110 \ Commonwealth Cyber Journal
ISSN 2959-3018 (print), ISSN 2959-3026 (online)
thecommonwealth.org/cyber-journal

The Commonwealth

# The National Security Exception in International Trade and Cybersecurity

Kartikeya Garg[1]

## Abstract

The national security exception is a crucial part of most trade agreements, and has historically protected against traditional attacks to states' security. However, over time, threats to national security have evolved, to include, among other things, cyberthreats. Article XXI of the General Agreement on Tariffs and Trade, first interpreted by the World Trade Organization's *Russia–Traffic in Transit Panel Report* in 2019, has led to many debates regarding the scope of the provision and its application to cyberthreats.

This article discusses the plausibility of including state-imposed cybersecurity measures within the ambit of this interpretation of Article XXI. Apart from this provision, various Free Trade Agreements (FTAs) have incorporated different formulations of the security exception. This article analyses four main formulations of the exception in various FTAs and discusses the best option to include cybersecurity measures within their ambit, without leaving too broad of a scope to allow misuse. It recommends a balance between an explicit reference to cybersecurity measures and an emphasis on the principle of good faith as an effective check to ensure the balance between trade and cybersecurity is met.

**Keywords: national security, Article XXI, cybersecurity, exception**

## Introduction: Trade, national security and cybersecurity

National security exceptions have formed a crucial part of multilateral trade agreements since the advent of international trade regulation. Given the sensitive nature of the issues at hand, states have rightly valued the security of their territory and their citizens

1 International Trade Policy section, Trade, Oceans and Natural Resources Directorate, Commonwealth Secretariat. Email: k.garg@commonwealth.int; kartikeya.garg@graduateinstitute.ch.

more than the economic benefits that they might derive from international trade.[2] It is for this reason that national security exceptions have been codified not just in World Trade Organization (WTO) Agreements but also in more than 290 regional and preferential trade agreements.[3] However, a perusal of these national security exceptions shows that they were originally drafted taking into consideration only military threats to national security.

In the past two decades, however, cybersecurity has become an increasingly important component of national security,[4] which, according to various lawmakers, requires special policy considerations. These rules in cybersecurity, mostly formulated as a part of domestic policy, cover, among other things, the restriction of cross-border data flows, transactions involving sensitive personal data and the imposition of technical and regulatory standards.[5] However, crucially, despite these innovative rules, there is still considerable ambiguity at the multilateral level on the question of *whether and when cybersecurity concerns should override the demands of trade liberalisation (or vice versa)*.[6]

The global expansion of the internet and increased data flows between businesses and consumers around the world, for e-commerce, for communication and as a source of information, has meant that international trade and cybersecurity are becoming increasingly intertwined. Digital connectivity has therefore transformed international trade and accelerated the global connectivity of businesses, governments and cross-border supply chains.

The interaction between trade and cybersecurity measures can take various forms, with the trading regime having to deal with various kinds of cyberthreats, each suggesting a different response.[7] Broadly, these threats have been classified to include the following: intrusions into military or defence systems; cyberattacks on critical public infrastructure; economic cyber-espionage aimed at stealing intellectual property (IP) and trade secrets; and the manipulation of digital information to create distrust.[8] Also, many cybersecurity measures are likely to restrict cross-border data flows and digital trade, including through data localisation requirements and import restrictions on data and digital products.

While threats to national security have been evolving over time, the national security exception has, for almost 70 years, been treated as a Pandora's box, owing to the highly

2 Van den Bossche, P.L.H. (2020) 'The National Security Exception in International Trade Law Today: Can We Avoid Abuse?', in *Association 'Commercial Law', Pre-Advice 2020: Review of Foreign Investment in Geopolitical and Legal Perspective*, pp. 111–143.

3 Dür, A., Baccini, L. and Elsig, M. (2014) 'The Design of International Trade Agreements: Introducing a New Database', *Review of International Organizations* 9(3): pp. 353–375.

4 Government of the United States of America (2015) *National Security Strategy.*

5 OECD (2009) *Security-Related Terms in International Investment Law and in National Security Strategies*. Paris: OECD.

6 Benton Heath, J. (2020) '*The New National Security Challenge to the Economic Order'*, Yale Law Journal 129: pp. 1020–1098.

7 Ibid.

8 Government of the People's Republic of China (2015) *National Security Law of the People's Republic of China.*

sensitive nature of the provision and the immense scope for misuse.[9] According to various trade officials and policy-makers, states can use the provision as an easy outlet to flout their trade obligations and protect their domestic industry, which could be immensely harmful to the multilateral trading system.[10] At the same time, the provision must not be so rigid as to prevent states from imposing measures to protect their national security from evolving threats, such as cyberattacks.

These are thus two sides of the same coin: while expanding the scope of the national security exception could lead to widespread misuse and hamper international trade, narrowing the scope of the provision to exclude its application for evolving threats to national security could prove highly disadvantageous to states, and would ultimately go against the very purpose of the provision. It thus becomes vital to determine whether such a balance between trade and evolving national security threats exists – and, if not, if it *can* exist, in order to create a situation where states can use the national security exception to implement measures to protect against cyberthreats but at the same time ensure that misuse is prevented.

In this regard, this article seeks to assess the various formulations of the national security exception in international trade law and attempts to determine whether any of these formulations achieve the cybersecurity/trade balance discussed above. First, the article analyses the national security exception under the WTO and attempts to determine whether it can be interpreted broadly to include measures to protect against cyberthreats. It then identifies four different formulations of the exception in various modern Free Trade Agreements (FTAs) and discusses whether any of these formulations are better suited to include evolving threats to national security within their ambit. The article concludes by recommending the formulation that is the most appropriate to combat cyberthreats and suggests a change in its interpretation to prevent misuse.

