

Internet Regulation and the Invocation of Security Exceptions in the WTO Agreement

Sun Nanxiang*

Abstract: Cyberspace is a virtual/notional environment for information exchange that can promote cross-border trade and investment significantly. In the 21st century, as the Internet penetrates societies ever deeper, e-commerce has gradually become the main form of international trading activities. Arguably, cyberspace is generally subject to the principles of sovereignty and territorial jurisdiction. However, laissez-faire economic practices in cyberspace, without due regulation, may pose a danger to national security, public order and, in general, everyday life. The WTO legal framework is a system of multiple agreements. Any issue may be the subject of provisions of different agreements or different provisions of the same agreement in WTO framework. In contrast to the general exception clause, the security exceptions clause is considered a “gentleman’s provision” and WTO members are committed to avoiding invoking it. However, an analysis of the security exceptions helps to provide a deeper understanding of the method the Internet regulations are applied. Through the analytical framework of the law of treaties, the core issue of the interpretation and application of security exceptions is to determine the “self-judging” nature of the security exceptions, and to define the concepts of “essential security interests” and “emergency in international relations” in a reasonable manner. Specifically, although the security exceptions entitle a member to assert both essential security interests and necessities, the principle of good faith should be followed in the application and interpretation of the clause. According to the law of treaties, cybersecurity may constitute “essential security interests” under Article XXI of GATT 1994, while cybersecurity threats may constitute an “emergency in international relations” under Article XXI of GATT 1994.

Keywords: Cybersecurity, Security Exceptions, Self-judging Clause, Essential Security Interests

I. INTRODUCTION

A famous report of the Organization for Economic Cooperation and Development (OECD) stated that almost all economic and social activities can be performed in cyberspace.¹ Economic growth is driven by many factors, including

* Sun Nanxiang, Associate Professor, Institute of International Law, Chinese Academy of Social Sciences. E-mail: yean35_1@hotmail.com.

¹ Organization for Economic Cooperation and Development, *Guide to Measuring the Information Society*, OECD Publishing, 2011, p. 14.

products, process and organizational innovations based on technological change.² The impact of the Internet on economic growth, to some extent, is comparable to the creation of fuel machines and steam engines. Cyberspace is a virtual/notional environment for information exchange that can promote cross-border trade and investment significantly.

As Rostam J. Neuwirth said, the historical evolution of trade and commerce has been closely entangled in a two-way relationship with the evolution of laws, in which one is inextricably linked to the other and both mutually influence each other.³ Because cyberspace is a virtual, borderless and electronic environment, no one nation can exercise exclusive jurisdiction over the Internet.⁴ In short, all nations in the world coexist in interdependent cyberspace.⁵ In essence, the Internet is inherently a global and international society; therefore, the mechanism to boost digital trade reflects a feature of global public good, which should be governed by international law.⁶ However, in comparison with traditional trading methods, in light of the existing agreements and arrangements in place, there is a lack of direct and clear regulation of e-commerce or digital trade multilaterally, such as in the areas on tariffs, customs and inspection procedures. Thus, it is necessary to explore a comprehensive and efficient global economic governance system on e-commerce and digital trade.

As Robert Uerpmann-Witzack has said, the freedom of internet communication, which is firmly rooted in international human rights law, is at the core of internet freedom, and internet freedom may comprise commercial internet freedoms.⁷ The Internet affects productivity growth.⁸ E-commerce has even become

2 OECD, Broadband and the Economy: Ministerial Background Report, OECD Doc. DSTI/ICCP/IE(2007) 3/FINAL, May, 2007, p. 8.

3 Rostam J. Neuwirth, Global Market Integration and the Creative Economy: The Paradox of Industry Convergence and Regulatory Divergence, *Journal of International Economic Law*, Vol. 18, 2015, p. 22.

4 Sun Nanxiang and Zhang Xiaojun, Games and Cooperation in Virtual Society: An Investigation Based on Data Sovereignty, *Journal of the Pacific*, No. 2, 2015.

