such as CETA and the China–New Zealand PTA) rather than 'which it considers'. Article 29.2(b) omits the separate sub-paragraphs and details found in GATT Article XXI(b) and XXI(c), stating simply that nothing in the CPTPP shall be construed to 'preclude a Party from applying measures that it considers necessary for the fulfilment of its obligations with respect to the maintenance or restoration of international peace and security, or the protection of its own essential security interests'.

Although the US is not a CPTPP party, having withdrawn from the TPP in 2017, its heavy influence on the TPP text (signed in 2016) is evident.[10] This phenomenon is also reflected in the fact that Article 32.2 of the United States–Mexico–Canada Agreement (USMCA), which entered into force in 2020, mirrors the CPTPP provision. The greater discretion granted to parties invoking the security exceptions in the CPTPP and USMCA is unsurprising, given the US stance in the WTO as discussed further below.

One difference appearing in some agreements (such as the CPTPP and USMCA but also the European Union–New Zealand PTA and the Digital Economy Partnership Agreement [DEPA] among Chile, New Zealand and Singapore) when compared to Article XXI GATT 1994/Article XIV*bis* GATS is the inclusion of the phrase 'or allow access to' next to 'furnish any information'. By adding this term, the parties may intend to extend the security exceptions to cover means of providing access to the sensitive information other than actively transferring or surrendering it. This textual change increases the degree of legal certainty that the security exceptions cover instances where the information is not actively transferred but provided by other means.

3. JUSTICIABILITY OF AND DEFERENCE IN SECURITY EXCEPTIONS

A longstanding question concerning the WTO security exceptions (and PTA exceptions modelled on them) is to what extent the exceptions are justiciable. Does a WTO Panel have jurisdiction to rule on whether a Member's action falls within these exceptions, or does each Member have the ability to invoke them at will? If a WTO Panel does have jurisdiction over such an invocation, what degree of deference must it give to the Member's interpretation or application of the exceptions? Does the Member have full autonomy in this regard?[11]

In *Russia – Traffic in Transit*, the first WTO Panel Report on GATT Article XXI (adopted without appeal in 2019), the Panel held that GATT Article XXI(b)(iii) is neither 'totally "self-judging" in the manner asserted by Russia' nor 'non-justiciable' as argued by the US.[12] Russia had argued that,

---

9 Including the 10 original States parties and the most recently acceded UK in 2023.

10 See, e.g., T. Allee and A. Lugg, 'Who Wrote the Rules for the Trans-Pacific Partnership?' (2016) 3(3) *Research and Politics* 1.

11 See, e.g., R.P. Alford, 'The Self-Judging WTO Security Exception' (2011) 3 *Utah Law Review* 697.

12 Panel Report, *Russia – Traffic in Transit*, paras. 7.102–7.103.

'under GATT Article XXI(b)(iii), both the determination of a Member's essential security interests the determination of whether any action is necessary for the protection' of those interests 'are at the sole discretion of the Member invoking the provision'.[13] The Panel instead found that the words 'which it considers' at the start of Article XXI(b) do not qualify its subparagraph (iii): '[F]or action to fall within the scope of Article XXI(b), it must objectively be found to meet the requirements in one of the enumerated subparagraphs of that provision'.[14] In reaching that conclusion, the Panel stated in:

> It would be entirely contrary to the security and predictability of the multilateral trading system established by … the WTO … to interpret Article XXI as an outright potestative condition, subjecting the existence of a Member's … WTO obligations to a mere expression of the unilateral will of that Member.[15]

As for Members' determination that a given action is 'necessary for the protection of its essential security interests' within the meaning of the opening words of GATT Article XXI(b), the same Panel emphasised that Members must 'interpret and apply' this provision 'in good faith'.[16] The Panel continued in the same paragraph by characterising this obligation as 'a general principle of law and a principle of general international law which underlies all treaties, as codified in' Articles 26 and 31(1) of the Vienna Convention on the Law of Treaties (VCLT). Thus, Members must not 'use the exceptions in Article XXI as a means to circumvent their obligations under the GATT 1994'.[17] The good faith obligation applies to the Member's identification of its 'essential security interests' (as discussed further in section **Fehler! Verweisquelle konnte nicht gefunden werden.** below) as well as the connection between those interests and the challenged measures. A Panel will therefore assess whether 'the measures at issue meet a minimum requirement of plausibility in relation to the proffered essential security interests, i.e. that they are not implausible as measures protective of these interests'.[18] We explain how the Panel applied that test to the dispute between Russia and Ukraine in section **Fehler! Verweisquelle konnte nicht gefunden werden.** below.