## 1. The national security exception under the WTO

The national security exception under the WTO is codified under Article XXI of the General Agreement on Tariffs and Trade (GATT). This provision is also found under Article XIV bis and Article 73, respectively, of the General Agreement on Trade in Services and the Agreement on Trade-Related Aspects of Intellectual Property Rights (the TRIPS) *mutatis mutandis.*

The provision reads:

> *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*

9 Van den Bossche (2020), p. 114.
10 Ibid., p. 115.

(b) *to prevent any contracting party 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 contracting party from taking any action in pursuance of its obligations under the United Nations Charter for the maintenance of international peace and security.*[11] (Emphasis added.)

Among these clauses, subparagraphs (a), (b)(i) and (c) have never been invoked and challenged before the WTO,[12] while subparagraph (b)(ii) has been invoked only once, in the first GATT case[13] dealing with national security exceptions. States therefore rely solely on Article XXI subparagraph (b)(iii), in order to take advantage of its '*controversial and ambiguous wording*.'[14]

## 1.1 The current interpretation of Article XXI according to the WTO Panel

Article XXI(b)(iii) was for the first time comprehensively analysed by the WTO Panel in the *Russia–Traffic in Transit* case.[15] It was subsequently referred to in a case brought about under Article 73 of the TRIPS, in *Saudi Arabia–IP*.[16] The Panel's landmark interpretation in *Russia–Traffic in Transit* has been widely debated, and has also opened the door for many more cases raising the defence of Article XXI. The Panel analysed the provision in two main parts: (i) determining whether Article XXI(b) is self-judging or not and (ii) understanding the scope of Article XXI(b) as well as Article XXI(b)(iii). This article does not focus on the Panel's interpretation regarding the self-judging nature of the provision, and also does not discuss the facts of these cases. Rather, it deals only with the interpretation of the terms of the chapeau of Article XXI(b), as well as the specific conditions laid down under clause (iii).

11 GATT Art. XXI, 1994.
12 Yoo, J.Y. and Ahn, D. (2016) 'Security Exceptions in the WTO System: Bridge or Bottle-Neck for Trade and Security?' *Journal of International Economic Law* 19(2): pp. 417–444.
13 Article XXI – United States Export Restrictions GD/4, Decision of 8 June 1949.
14 Yoo and Ahn (2016), p. 427.
15 WTO (2019) 'Panel Report, Russia – Measures Concerning Traffic in Transit'. WTO Doc. WT/DS512/R, 5 April.
16 WTO (2020) 'Panel Report, Saudi Arabia – Measures Concerning the Protection of Intellectual Property Rights'. WTO Doc. WT/DS567/R, 16 June.

1. *The chapeau of Article XXI(b): 'any action which it considers necessary for the protection of its essential security interests'*

The first question before the Panel in this regard was whether the phrase '*which it considers*' allows Members to determine on their own their essential security interests as well as the necessity of the measures to protect them; or only the necessity of the measures.[17] Russia argued that the entire provision was self-judging and that both determinations were left entirely to the discretion of the Member, whereas Ukraine contended that it was for the Panel to interpret '*essential security interests*' while applying customary treaty interpretation rules under public international law.[18]

The Panel agreed with the proposed interpretation of Ukraine and attempted to define '*essential security interests*.' Differentiating the term from '*security interests*,' it explicitly qualified the term to mean those relating to *'quintessential functions of the state, namely, the protection from external threats, and the maintenance of law and public order internally.'*[19] It thus expressly provided two functions of the state, the protection of which would fall under the ambit of '*essential*' under Article XXI(b). Despite this rather specific interpretation, the Panel did consider that specific interests that Members sought to protect under this provision would vary depending on situations and changing circumstances.[20]

Therefore, despite initially defining the term rather narrowly, the Panel conferred some discretion to Members to choose what constitutes an essential security interest. However, this discretion was further qualified by the Panel as it obliged Members to exercise this determination keeping in mind the general principle of good faith.

2. *The inherent good faith obligation on Members*

The Panel interpreted that Members had an inherent obligation of good faith when declaring what constituted an essential security interest that needed protection under Article XXI. This obligation is two-fold: (i) Members should not use the provision as a disguise in order to use increasingly protectionist measures; and (ii) there should be a logical link between the essential security interest and the measure imposed by the Member.

The Panel illustrated the first good faith obligation by describing a situation where the invoking Member would seek to evade obligations inherent in the multilateral trading regime, built on principles of non-discrimination, by merely classifying trade interests as '*essential security interests*' falling within the exception. In order to prevent Members from using Article XXI to circumvent obligations under the GATT, the Panel required Members to articulate their essential security interests in such a way that they are '*sufficiently enough to demonstrate their veracity.*'[21]

17 WTO (2019) 'Panel Report, Russia', para. 7.128.
18 Ibid., para. 7.129.
19 Ibid., para. 7.130.
20 Ibid., para. 7.131.
21 Ibid., para. 7.134.

The Panel went on to provide guidelines on what could constitute such 'sufficiency' in articulation by a Member. This would depend on the nature of the '*emergency in international relations*' requiring the imposition of the measure. For more serious emergencies in international relations, the requirement for the Member to sufficiently articulate is less stringent, since essential security interests in these cases would be far more evident. However, for emergencies that are less serious – that is, where defence or military interests, or maintenance of law and public order interests, are not as evident – the obligation to sufficiently articulate to the Panel is enhanced.[22]

The second good faith obligation requires that Members clearly establish the connection between the essential security interest they seek to be protected and the measure actually imposed. In other words, the measure must '*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.*'[23] As per the facts of the case, since all measures that Russia had imposed attempted to prevent the transit of goods from the Ukraine–Russia border, and considering that there was a situation of armed conflict between the two countries as recognised by the United Nations General Assembly,[24] the Panel concluded that the measures met the minimum requirement of plausibility.