5 The classic monograph on international relations "Power and Interdependence" describes the national connection in the information age. See Robert Keohane and Joseph Nye, *Power and Interdependence*, Translated by Men Honghua, Beijing University Press, 2012, pp. 237-295.

6 Gregory Shaffer, International Law and Global Public Goods in a Legal Pluralist World, *European Journal of International Law*, Vol. 23, No. 3, 2012, pp. 670-671.

7 Robert Uerpmann-Witzack, Principles of International Internet Law, *German Law Journal*, Vol. 11, No. 11, 2010, p. 1247.

8 Jonathan L. Zittrain, The Generative Internet, *Harvard Law Review*, Vol. 119, 2006, p. 1976.

the main form of transnational trade in recent times, particularly since the start of the COVID-19 pandemic. To describe but a few examples, cross-border trade activities use information technology to share business messages, modern banking and financial institutions are deeply dependent on electronic communication systems, and even investors request foreign law and regulations via government websites. In general, the positive impact of the Internet on trade can be summarized as follows: the first is that e-commerce technology facilitates smooth flow of services from producers to suppliers to consumers, and makes the supply cheaper; the second is that information transmission and data exchange has become faster and more convenient, which does benefit trade around the globe. Doubtlessly, the creation of the Internet reduces cross-border transaction costs substantially, enhancing the development of international trade.

Consequently, whether international trade law can govern e-commerce activities has become a major question in academia. As Sascha Wunsch-Vincent stated, the WTO has taken several steps to define how the multilateral, rules-based trading system should be applied in the online world, but its work is really just beginning.⁹ Particularly, WTO members implemented the Uruguay Round agreements, which liberalized trade in value-added telecommunications, as well as computer and related services, and guaranteed non-discriminatory access to telecommunication networks in 1995. In 1996, WTO members completed negotiations on the Reference Paper for Basic Telecommunications Services. In 1997, WTO members completed negotiations on the Information Technology Agreement (ITA) to eliminate tariffs on a number of information technology products. In 1998, WTO members agreed to continue their practice of not imposing customs duties on electronic transmissions and established a work programme to examine comprehensively all trade related issues relating to e-commerce. WTO members also launched the Doha Development Agenda in 2001, which includes negotiations that may help to define how the rules-based trading system can be applied to e-commerce, though it has made slow progress in the last 20 years.¹⁰ But it has to be admitted that, with the rise of

⁹ Sascha Wunsch-Vincent, *WTO, E-commerce and Information Technologies, from the Uruguay Round through the Doha Development Agenda*, UN ICT Task Force, 2005, p. 1.

¹⁰ *Ibid.*

e-commerce, the pace of formulating multilateral trading rules on virtual society is also accelerating.

In the 21st century, as the Internet penetrates societies ever deeper, e-commerce has gradually become the main form of international trading activities. According to Anupam Chander, the electronic Silk Road winds its way through undersea fiber optic cables and satellite links, ferrying electrons brimming with information. This modern Silk Road makes possible trade in services previously impossible in human history.¹¹ As per classical economics, a free and open trading system enables more goods and services to reach domestic consumers at lower prices, thereby substantially improving their standard of living. In this way, e-commerce contributes to economic growth.

However, a free and open trading system in the online world sometimes poses a threat to national security and public interests. For instance, criminals may hack e-commerce technology or information infrastructure for stealing or extorting money. Thus, nearly all governments pass laws for Internet regulation to safeguard their citizens' rights. However, to some extent, these regulations may curb and act as an obstacle to the freedom of commerce over the Internet.

According to the Lotus principle established by the Permanent Court of International Justice in 1927, international law governs the relationship between independent states. The rules of law binding upon States, therefore, emanate from their own free will as expressed in conventions or by usages generally accepted as expressing principles of law and established in order to regulate the relations between these co-existing independent communities with a view to the achievement of common aims. Therefore, theoretically, restrictions upon the independence of states cannot be presumed.¹² From this point, national sovereignty is independent, the power to regulate the Internet is independent, and jurisdiction in cyberspace is also equal. In short, cyberspace is generally subject to the principles of sovereignty and jurisdiction.