At the meeting of the WTO Dispute Settlement Body (DSB) at which this Panel Report was adopted in 2019, Members such as the European Union and Australia welcomed the Panel's decision that its jurisdiction to determine Russia's invocation of Article XXI.[19] However, the US maintained that:

> WTO Members had understood, from the very beginning of the international trading system, that each Member could judge for itself what actions it considered necessary to protect its essential security interests. This had been the position of the United States for over 70 years, since the negotiation of the GATT. That position had been shared by every WTO Member

---

13 Ibid., para. 7.27.
14 Ibid., para. 7.82.
15 Ibid., para. 7.79.
16 Ibid., para. 7.132.
17 Ibid., para. 7.132.
18 Ibid., para. 7.138.
19 WTO, *Dispute Settlement Body: Minutes of Meeting on 26 April 2019*, WTO Doc WT/DSB/M/428 (25 June 2019), para. 8.6 (European Union) and para. 8.10 (Australia).

> whose national security action had previously been the subject of complaint, including the European Union, Canada, Russia, and others.[20]

In its subsequent report circulated in 2020, the Panel in *Saudi Arabia – IPRs* refused Saudi Arabia's request (in the context of TRIPS Article 73(b)(iii)) that the Panel decline to make any findings because (in Saudi Arabia's words) the dispute was not about 'trade' but about 'political, geopolitical and essential security'.[21] The Panel noted that Saudi Arabia did not frame these arguments in terms of jurisdiction or justiciability, but several third parties saw them as implying non-justiciability.[22] The Panel essentially took the reasoning of the Panel in *Russia – Traffic in Transit* regarding GATT Article XXI(b)(iii) and applied it to TRIPS Article 73(b)(iii),[23] as elaborated in sections **Fehler! Verweisquelle konnte nicht gefunden werden.** and **Fehler! Verweisquelle konnte nicht gefunden werden.** below.

Two further WTO disputes have led to Panel Reports regarding GATT Article XXI(b)(iii), both circulated in late 2022. The US, as respondent in both these disputes, has appealed them both to the currently non-functional WTO Appellate Body, leaving the Panel Reports in limbo and unadopted. In *US – Origin Marking*, the Panel agreed with the Panel in *Russia – Traffic in Transit* that the words 'which it considers' at the beginning of GATT Article XXI(b) do 'not extend to the subparagraphs', which are 'subject to review by a panel'.[24] Similarly, in *US – Steel and Aluminium Products*, the Panel determined that Article XXI(b) is not '"self-judging" or "non-justiciable" in the sense argued by the United States'; nor does it contain '"a single relative clause" that wholly reserves the conditions and circumstances of the subparagraphs to the judgment of the invoking Member'.[25] In appealing this decision, the US insisted that '[i]ssues of national security are political matters not susceptible to review or capable of resolution by WTO dispute settlement'.[26]

Different States' positions on these questions may be reflected in their PTA provisions. For example, Article 1.5.1 of the PTA between Japan and UK mentioned above corresponds fairly closely to GATT Article XXI but includes a potentially significant modification in Article 1.5.1(b) (corresponding to GATT Article XXI(b)). Whereas the GATT Article XXI(b) wording is arguably ambiguous as to whether the words 'which it considers' qualify the subsequent sub-paragraphs, Article 1.5.1(b) of the Japan–UK PTA indicate that they do not, stating: 'Nothing in this Agreement shall be construed … as preventing a Party from taking any action, which it considers necessary for the protection of its essential security interests, including action: (i) relating to fissionable and fusionable materials …'. The placement of the second comma suggests, consistent with the reasoning of WTO Panels with respect to GATT Article XXI(b), that whether an action falls within a sub-paragraph is an objective question not simply left to the party's discretion. However, the

---

20 Ibid., at para. 8.11 (United States).

21 Panel Report, *Saudi Arabia – IPRs*, paras. 7.8, 7.23.

22 Ibid., para. 7.9.

23 Unlike in *Russia – Traffic in Transit*, the Panel Report in *Saudi Arabia – IPRs* was not adopted and is of limited legal significance because the parties agreed to terminate their dispute almost two years after circulation of the Panel Report, following suspension of the appeal.