*3. Article XXI(b)(iii): In time of war or other emergency in international relations*

The Panel defines '*emergency in international relations*' to include four specific situations: armed conflict; latent armed conflict; a heightened tension or crisis; or of general instability engulfing or surrounding a state.[25] Mere political and economic differences are insufficient to constitute such an emergency.[26] Accordingly, Russia identified various factors that proved that there did in fact exist such an emergency between itself and Ukraine: (i) that the time period during which the emergency arose continued to exist; (ii) that Ukraine was involved; (iii) that it affected the security of the Russia–Ukraine border; (iv) that other countries had imposed sanctions on Russia resultantly; and (v) that the entire situation was publicly known.[27]

The Panel deemed these reasons sufficient to enable a conclusion that there did exist a situation of emergency in international relations in the case. The Panel interpreted the term '*war*' to mean '*armed attack*'[28] and did not analyse it further, presumably because the WTO was not designed as a body for the resolution of conflicts such as wars, insurrections and unrests.[29]

22 Ibid., para. 7.135.
23 Ibid., para. 7.138.
24 Ibid., para. 7.145.
25 Ibid., para. 7.111.
26 Ibid., para. 7.74.
27 Ibid., para. 7.119.
28 Ibid.
29 Ibid., para. 7.112.

## 1.2 The current interpretation being sufficient to combat evolving threats to national security?

The term '*essential security interests*' was the subject of intense debate during the Preparatory Sessions of the GATT. The purpose of Article XXI, according to the drafters, was to create a balancing act between genuine security interests that warrant protection and to prevent Members from adopting excessively protectionist measures.[30] The only way this balance and the prevention of abuse can be guaranteed is through the '*spirit in which Members would interpret these provisions*.'[31] The Panel attempted to reach this balance by amalgamating the '*deferent standard of review*' provided by the chapeau of Article XXI(b) and the stricter '*objective analysis*' envisaged by subparagraphs (i) to (iii).[32] Thus, although states are allowed to determine their own national security interests as they deem fit, such absolute deference would prevent states from justifying or notifying the imposition of any such trade-restrictive national security measure,[33] and would seriously impair the objectives sought to be achieved by the global trade system.[34]

The Panel thus concluded that most elements of Article XXI(b) required an objective standard of review,[35] including an assessment on whether a measure first concerns an essential security interest and then falls under one of the specified subparagraphs. However, this would generally not be a problem for panels, because traditional security issues would be objectively identifiable. It would be very difficult for governments to disguise protectionist measures as claims of national security.[36]

This position changes, however, when we discuss evolving threats to national security, such as claims regarding cybersecurity. Since cybersecurity policies are more risk-based and generally require long-term adoption,[37] it is necessary to ascertain whether the current interpretation of Article XXI(b) allows for states to take measures they deem necessary to protect themselves against evolving cybersecurity threats, or whether it restricts the scope of the provision to only traditional notions of security. The current interpretation of the provision from the Panel illustrates two possible options.

30 WTO Article XXI: Security Exceptions.
31 Ibid.
32 Blanco, S. and Pehl, A. (2020) *National Security Exceptions in International Trade and Investment Agreements: Justiciability and Standards of Review*. Springer, p. 24.
33 Bhala, R. (1998) *International Trade Law: Theory and Practice*. Second Edition. New York: LexisNexis.
34 WTO (nd) 'Principles of the Trading System'. www.wto.org/english/thewto_e/whatis_e/tif_e/fact2_e.htm
35 Blanco and Pehl (2020).
36 Meltzer, J.P. (2020) *Cybersecurity, Digital Trade and Data Flows: Re-thinking a Role for International Trade Rules*. Working Paper 123. Washington, DC: The Brookings Institution (2020).
37 Ibid.

1. *Cybersecurity measures falling within the ambit of Article XXI(b)?*

Because of the changing character of threats to peace and security and increasing issues of cybersecurity,[38] it becomes crucial to determine whether a dynamic interpretative approach could be used to allow such evolving notions of security threats into the ambit of Article XXI. Interpreting the WTO provisions in light of these contemporary developments, however, does not '*subsume completely different or novel meanings and concepts under their notions*.'[39] This dynamic interpretation is in contrast to an '*overall expansive approach that would subsume all sorts of novel security allegations under Article XXI, irrespective of its boundaries*.'[40]

Although the Panel determined that Article XXI was not wholly self-judging,[41] it still gave states the freedom to articulate their own '*essential security interest'* and noted that, as long as states could sufficiently link this interest to the adopted measure, panels would not hesitate to allow the application of the provision.[42] However, establishing this 'plausible link' may be difficult for states in practice since security vulnerabilities in digital systems are still not known.[43] Nonetheless, if it can be demonstrated, it may be possible for states to avail the exception under any of the three subparagraphs under Article XXI(b).

States have been increasingly digitising their militaries, making them more vulnerable to cyberattacks.[44] Members could justify the imposition of cybersecurity measures to prevent cyberthreats to their nuclear or military facilities under Articles XII(b)(i) and (ii).[45] Since military threats have themselves evolved, the concept of arms used and potentially covered by Article XXI(b)(ii) could also evolve to include measures as necessary for such conflicts.[46] Since combating cyberwarfare would require different goods, it can be argued that Article (b)(ii) could be interpreted in light of these contemporary national security concerns.