As the Appellate Body stated clearly in *China — Rare Earths*, all members must undertake the obligations arising from the treaty, but the WTO

11 Anupam Chander, Trade 2.0, *Yale Journal of International Law*, Vol. 34, 2008, p. 281; Anupam Chander, *The Electronic Silk Road: How the Web Binds the World Together in Commerce*, Yale University Press, 2013, pp. 2-16.

12 S.S. *Lotus (France v. Turkey)*, 1927 P.C.I.J. (ser. A) No. 10, September 7, 1927, p. 18.

agreement does not deny the members' individual economic sovereignty.¹³ Taking Internet information regulation as an example, sovereign states have the full power to manage, supervise, and control illegal activities and fake information within their territories. Traditionally, information used to be embodied in tangible objects such as books, newspapers and periodicals, which could be subject to strict territorial jurisdiction. In the online world, Internet communication begins from a fixed location and ends at another fixed location. Currently, filtering technologies can be placed within the information infrastructure to create e-borders.¹⁴ Based on this, governments retain the ability to claim national sovereignty and jurisdiction in cyberspace, though comprehensive supervision of the flow of information is rather difficult and costly from the technological perspective.

Based on the analysis above, this paper attempts to employ the tools of treaty interpretation as the starting point to scrutinize the applicability of WTO rules on e-commerce, and then identify trade barriers in the virtual world, as well as explore a suitable method to balance the interest of free trade against the need for protection of national security.

II. THE JURISPRUDENCE OF NATIONAL SECURITY UNDER THE WTO FRAMEWORK

In the WTO framework, it is not uncommon for one measure to be simultaneously governed by different provisions, or even different agreements. For instance, some commentators had advised that China could invoke the general exceptions in Article XX, as well as the security exceptions in Article XXI, of the GATT 1994, to justify its export restrictions in both the Raw Material and Rare Earths disputes.¹⁵ Arguably, the subject of Internet regulation is closely connected with the ground of national security.

Compared to Article XX of the GATT 1994, Article XXI has always been

13 Appellate Body Report, *China — Measures Related to the Exportation of Rare Earths, Tungsten, and Molybdenum*, WT/DS431/AB/R, August 7, 2014, para. 5.78.

14 Tim Gerlach, *Using Internet Content Filters to Create E-borders to Aid International Choice of Law and Jurisdiction*, *Whittier Law Review*, Vol. 26, 2005, p. 912.

15 Shin-yi Peng, *Cybersecurity Threats and the WTO National Security Exceptions*, *Journal of International Economic Law*, Vol. 18, 2015, pp. 461-462.

assumed to be a sort of “gentlemen’s agreement”.¹⁶ One of the main reasons for this is that WTO members believe that it is necessary to maintain the ambiguity of the security exceptions clause, since the members have not yet been able to determine their respective positions and attitudes towards the different interpretations, particularly if significant factual changes were to occur in the future. Additionally, the ambiguity of the national security exceptions leaves a lot of room for legal interpretations, but the GATT/WTO regime has consistently avoided issuing findings on the merits and, therefore, there is very little jurisprudence that is relevant.¹⁷ It is obvious for national security to be of paramount importance for WTO members. In cyberspace, all nations seek to impose their own internet regulatory measures having consideration for their own respective national security agenda. Therefore, it is necessary to seriously scrutinize the various legal interpretations for application of the security exceptions clause in the WTO agreements.