24 Panel Report, *US – Origin Marking*, para. 7.185.

25 Panel Report, US – Steel and Aluminium Products, para. 7.128.

26 Letter from M. Pagán, US Ambassador, to Athaliah Lesiba Molkomme, DSB Chairperson (26 January 2023).

inclusion of the word 'including' suggests that actions falling within Article 1.5.1(b) need not necessarily fall within any of the sub-paragraphs, contrary to the reading of the differently worded GATT Article XXI(b) by WTO Panels. Such modifications may expand the breadth of the security exceptions in the relevant PTA.

A few other PTAs, particularly Asian-led ones,[27] contain an exception for the protection of a party's essential security interests with particular regard to digital trade, with the additional requirement that other parties cannot dispute the necessity of such measures.[28] The PTA between Moldova and the European Free Trade Association (EFTA) has a similar provision only for the bilateral relationship between Norway and Moldova, without an explicit mention as to its self-judging effect.[29]

4. GROWING RANGE OF SECURITY CONCERNS AND RESPONSES

4.1 Essential Security Interests and Their Connection to the Challenged Measures: Article XXI(a), (b)

In *Russia – Traffic in Transit*, the Panel characterised 'essential security interests' (with reference to Article XXI(b)) as 'a narrower concept' than 'security interests' and as referring to 'those interests relating to the quintessential functions of the state, namely, the protection of its territory and its population from external threats, and the maintenance of law and public order internally'.[30] Russia's relevant interests in that dispute involved 'the security of the Ukraine–Russia border'.[31] The Panel found plausible (as explained in section 3 above) Russia's contention that it implemented measures restricting transit of goods from Ukraine across Russia to protect those interests.[32]

In *Saudi Arabia – IPRs*, the Panel described the relevant interests as expressed by Saudi Arabia as involving 'protecting itself "from the dangers of terrorism and extremism"'.[33] The Panel accepted as plausible (following the standard identified in *Russia – Traffic in Transit*) Saudi Arabia's argument that it implemented 'anti-sympathy' measures (preventing a Qatari corporate group from obtaining counsel to enforce its intellectual property rights in Saudi Arabia) to protect those interests.[34] However, the Panel rejected Saudi Arabia's suggestion that its decision not to apply criminal penalties to the Saudi-based media group beoutQ for violation of beIN's intellectual property rights

---

27 Eurasian Economic Union (EAEU)–Singapore FTA; RCEP; ASEAN–Australia–NZ FTA (Second Protocol).

28 See, e.g., RCEP, in which the data localization provision (Article 12.14(3)) is expressed not to prevent a party from taking 'any measure that it considers necessary for the protection of its essential security interests. Such measures shall not be disputed by other Parties'. Article 12.15 RCEP has an identical exception with regard to data flow commitments.

29 Article 5.11 EFTA–Moldova FTA: 'Between Norway and the Republic of Moldova, nothing in this Article shall be construed to prevent Norway or the Republic of Moldova from taking any action which it considers necessary for the protection of its essential security interests'.

30 Panel Report, *Russia – Traffic in Transit*, para. 7.130.

31 Ibid., para. 7.136.

32 Ibid., para. 7.145.

33 Panel Report, *Saudi Arabia – IPRs*, para. 7.280.

34 Ibid., para. 7.288.

(through illegal broadcasts of beIN's material) was plausibly necessary to protect these security interests.[35] The Panel considered that, unlike the anti-sympathy measures, the non-enforcement of criminal procedures against beoutQ could not be seen as part of 'Saudi Arabia's umbrella policy of ending or preventing any form of interaction with Qatari nationals'.[36]

In *US – Steel and Aluminium Products*, the Panel explained that the word 'essential' in Article XXI(b) 'indicates the heightened significance of the security interests that Members are not prevented from taking action to protect'.[37] This aspect did not play a significant role in this decision (or that in *US – Origin Marking*) because of the Panel's conclusion regarding the absence of an emergency in international relations, as discussed in section 4.2 below.