However, the exception most suited to expanding the provision to cybersecurity measures is Article (b)(iii). This view emphasises the enhanced discretion that states are conferred under the exception, holding that it provides '*almost no limits*' on governments in justifying

38 Weiß, W. (2008) 'Security Council Powers and the Exigencies of Justice after War'. *Max Planck Yearbook of UN Law*, 1 January.
39 Weiß, W. (2020) 'Interpreting Essential Security Exceptions in WTO Law in View of Economic Security Interests'. *Global Politics and EU Trade Policy, European Yearbook of International Economic Law*, p. 267.
40 Ibid.
41 WTO (2019) 'Panel Report, Russia'.
42 Meltzer (2020).
43 Mishra, N. (2020) 'The Trade: (Cyber)Security Dilemma and Its Impact on Global Cybersecurity Governance', *Journal of World Trade* 54(4): 567–590.
44 Delcker, J. (2027) 'Digitizing Military Will Cost Europe Up to €41 Billion Per Year: Study'. Politico, 23 November. www.politico.eu/article/digitizing-military-will-cost-europe-up-to-e41-billion-per-year-study/
45 Mishra (2020).
46 Weiß (2008).

their security measure.[47] This discretion, coupled with the fact that the Panel interpreted '*emergency in international relations*' expansively to include not just defence and military concerns but also the '*maintenance of law and public order,*'[48] implies that cybersecurity measures could, in fact, be included within the scope of Article XXI(b)(iii). In other words, as long as Members are able to sufficiently articulate their '*essential security interests*' and the 'plausible link' to the cybersecurity measure, panels could be willing to accept the claim that cybersecurity measures are necessary to protect their essential security interests.[49]

For example, a state may impose a ban on foreign digital services during an armed attack in order to minimise risks of cyberattacks.[50] Once a state shows that it does in fact face an emergency in international relations, it can argue that cybersecurity measures were imposed to prevent cyberthreats to critical infrastructure underlying public utility claims,[51] which constitutes an 'essential security interest.' If this measure is analysed using the lens of this broad interpretation, panels might be inclined to allow it as a national security exception under Article XXI(b)(iii).

As the Panel concluded in *Russia–Traffic in Transit*, the onus is on the invoking state to sufficiently articulate its essential security interests. However, this articulation becomes problematic if the state invokes Article XXI(a), since this allows states to refrain from providing information that could hamper its essential security interests. The absence of subparagraphs and qualifiers for this clause implies that it is of a more self-judging nature than Article XXI(b). Therefore, if a state uses Article XXI(a) to justify its non-articulation of its essential security interest, the Panel would not be able to do much in response.[52] This is even more the case if the information that ought to be disclosed is highly confidential, or is limited, which might be the case for an emergency relating to cybersecurity.[53] Thus, states could argue that, by invoking Article XXI(a), they would not be required to provide substantive evidence regarding the 'plausible link' between the cybersecurity measure and its essential security interest, which could relate to the protection of its cyberinfrastructure.[54]

Additionally, the temporal requirement that the measure be taken '*in time of*' an emergency in international relations could potentially extend to '*time-unlimited cybersecurity measures,*'[55] given the uncertain nature of cyberattacks. In this situation, scope for misuse by Members is tackled by the good faith obligation inherent in Article XXI.

47 Benton Heath (2020).
48 WTO (2019) 'Panel Report, Russia'.
49 Meltzer (2020).
50 Mishra (2020).
51 Ibid.
52 Van den Bossche (2019).
53 Ibid.
54 Voon, T. and Mitchell, A. (2019) 'Australia's Huawei Ban Raises Difficult Questions for the WTO'. EastAsia Forum, 22 April. https://eastasiaforum.org/2019/04/22/australias-huawei-ban-raises-difficult-questions-for-the-wto/
55 Benton Heath (2020).

These are thus the various arguments raised in favour of a broad reading of Article XXI to include measures taken to protect cybersecurity based on the interpretation of the Panel.

*2. Cybersecurity measures falling outside the scope of Article XXI(b)?*

The first problem created by using a broader understanding of the Article XXI interpretation is that it would contradict the intention of the drafters of the provision. In order to prevent the use of the exception to '*permit anything under the sun*,'[56] it was reasoned that the provision should be drafted in a way that '*would take care of real essential security interests and, at the same time, so far as we could, limit the exception so as to prevent the adoption of protection of industries under every conceivable circumstance*.'[57] The wording of Article XXI, as well as the Panel's interpretation that the provision is not entirely self-judging and is therefore subject to an objective standard of review, implies that a broad interpretation is not possible, and it is difficult to include non-traditional notions of security under the provision.