As Hannes L. Schloemann and Stefan Ohlhoff have said, national security is the Achilles’ heel of international law. Wherever international law is created, the issue of national security gives rise to some sort of loophole, often in the form of an explicit exception on the ground of national security.¹⁸ In the treaty, the inclusion of exceptions on the ground of national security was indicative of formal recognition of state sovereignty and the members’ right to self-protection.¹⁹ Thus, security exceptions are marked as “escape clauses”.²⁰ Article XXI of the GATT 1994, for instance, safeguards member states’ secrets relating to essential security interests, and any necessary action needed to protect essential security interests, as well as any action in pursuance of their obligations under the United Nations Charter for the maintenance of international peace and security.

Articles 31 and 32 of the Vienna Convention on the Law of Treaties, 1969

16 Nathaniel Ahrens, National Security and China’s Information Security Standards: A Report of the CSIS Hills Program on Governance, Center for Strategic and International Studies Report, 2012, p.13.

17 *Supra* n. 15, p. 459.

18 Hannes L. Schloemann and Stefan Ohlhoff, “Constitutionalization” and Dispute Settlement in the WTO: National Security as an Issue of Competence, *American Journal of International Law*, Vol. 93, 1999, p. 426.

19 Andrew Emmerson, Conceptualizing Security Exceptions: Legal Doctrine or Political Excuse? *Journal of International Economic Law*, Vol. 11, No. 1, 2008, p. 135.

20 Michael J. Hahn, Vital Interests and the Law of GATT: An Analysis of GATT’s Security Exception, *Michigan Journal of International Law*, Vol. 12, 1991, p. 591.

(VCLT), are regarded as customary international rules for interpretation of the WTO agreements. According to Articles 31 and 32 of the VCLT, when contemplating the use of security-based measures, WTO members must weigh their essential security interests against potential disruptions to the multilateral trading system. Particularly, members must strike a balance between other members' right of non-intervention in their sovereign territory/jurisdiction and the right to take action in light of necessity, exhaustion of remedies, and keeping in view the least restrictive alternatives.²¹ Hence, the next section of this paper will examine treaty exceptions available on the ground of national security with reference to the above analysis.

In the domain of Internet regulations, a member needs to answer two questions: whether it is “reasonable” to classify cybersecurity as an “essential interest”, and whether a member must “genuinely believe” that regulation of cyberspace is a necessary measure for the protection of its essential security interests.²² The above-mentioned practice and treaty interpretation are relevant in this respect. These being self-judging clauses, members should also practice good faith when applying it. As the Appellate Body has emphasized, an interpreter is not free to adopt a reading that would result in reducing whole clauses or paragraphs of a treaty to redundancy or inutility.²³ In the subsequent section, this paper will analyze the issue of national security and free trade in the context of the Internet.

III. SELF-JUDGING CRITERIA FOR ENSURING CYBERSECURITY IN THE WTO REGIME

With respect to Article XXI of the GATT 1994, Professor Jackson has noted that the language of the Article is “so broad, self-judging, and ambiguous that it obviously can be abused”.²⁴ The ambiguity in the language of the clause for

21 Wesley A. Cann, *Creating Standards of Accountability for the Use of the WTO Security Exception: Reducing the Role of Power-based Relations and Establishing a New Balance between Sovereignty and Multilateral*, *Yale Journal of International Law*, Vol. 26, No. 2, 2001, p. 472.

22 *Supra* n. 15, p. 468.

23 Appellate Body Report, *US — Gasoline*, WT/DS2/AB/R, p. 23.

24 John H. Jackson, *The World Trading System: Law and Policy of International Economic Relations*, Massachusetts Institute of Technology Press, 1997, p. 230.

security exceptions is so significant that it also poses a problem in its interpretation and application. In the following paragraphs, this paper attempts to explore the ways in which the security exceptions are usually invoked in light of the existing controversies.