4.2 War and Other Emergencies in International Relations: Article XXI(b)(iii)

The identification of a war or other emergency in international relations for the purposes of GATT Article XXI(b)(iii) has been central to the WTO cases on the security exceptions to date. In two of these cases, the Panel agreed with the respondent that the situation between the parties did constitute an emergency in international relations. In *Russia – Traffic in Transit*, the Panel described such an emergency as '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] The Panel concluded that the 'situation between Ukraine and Russia since 2014' constituted such an emergency, noting that the countries' relations had 'deteriorated to such a degree that they were a matter of concern to the international community', and that the General Assembly of the United Nations recognised the situation as involving 'armed conflict'.[39] In *Saudi Arabia – IPRs* (with respect to the equivalent TRIPS provision, as noted above), such an emergency began between Saudi Arabia and Qatar in at least mid-2017 when Saudi Arabia severed 'all diplomatic, consular and economic relations' with Qatar.[40]

In contrast, in the most recent two WTO cases on the security exceptions, the Panel found no emergency in international relations. In *US – Origin Marking*, the Panel summarised such an emergency as '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'.[41] It concluded that concerns about the 'human rights situation in Hong Kong' had not 'escalated to a threshold of requisite gravity to constitute an emergency in international relations'.[42] Accordingly, the US requirement that goods imported from Hong Kong be marked 'China' rather than 'Hong

35 Ibid., para. 7.293.
36 Ibid., para. 7.289.
37 Ibid., para. 7.141.
38 Panel Report, *Russia – Traffic in Transit*, para. 7.76.
39 Ibid., paras. 7.122 and 7.123.
40 Panel Report, *Saudi Arabia – IPRs*, paras. 7.259 and 7.262.
41 Panel Report, *US – Origin Marking*, para. 7.315.
42 Ibid., para. 7.358.

Kong' (contrary to the most-favoured-nation (MFN) obligation with respect to marks of origin in GATT Article IX:1) did not fall within the exception in GATT Article XXI(b)(iii).[43]

In *US – Steel and Aluminium Products*, the Panel characterised such emergencies as 'situations of a certain gravity or severity and international tensions that are of a critical or serious nature in terms of their impact on the conduct of international relations'.[44] It found that 'concerns regarding global excess capacity in steel and aluminium' did not 'ris[e] to the gravity or severity of tensions on the international plane' necessary to constitute such an emergency.[45] Therefore, the challenged US measures (being additional import duties on derivative steel and aluminium products from early 2020, and corresponding exemptions from those duties for certain products from certain countries, contrary to US tariff bindings in GATT Article II:1 and the general MFN obligation in GATT Article I:1) were not justified under GATT Article XXI(b)(iii).[46]

Article 17.13 of the 2022 Regional Comprehensive Economic Partnership (RCEP), which notably includes China among its (now) 14 States parties, contains security exceptions modelled on GATT Article XXI, but with the addition of subparagraph (iii) to Article 17.13(b) (corresponding to GATT Article XXI(b)), which refers to actions 'taken so as to protect critical public infrastructures including communications, power, and water infrastructures'. Footnote 7 adds, '[f]or greater certainty', that 'this includes critical public infrastructures whether publicly or privately owned'. This addition to GATT Article XXI provides a hint of the ways in which the concept of national security is expanding into new areas, with the potential for a significant expansion in the scope of security exceptions. This shift is particularly relevant in the domain of cybersecurity, as discussed in the next section.

5. CYBERSECURITY AND THE SECURITY EXCEPTIONS

As noted earlier, cybersecurity has become a critical topic for many States around the world, and restrictions on trade driven by cybersecurity concerns are on the rise.[47] Such cybersecurity measures may be inconsistent with a number of trade obligations across the different WTO Agreements, potentially violating non-discrimination obligations, rules on market access for goods and services, transparency, and intellectual property rights protection or constituting unlawful technical barriers to trade.[48] Indeed, the possibilities for such violations have only increased with the changed and

43 Ibid., paras. 8.1(b)–8.1(c).

44 Panel Reports, US – Steel and Aluminium Products, para. 7.147.

45 Ibid., para. 7.148.

46 Ibid., para. 7.149.

47 See, e.g., S. Peng, 'Cybersecurity Threats and the WTO National Security Exceptions' (2015) 18 *Journal of International Economic Law* 44; G. Gagliani, 'Cybersecurity, Technological Neutrality, and International Trade Law' (2020) 23 *Journal of International Economic Law* 723; J.P. Meltzer, 'Cybersecurity, Digital Trade, and Data Flows' (2020) 132 *Global Economy and Development Working Paper*.