This is more the case given the Panel's definitions of '*war*' and '*emergency in international relations,*' where it discusses traditional notions of security threats that are easily identifiable and objectively discernible. However, when it comes to cyberwarfare or cyberthreats, this is not the case. Thus, even though a Member could classify a cybersecurity measure as one protecting an '*essential security interest,*' it will be difficult for panels to assess when the cyberthreat is grave enough to justify a measure under Article XXI.[58] Further, given that cyberthreats can be characterised into various kinds of security threats (military, political or even commercial), panels would require substantial evidence to assess whether the cybersecurity measure is actually imposed in order to contain an 'emergency in international relations' under Article XXI(b)(iii). For example, a systematic theft of trade secrets of digital companies would not, according to the Panel's interpretation in *Russia–Traffic in Transit*, constitute a situation of '*war*' or '*emergency in international relations.*'[59]

This difficulty also exists when assessing an imminent cyberthreat, whereby panels would have to determine whether the cyberthreat constituted as much of a threat as an armed attack. This is because the industry surrounding cyberwarfare and cyberweapons is highly dynamic and uncertain, making it impossible to predict the nature and intensity of cyberthreats.[60] Therefore, if Members, while acting in good faith, believe there exists a legitimate basis for imposing cybersecurity measures, it will be difficult to prove to panels the necessity of such measures owing to a lack of evidence.[61]

56 Weiß (2008).
57 Ibid.
58 Mishra (2020).
59 Ibid.
60 Mishra (2020).
61 Ibid.

The biggest problem with the inclusion of cybersecurity measures within Article XXI relates to the Panel's interpretation of the temporal requirement provided under Article XXI(b)(iii). By requiring that the measure be taken during the time of the emergency in international relations, the Panel seemed to exclude many 'risk-based' cybersecurity measures from its scope. Since cyberthreats are of such a nature that they may arise from any country with an internet connection, the nature of the risk is such that the only way it can be truly neutralised is if states adopt continuous cybersecurity measures, irrespective of the existence of an emergency in international relations or not.[62]

Therefore, although in theory Article XXI(b)(iii) could be applied to cybersecurity measures that are taken during the specified period of time of 'war or emergency in international relations,' in practice, since cyber-related emergencies are permanent and long in term rather than timebound, and given that they can originate anywhere, it would be rare for such measures to fall under the ambit of Article XXI.[63]

Thus, although Article XXI could possibly be interpreted broadly to include cybersecurity measures, this claim would be difficult to prove, for the reasons explained above. Nonetheless, both the narrow and the broad interpretations lead to the same outcome – that is, a *'lack of an effective governance mechanism to mediate cybersecurity/trade tradeoffs*.'[64]

## 2. Alternate formulations of the national security exception in FTAs

Despite the various economic and technological developments that have led to evolving threats to national security, there have been no amendments to the text of Article XXI since it was first formulated in 1947.[65] Even in the post-WTO era, with the increase in the number of FTAs between states, little or no attention has been paid to the national security exception. In fact, multiple FTAs do not even contain security exceptions.[66]

This article identifies four different kinds of formulations of the national security exception commonly found in FTAs, and attempts to analyse whether any of these variations are better equipped to cover cybersecurity measures imposed by states. These formulations include the incorporation of Article XXI GATT **(A)**; incorporating the national security exception as part of the General Exceptions **(B)**; formulating a wholly 'self-judging' national security exception **(C)**; and an explicit clause allowing for the imposition of certain cybersecurity measures **(D)**.

62 Meltzer (2020).
63 Benton Heath (2020).
64 Meltzer (2020).
65 Yoo and Ahn (2016).
66 Korea–EU Free Trade Agreement; Korea–India Free Trade Agreement.

## 2.1 The incorporation of Article XXI GATT

Despite the various debates concerning the interpretation of Article XXI as discussed in the previous section, this formulation has been the most prevalent form of security exceptions in FTAs.[67] This formulation can take two forms.

1. *Directly transposing Article XXI into FTAs*

Many FTAs incorporate the provision as it stands, without any modification;[68] however, a few make minor changes to the language of the provision, especially with respect to that in Article XXI(b)(iii). For instance, many FTAs replace the terms 'in time of war or emergency in international relations' with terms such as '*serious internal disturbances affecting the maintenance of law and order, in time of war or serious international tension constituting threat of war*.'[69] In some cases, the term 'emergency in international relations' is replaced by '*serious international tension*'[70] or '*extraordinary circumstances in international relations*.'[71]

This can be interpreted as either broadening or widening the scope of the provision based on the same interpretation given by the Panel in Russia–Traffic in Transit. In other words, this formulation faces the same issues that Article XXI does. It allows states the discretion to determine what constitutes an essential security interest and sufficiently articulate that the measure has been taken in good faith to protect the same. According to the dictionary, the term '*emergency*' refers to a '*serious situation that occurs suddenly or unexpectedly and requires urgent attention*,'[72] which has a much narrower scope than the term '*serious.*'

Thus, it would seem more likely that states will justify the imposition of cybersecurity measures under the broader ambit of '*serious international tension.*' However, despite this possible additional leeway the provision gives to include measures other than those to protect traditional security concerns, the temporal requirement remains the same as under Article XXI(b)(iii), which severely restricts the scope of the provision to include long-term cybersecurity measures.

2. *Reference to abide by GATT provisions*

Multiple FTAs contain provisions that do not explicitly mention a national security exception; rather, they refer directly to the provisions of the GATT. For instance, they can take the form of the following:

67 Yoo and Ahn (2016).
68 EU–UK Trade and Cooperation Agreement 2020, Article EXC:4; Agreement Establishing the African Continental Free Trade Area 2018, Article 27.
69 Agreement on the European Economic Area 1994, Article 123.
70 Economic Cooperation Organization Trade Agreement 2008, Article 15/B.
71 Free Trade Agreement between Azerbaijan, Armenia, Belarus, Georgia, Moldova, Kazakhstan, The Russian Federation, Ukraine, Uzbekistan, Tajikistan and the Kyrgyz Republic Agreement on the Creation of a Free-Trade Area, Exceptions for the Reasons of Safety 1994.
72 Cambridge Dictionary, Fourth Edition.

> *For the purposes of this Chapter, the rights and obligations of the Parties in respect of Security Exceptions shall be governed by Article XXI of the GATT 1994, which is hereby incorporated into and made part of this Agreement, mutatis mutandis.*[73] (Emphasis added.)