48 See, e.g., Gagliani, ibid.; N. Mishra, 'The Trade: (Cyber)Security Dilemma and Its Impact on Global Cybersecurity Governance' (2020) 54 *Journal of World Trade* 567.

changing nature of cybersecurity in the contemporary digital environment.[49] We are no longer talking about mere security of computers but about security in a digitally (hyper)connected environment enabled by cross-border data flows and also interdependent with the development and deployment of Artificial Intelligence (AI) and Internet of Things (IoT). With the increased datafication and connectivity, trade and cybersecurity become more entangled.[50] This is true not only for Chinese and Russian cybersecurity laws that extensively cover data security and control over data flows but also for the United States and other countries that share broad conceptualizations of cybersecurity.[51]

The question then is to what extent the multitude of measures that fall under the broad chapter of cybersecurity can be 'excused' under the existing security exceptions. As highlighted earlier, the WTO security exceptions were negotiated in different times, during the Cold War and with the atrocities of the World War II not far behind. They were also adopted with the underlying understanding that national security issues would be tackled through diplomatic rather than trade channels.[52] For the specific context of cybersecurity, it should be above all noted that the security exceptions were designed for conventional, 'offline', types of security measures.[53] This renders efforts to distinguish between economic protectionism and genuine national security concerns in the cyber domain only harder.

The *Russia – Traffic in Transit* case, discussed in detail above, does give us some baselines to test cybersecurity measures, but by no means clear answers. As noted, in addition to clarifying the justiciability under GATT Article XXI, the Panel applied a two-step approach in its analysis — first, in reviewing objectively the existence of a 'war', 'emergency' or other basis for invoking the exception and second, applying a deferential good faith test as to whether the measure for the state's security interest is necessary.

One of the difficulties in applying this test to cybersecurity situations is that the facts in the Russia–Ukraine case were quite straightforward and relatively 'easy' to adjudicate on, especially as the

---

49 Gagliani, ibid. The broad conceptualization of cybersecurity is reflected in the definition given by the International Telecommunication Union (ITU): 'Cybersecurity is the 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 organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: Availability; Integrity, which may include authenticity and non-repudiation; and Confidentiality.' ITU, Overview of Cybersecurity, Recommendation ITU-T X.1205 (2008).

50 Meltzer, supra note 47. Meltzer (ibid., at 8) defines five areas of cyber risk with impact on the digital economy: (1) the national defense space, including all military and intelligence services; (2) critical infrastructure; (3) trade secrets and IP with commercial value; (4) other online information; and (5) access to data and technology through international investment. With specific regard to IoT, see J.P. Trachtman, 'Cybersecurity versus Trade in Internet of Things Products' (2019) 16(3) *Manchester Journal of International Economic Law* 301.

51 Meltzer, ibid.

52 See, e.g., Pinchis-Paulsen, supra note 8; see also J.B. Heath, 'The New National Security Challenge to the Economic Order' (2020) 129 *The Yale Law Journal* 1020.

53 Meltzer, supra note 47.

situation of emergency was close to a 'hard core' emergency in international relations.[54] Yet, in many cybersecurity cases, a finding that the circumstances amount to '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'[55] might be difficult. Indeed, cybersecurity is not necessarily linked to armed conflict or even any conflict. As the Tallinn Manual 2.0 itself notes, 'States have to deal with cyber issues that lie below the use of force threshold on a daily basis'.[56] Furthermore, as security in the hyper connected cyberspace is not about 'zero risk', it is unclear how much 'risk' in cyberspace would amount to a danger to 'essential interests'.[57] It is in the same vein unclear how governments' responses to the diffuse, longer-term nature of cyber risk would be qualified.

The temporal element, namely that the restrictions were 'taken in time of' the emergency in international relations[58] might also be hard to prove. As noted, the changed nature of cybersecurity means rather that we have a situation of 'indefinite emergencies'.[59] In certain situations, it might be easier for a WTO Member to use the general exception clauses, under GATT Article XX or GATS Article XIV, to satisfy at least the first stage of the legal test by showing that a cybersecurity measure is intended to address public morals or public order, rather than by seeking to establish that there is an emergency in international relations and the measures were taken during that emergency (yet proving the necessity of the measure as well as satisfying the chapeau tests under the general exception clauses would pose a higher hurdle than the security exceptions).[60]