This sort of provision prevents any further interpretation of the national security exception under the FTA, since it allows for the application of Article XXI as it stands. It therefore directly binds states under the interpretation of the provision given by the Panel in *Russia–Traffic in Transit*. Reference to GATT national security exceptions in this manner can be either explicit, as in the formulation mentioned above, specifying the *mutatis mutandis* incorporation of Article XXI, or implied, in the following way:

> *No provision in this Agreement shall be interpreted to prevent either Party from adopting or maintaining exception measures consistent with the rules of the World Trade Organization.*[74](Emphasis added.)

This leaves Members with no room to interpret Article XXI differently and expansively to include cybersecurity measures. They must satisfy the same conditions that the Panel imposed.

## 2.2 Incorporating the national security exception as a part of the General Exceptions

The first drafts of the International Trade Organization Charter did not contain a separate provision for security exceptions, with the current set of exceptions under Article XXI being listed as separate items in parallel with other clauses of the General Exceptions provision.[75] It was only much later, at the final stage of negotiations in 1947, that the security provisions were divided completely from the General Exceptions.[76] Despite this separation, various FTAs have incorporated the national security exception as one of the clauses in its General Exceptions provision, which often mirrors Article XX GATT. These can take the form of the following:

> *Member States during the mutual trade of goods may apply restrictions (subject to the fact that these measures do not serve as unjustifiable discrimination or covered restriction on trade), if such restrictions are necessary for: 1) protection of human life and health;... 6) the defense and security of the Member state.*[77] (Emphasis added.)

The incorporation of security exceptions into General Exceptions chapters could either be in the form of a general reference to 'security of a state' as mentioned above or

73 EU-Peru Free Trade Agreement 2010, Article 2.20.
74 Cross-Straits Economic Cooperation Framework Agreement 2010, Article 9.
75 Yoo and Ahn (2016).
76 Ibid.
77 Treaty on the Eurasian Economic Union 2015, Article 29.

be specific to certain situations for which cybersecurity measures would be allowed. For example:

> *For the purposes of the following chapters… subject to the requirement that measures are not applied in a manner that would constitute a means of arbitrary or unjustifiable discrimination between parties… or a disguised restriction on trade…, nothing in this Agreement shall be construed to prevent the adoption or enforcement by a Party of measures necessary: a) to protect public security or public morals or maintain public order;… c) to secure compliance with laws or regulations which are not inconsistent with provisions of this Agreement including those relating to:… ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts;…*[78] (Emphasis added.)

Incorporating the national security exemptions into the General Exceptions could serve to be advantageous to Members because WTO panels have in various instances already given Article XX clauses extremely broad interpretations, taking into consideration contemporary circumstances to include within its ambit different sets of domestic policy objectives.[79] For example, at the time of drafting Article XX(g), the term 'exhaustible natural resources' was thought to be limited to 'stock resources of raw materials or minerals.'[80] The Panel, however, interpreted the term broadly to also include 'fresh air or endangered species.'[81]

This was also the case in *US–Gambling*, where the Panel found that a regulation preventing underage gambling fell within the scope of Article XX(a) as a measure to protect public morals or public order.[82] In the same case, it was decided that Members were empowered under the provision to decide for themselves the content of 'public morals' and 'public order' according to '*their own systems and scales of values*' and that this would vary according to the '*prevailing social, cultural, ethical and religious*' values and concepts of Members.[83]

These examples are encouraging for Members in the sense that they can adopt cybersecurity policies in light of the security exception clause provided for under the General Exceptions, with considerably less backlash from dispute settlement bodies. This is because, although the clauses of Article XX are often interpreted broadly, its chapeau is interpreted very narrowly, in the form of a final litmus test,[84] in order to prevent misuse

78 EU–Canada Comprehensive Economic and Trade Agreement 2014, Article 28.3.
79 Weiß (2008).
80 WTO (2001) 'Appellate Body Report: United States–Import Prohibition of Certain Shrimp and Shrimp Products'. WTO Doc. WT/DS58/23, 21 November.
81 Ibid.
82 WTO (2015) 'Appellate Body Report: United States–Measures Affecting the Cross-Border Supply of Gambling and Betting Services'. WTO Doc. WT/DS285/AB/R, para. 299, 20 April.
83 WTO (2006) 'Panel Report: United States–Measures Affecting the Cross-Border Supply of Gambling and Betting Services'. WTO Doc. WT/DS285/R, para. 6.461, 20 April.
84 Weiß, W. (2019) *WTO Law and Domestic Regulation*. Beck Hart Nomos Publishing.

of the provisions.[85] In other words, the expansive interpretation of the clauses and the limiting effect intended by the chapeau must be seen as 'counteracting movements' and must be analysed together to enable a thorough understanding of the balanced approach sought by the provision to allow Members to pursue domestic policies.[86]

It is precisely this point that differentiates Articles XX and XXI, and this may also be the reason states choose to include national security measures as part of the General Exceptions. Article XXI does not contain a chapeau like in Article XX that can act as a balance to wider interpretations that may be conferred to the clauses under it. Therefore, widely expansive constructions to clauses under Article XXI in the same manner as in Article XX would seem unlikely, as this would lead to immense misuse.[87] Thus, *prima facie*, it seems that this formulation could be the most beneficial for states in implementing cybersecurity measures in order to combat evolving threats to national security.

However, including national security exceptions as part of General Exceptions can be problematic for various reasons. First, this formulation goes against the very reason General Exceptions and security exceptions were split into two different provisions. It was reasoned at the time that the chapeau of Article XX was too constraining, and that, for emergency measures to be taken during military conflicts, a wider basis would be needed.[88] However, at the same time, the formulations in these FTAs give states too much discretion, taking away the qualifiers specified under Article XXI, such as the need to articulate an 'essential security interest,' as well as the conditions specified under Article XXI(b). Having such a broad formulation removes the balance that the framers of the GATT sought, and leaves the provision open to immense abuse. This is also therefore not a very common formulation in FTAs.

## 2.3 A wholly 'self-judging' national security exception

The most common argument raised by Members invoking Article XXI is that the provision is entirely self-judging, and the WTO Panel therefore has no jurisdiction over it.[89] The Panel in *Russia–Traffic in Transit*, however, much to the discontent of invoking Members, ruled that the exception was not 'wholly self-judging'[90] and that, although the chapeau of Article XXI(b) allows for some measure of discretion, its subparagraphs acted as qualifiers. However, various FTAs, given the interests of many developed countries,

85 WTO (2001) 'Appellate Body Report: United States–Import Prohibition of Certain Shrimp and Shrimp Products'.
86 WTO (2015) 'Appellate Body Report: United States–Measures Affecting the Cross-Border Supply of Gambling and Betting Services'.
87 Weiß (2008).
88 Yoo and Ahn (2016).
89 U.S. First Written Submission 2019, 'US–Certain Measures on Steel and Aluminum Products' (DS548).
90 WTO (2019) 'Panel Report, Russia'.

intentionally broaden this discretion and arbitrariness of security exception clauses.[91] This could be in the form of the following:

> *Nothing in this Agreement shall be construed to:... (b) 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 or security, or the protection of its own essential security interests.*[92](Emphasis added.)

This formulation removes the qualifying conditions specified under Article XXI(b), limiting the provision to only its chapeau. As a result, it bypasses the Panel's interpretation and makes the provision wholly self-judging. In other words, as a result of this provision, states not only would be free to classify any interest they deem fit as an 'essential security interest' but also would have the discretion to adopt any measure they deem necessary in order to protect their interest. This unfettered discretion would naturally allow states to impose cybersecurity measures even if the term 'essential security interests' is conferred with the same meaning as that given by WTO panels.

It would be conceivable for states to argue that cybersecurity measures have been imposed for the protection of the state from 'external threats' as well as for the 'maintenance of law and public order.'[93] However, the absence of the qualifying subparagraphs mentioned in Article XXI(b) leaves states with a large amount of discretion and, consequently, the scope for misuse. A wholly self-judging provision also has the effect that an affected state would have no recourse to a dispute settlement body, since this latter would not have jurisdiction over this clause. This formulation therefore also fails to strike the balance between trade and evolving security concerns.

## 2.4 Explicit inclusion of cybersecurity measures

The last formulation in FTAs is a fairly recent phenomenon. As many states have begun to recognise the evolving nature of security concerns, they have understood the need to protect their interests from cyberthreats and have incorporated a specific clause in their security exception provisions to that effect. These provisions largely mirror Article XXI, merely adding an additional subparagraph under Article XXI(b). For instance, many FTAs incorporate the following clause:

> *Nothing in this Agreement shall be construed... (b) to prevent any Party from taking any action which it considers necessary for the protection of its essential security interests... (iii) taken so as to protect critical public infrastructures including communications, power, and water infrastructures...*[94](Emphasis added.)

91 Yoo and Ahn (2016).
92 US–Mexico–Canada Agreement 2020, Article 32.2; Dominican Republic–Central America Free Trade Agreement 2004, Article 21.1.
93 WTO (2019) 'Panel Report, Russia', para. 7.130.
94 Regional Comprehensive Economic Partnership 2020, Article 17.13.

This clause has also been drafted in the following way:

> *Nothing in this Agreement shall be construed… (b) to prevent any Party from taking any action which it considers necessary for the protection of its essential security interests… (iii) taken so as to protect critical public infrastructure including communications, power and water infrastructures from deliberate attempts intended to disable or degrade such infrastructures;…*[95] (Emphasis added.)

This formulation expands the scope of the national security exception by including within its ambit security threats other than traditional military threats. The term 'critical infrastructure' has been defined by various states as 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*'[96] and includes those functions, systems and processes necessary for a country and the daily lives of its people to function,[97] whether publicly or privately owned.[98] As the clause reads, such critical infrastructure includes (but is not limited to) power, communication and water infrastructure; it could also include infrastructure regarding finance, health, food and space.[99] This second formulation increases the scope of the provision by explicitly including 'attempted attacks' as well.

Thus, this formulation recognises not only that protection of these 'critical public infrastructures' can constitute an essential security interest for a state but also that, given the nature of such infrastructure, it can be prone to attacks other than traditional military action, such as cyberthreats. It therefore implies that states may be allowed to impose cybersecurity measures, provided they satisfy the other conditions laid out by the chapeau of the provision and its interpretation by the Panel. States would, therefore, have to articulate with sufficient clarity whether the 'critical public infrastructure' they are seeking to protect by means of the imposition of the cybersecurity measure does in fact constitute an 'essential security interest,' and then whether the measure is actually performing the function it set out to achieve.