The chapeau test of GATT Article XXI(b) does provide certain flexibilities as to what constitutes 'essential security interests', as the Panel in *Russia – Traffic in Transit* noted that these can change according to circumstances and that WTO Members can define their own essential security interests. Yet, this determination is limited by the requirement that it must be done in good faith. The latter is also true for the determination of the 'necessity' of the measure and requires some minimal plausible relation between the measure adopted and the essential security interest.[61] In this sense, reacting upon high risk catastrophic cyberattacks can be considered an 'essential security interest'. Yet, a large palette of cybersecurity measures that are not linked to an imminent catastrophic attack might not qualify.[62] Furthermore, the complexity of the issues, as well as governments' reliance on classified

---

54 Panel Report, *Russia – Traffic in Transit*, para. 7.136; see also Lapa, supra note 4, referring to J.B. Heath, 'Guest Post: Trade, Security and Stewardship (Part IV): A Variable Framework for Security Governance' International Economic Law and Policy Blog (8 May 2019) <https://worldtradelaw.typepad.com/ielpblog/2019/05/guest-post-trade-security-and-stewardship-part-iv-a-variable-framework-for-security-governance.html>.

55 Panel Report, *Russia – Traffic in Transit*, para. 7.76.

56 Gagliani, supra note 47, citing M.N. Schmitt, 'Introduction', in M.N. Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: CUP 2017), at 1.

57 Lapa, supra note 4.

58 Panel Report, *Russia – Traffic in Transit*, para. 7.70.

59 Heath, supra note 52, at 1045.

60 See, e.g., N. Mishra, 'Privacy, Cybersecurity, and GATS Article XIV: A New Frontier for Trade and Internet Regulation?' (2020) 19(3) *World Trade Review* 341; N. Mishra, 'Breaking Down Digital Walls: The Interface of International Trade Law and Online Content Regulation through the Lens of the Chinese VPN Measure' (2022) 47(2) *Brooklyn Journal of International Law* 359.

61 Panel Report, *Russia – Traffic in Transit*, paras. 7.132–7.138.

62 Meltzer, supra note 47, at 26, referring also to Trachtman, supra note 50.

information,[63] are likely to present substantial hurdles to using the security exceptions as a way to discipline disguised protectionism.[64]

Overall, it appears that the WTO security exceptions do not provide an adequate toolbox to balance economic and cybersecurity concerns.[65] As mentioned, this has to do with the changed nature of cybersecurity concerns and measures that address them. This also unfolds in a broader context where the relationship between economic liberalization and national security has been reconfigured, and industrial policy has become intrinsically linked to national security.[66] Taking this into account, some authors have suggested that a model of non-judicial rebalancing, similar to the WTO safeguards regime, can work better to manage the interface between trade and national security, as States would be permitted to unilaterally restrict trade due to security concerns but would need to offer compensatory trade liberalization in other sectors or be subject to retaliation by other Members.[67] Others see the WTO Appellate Body's current crisis as a 'pause' that allows experimentation across different venues with alternative models for managing trade-and-security disputes,[68] including, for instance, the development of new cybersecurity-related trade rules or the development of global cybersecurity standards.[69]

In the latter context, it should be mentioned that many PTAs, especially those that have extensive digital trade commitments, have norms of relevance to cybersecurity. Presently, out of 432 PTAs, 122 have deeper dedicated e-commerce/digital trade chapters and 67 have provisions on cybersecurity.[70] Many of these are of soft legal nature and provide for mere cooperation efforts.[71] Other treaties, such as the USMCA, elaborate, alongside cooperation efforts, a risk-based approach to cybersecurity. Article 19.15(2) USMCA states in this sense: 'Given the evolving nature of cybersecurity threats, the Parties recognize that risk-based approaches may be more effective than prescriptive regulation in addressing those threats. Accordingly, each Party shall endeavor to employ, and encourage enterprises within its jurisdiction to use, risk-based approaches that rely on

---

63 It is noteworthy in this context that the Panel in *Russia – Traffic in Transit* (para 7.135) underscored that: 'What qualifies as a sufficient level of articulation will depend on the emergency in international relations at issue. In particular, the Panel considers that the less characteristic is the "emergency in international relations" invoked by the Member, i.e. the further it is removed from armed conflict, or a situation of breakdown of law and public order (whether in the invoking Member or in its immediate surroundings), the less obvious are the defence or military interests, or maintenance of law and public order interests, that can be generally expected to arise. In such cases, a Member would need to articulate its essential security interests with greater specificity than would be required when the emergency in international relations involved, for example, armed conflict'.