An important critique on Article XXI(b)(iii) and why cybersecurity measures fall outside its scope has been the temporal requirement mandated by the provision, requiring that the measure be 'taken in time of war or emergency in international relations.' Since most cybersecurity measures are generally taken as long-term measures without any clear start or end date, it would be difficult for these measures to be valid under Article XXI. This formulation remedies this by removing the temporal requirement altogether. It does

95 Pacific Agreement on Closer Economic Relations Plus 2020, Article 2; Agreement Establishing the ASEAN–Australia–New Zealand Free Trade Area 2009, Chapter 15, Article 2.
96 U.S. Department of Homeland Security (nd) 'Critical Infrastructure Security and Resilience'. www.dhs.gov/topic/critical-infrastructure-security
97 Center for the Protection of National Infrastructure (2021) 'Critical National Infrastructure'. 20 April. www.cpni.gov.uk/critical-national-infrastructure-0
98 WTO (2019) 'Panel Report, Russia', para. 7.130.
99 U.S. Department of Homeland Security (nd) 'Critical Infrastructure Security and Resilience'.

not specify the duration that the measure must be taken for, with the only caveat being the principle of good faith.

Thus, at least *prima facie*, this formulation seems to address concerns of evolving threats of security by allowing states to impose cybersecurity measures. However, these formulations are rather recent, and not many FTAs have included these clauses in their FTAs. Based on this formulation, the US's measures against China's Huawei in early 2020 would, in theory, be accepted as a measure to protect national security but might not be so readily accepted under the Article XXI formulation.

## Conclusion

This article has sought to explain how the multilateral trading regime has to equip itself to deal with completely different notions of security.[100] Among these evolving notions, cybersecurity is one of the most important and pressing issues, with the potential to severely hamper international trade. When the security exception was first formulated, the prevailing thought was that security objectives automatically outweighed the trade concerns of states. Since then, however, the scope of the trade and security nexus has widened,[101] and the security exception has failed to reflect this transition. This is evident in that the exception has not been amended since 1947. Two questions were raised at the start of this article: whether Article XXI as it stands is sufficient to combat the evolving threat of cyberwarfare; and, if not, whether any other formulations in FTAs provide a more viable alternative.

As explained earlier, given the dynamic and rather abstract nature of cybersecurity measures, it would be difficult for states, and consequently the Panel, to explain and approve the measure as protecting an essential security interest; and whether cyberwarfare actually constitutes a situation of 'war or emergency in international relations.' According to the Panel, such articulation would not be necessary if the emergency were objectively identifiable.[102] A step in this direction would be to increase the co-ordination between the WTO and the United Nations Security Council. Bhala recommends the establishment of a joint WTO–Security Council Committee, which could render non-binding opinions on whether the use of sanctions by the Security Council comports with the terms of Article XXI(b).[103]

Further, if there is a Security Council Resolution regarding the existence of a particular international situation, panels will be more likely to accept that this does in fact constitute an 'emergency in international relations.' Thus, the first step would be for the Security Council to recognise the credible threat cyberattacks pose, which it has done, by

100 Yoo and Ahn (2016).
101 Ibid.
102 WTO (2019) 'Panel Report, Russia'.
103 Bhala (1998).

realising the threat posed to states' critical infrastructure by possible cyberattacks from terrorists.[104] However, despite all of these steps, the risk-based long-term nature of cybersecurity measures means that it would be extremely difficult to implement them under Article XXI, thereby pointing to the need for reform and new formulations.

In this regard, we have found that modern FTAs have formulated the exception in four main ways: by making minor modifications to Article XXI; by incorporating the provision as it is; by incorporating it as a part of the General Exceptions provision; or by explicitly incorporating cybersecurity measures. Of these four kinds, the last option seems to be the most appropriate formulation in dealing with evolving concerns of national security in relation to trade. By explicitly allowing for the imposition of cybersecurity measures, it addresses all the concerns raised against the application of Article XXI to evolving security threats. This is why newer FTAs such as the Regional Comprehensive Economic Partnership have chosen to incorporate this form.

The caveat is that the only restriction available against the indiscriminate use of this new formulation is the principle of good faith.[105] The Panel has interpreted the good faith principle under Article XXI to include two specific obligations: sufficiently articulating the essential security interest that is meant to be protected; and demonstrating a plausible link between the measure and the interest. However, the good faith principle is applied differently in the application of Article XX. According to this principle, a state imposing a measure under Article XX must demonstrate that it has been imposed a last resort, and is the only way the specific interest can be protected.[106]

This is also reflected in various countries' domestic cybersecurity policies, recognising the need for closer co-operation, improving information exchange, optimising skills and promoting a common global approach to network and information security issues.[107]

A case can be made that the principle of good faith under Article XXI should also include this interpretation in order to ensure the discretion of states is limited. Since arguments have been made regarding the self-judging character of the provision, the only limitation to this is the principle of good faith, which, therefore, requires stronger clarity.[108] A more coherent understanding of the application of the good faith principle to the latest formulation allowing measures to be imposed to protect 'critical public infrastructure' is the best bet to ensure that the international trading regime can sufficiently combat evolving threats to national security.

104 United Nations Security Council Resolution 2341/2017.
105 Vienna Convention on Law of Treaties 1969, Article 31(1).
106 World Trade Organization (2001) 'Appellate Body Report: United States–Import Prohibition of Certain Shrimp and Shrimp Products'.
107 EU Cybersecurity Act (Regulation 2019/881) 2019; U.S. National Cybersecurity Strategy 2023.
108 Trujillo, E. (2020) 'An Introduction to Trade and National Security: New Concepts of National Security in a Time of Economic Uncertainty'. Symposium on Trade and National Security, 7 February.

## About the author

**Kartikeya Garg** is an Assistant Research Officer working in the International Trade Policy section of the Trade, Oceans and Natural Resources Directorate within the Commonwealth Secretariat. He previously worked at the Trade and Environment Division of the World Trade Organization, and has an LLM in International Law from the Geneva Graduate Institute.