64 Meltzer, supra note 47, at 3.

65 See also N. Mishra, 'The Trade: (Cyber)Security Dilemma and Its Impact on Global Cybersecurity Governance' (2020) 54(4) *Journal of World Trade* 567.

66 J.B. Heath, 'Trade and Security among the Ruins' (2020) 30 *Duke Journal of Comparative and International Law* 223; see also V.K. Aggarwal and A.W. Reddie, 'Comparative Industrial Policy and Cybersecurity: A Framework for Analysis' (2018) 3 *Journal of Cyber Policy* 291.

67 S. Lester and H. Zhu, 'A Proposal for "Rebalancing" to Deal with "National Security" Trade Restrictions' (2019) 42 *Fordham International Law Journal* 1451.

68 Heath, supra note 66.

69 Meltzer, supra note 47.

70 This information is based on the TAPED dataset, which covers all PTAs from January 2000 to November 2023 and codes 124 different items with relevance for digital trade. See M. Burri, M. Vásquez Callo-Müller and K. Kugler, *TAPED: Trade Agreement Provisions on Electronic Commerce and Data* <https://unilu.ch/taped>.

71 See, e.g., Article 5.1 DEPA.

consensus-based standards and risk management best practices to identify and protect against cybersecurity risks and to detect, respond to, and recover from cybersecurity events'.

Overall, PTA security exceptions coupled with cooperation initiatives do provide for more flexibility in employing cybersecurity measures that may restrict digital trade — this may however seriously undermine the commitments made.[72] There are still no precedents that clarify the use of these exceptions. Experience from investment treaties shows however that, even in cases involving potentially self-judging exceptions, the tribunals' interpretation of essential security interests suggests thus far that restraint has been exercised and the breadth of the concept has not had 'an unduly detrimental impact on the regime's ability to protect their [*sic:* investors'] interests'.[73]

6. CONCLUSION

A review of WTO caselaw demonstrates two key areas in which security exceptions generate controversy: the extent of a Member's discretion to identify both their own security interests and the measures needed to protect those interests without oversight by external decisionmakers such as WTO Panels; and the nature of legitimate security concerns in today's world, as we move further beyond supplies for military establishments — for instance, in the domain of cybersecurity. In general, PTAs show the strong influence of WTO security exceptions, while also highlighting potential areas for reform according to individual States' positions with respect to these two controversial areas.

The greater the deference accorded to WTO Members in selecting the measures necessary to protect national security, and the greater the scope of security interests recognised as valid in WTO disputes, the more autonomy Members will have with respect to their own security. The US position is that these are not matters for dispute resolution. However, if no objective standard applies to a respondent's invocation of the WTO security exceptions, and if Panels decline jurisdiction to resolve disputes involving these exceptions, the international trading system established by the WTO risks collapse. If a WTO Member merely has to declare that their measure is justified on security grounds in order for it to be unchallengeable in the WTO dispute settlement system, the oversight provided by the WTO will dissipate. Yet, paradoxically, the current WTO law on the limited deference available to Members with respect to security exceptions, exemplified by the adopted Panel Report in *Russia – Traffic in Transit*, also arguably threatens the WTO dispute settlement system by providing further reasons for the US refusal to appoint new Appellate Body Members.

In a geopolitically complex world, where industrial policy looms large and is underpinned by national security considerations, we are bound to see more experimentation as to the balancing of trade and security. Digital trade rulemaking is likely to be one of the areas where such experimentation (for good or bad) takes place, as both the fostering of the digital economy as well as

---

72 Meltzer, supra note 47, 2–3; Heath, supra note 66.

73 C. Henckels, 'Whither Security? The Concept of "Essential Security interests" in Investment Treaties' Security Exceptions' (2024) 27 *Journal of International Economic Law* 1, at 16.

cybersecurity concerns are high on States' priority lists. The current WTO jurisprudence on the security exceptions does not sit easily with cybersecurity scenarios; nor do the developments in such exceptions in PTAs necessarily offer a better balance. Further innovations may be required to ensure that security exceptions are drafted, interpreted and applied in such a way that the reality of modern day national security is acknowledged without detracting from the long-recognized benefits of multilateral, regional and bilateral trade liberalization.