A. WTO Members' Self-judgment and Discretion

Conceptually, there are almost always provisions in international legal instruments by means of which states retain their right to escape or derogate from a treaty obligation based on unilateral considerations, and based on their subjective appreciation of whether to make use of and invoke the clause containing the grounds for exceptions *vis-à-vis* other states or international organizations.²⁵ Stephan W. Schill classifies self-judging clauses into four categories: i) clauses concerning the restriction of, or derogations from, international obligations; ii) exit-clauses in case of international regimes; iii) clauses pertaining to the jurisdiction of an international court or tribunal; and iv) clauses concerning reservations for international treaties.²⁶

Self-judging clauses are generally expressed using phrases such as “if the state considers”, “in the state’s opinion”, or “if the state determines”, etc. The phrase “when it considers necessary” is indicative of the meaning of “self-judging” or “self-interpretation”. Such clauses are used more and more frequently in free trade agreements, such as in Article 1106 of the Thailand-Australia Free Trade Agreement (TAFTA), Article 7 of the Singapore-Australia Free Trade Agreement (SAFTA) (in the terms and conditions related to e-commerce network and personal data protection), etc.

With respect to the WTO agreement, the key question is whether, and to what extent, Article XXI of the GATT 1994, is self-judging in nature.²⁷ Different scholars have different ways of understanding the self-judging criteria of security exceptions. There exist three main views.

Firstly, a subjective standard review is proposed. The subjective standard

25 Stephan Schill and Robyn Briese, “If the State Considers”: Self-judging Clauses in International Dispute Settlement, *Max Planck Yearbook of United Nations Law*, Vol. 13, 2009, p. 68.

26 *Ibid*, pp. 81-93.

27 Antonio F. Perez, WTO and UN Law: Institutional Comity in National Security, *Yale Journal of International Law*, Vol. 23, 1998, p. 302.

holds that the “necessity test” for the national security exceptions in Article XXI should be undertaken independently by each of the WTO members. For example, some scholars argue that, by its very nature, the clause leaves it to the member invoking the security exceptions to determine what may constitute essential security interests for it and what action is necessary for the protection of its essential security interests.²⁸ In light of the WTO Doha Declaration on the TRIPs Agreement and Public Health, Lindsay argues that the WTO Panel does not have jurisdiction to review the security exceptions.²⁹ Other scholars, led by Emerson, argue that when invoking Article XXI of the GATT 1994, members have the discretion to define their own essential security interests and decide upon their corresponding activities.

Secondly, objective scrutiny is considered imperative. It requires that the WTO Panel and the Appellate Body have the authority to conduct objective scrutiny when and after security exceptions are invoked. The view is that the security exceptions are not completely excluded from the scope of judicial review. As Andrew Emmerson said, if the invocation of Article XXI(b) can be done by members alone in a subjective decision, then it can easily lead to the abuse of the security exceptions clause by members, and weaken the stability of the trading system.³⁰ Therefore, other experts argue that the security exceptions must be subject to review, and that there exist specific review criteria to determine the legality of unilateral measures.

Thirdly, there are calls for a combination of subjective and objective reviews. The view is that a WTO member should have the decisive authority to determine its own essential security interests, but it must also meet certain objective criteria. For example, Shin-yi Peng proposes that the “good faith principle” should be complied with when examining the security exceptions. To be more specific, the “objective” good faith doctrine requires that the invocation of the clauses and their interpretation should be based on a reasonable expectation of the contracting party, while “subjective” good faith requires that the interpretation should be based on the member’s intent.³¹

²⁸ *Supra* n. 25, pp. 61-140.

²⁹ Peter Lindsay, *The Ambiguity of GATT Article XXI: Subtle Success or Rampant Failure?* *Duke Law Journal*, Vol. 52, 2003, p. 1279.

³⁰ *Supra* n. 19, p. 143; n. 20, p. 558.

³¹ *Supra* n. 15, p. 468.

Self-judging clauses provide that a member may unilaterally fail to perform a specific obligation under certain circumstances. Essentially, it is an opt-out mechanism. However, if the clause is admitted to be entirely self-judging in nature, the security exceptions clause will become a pretext for political interests to further curtail the WTO's foundational principles of "most-favored-nation treatment" and "national treatment". In other words, the subjective standard is a disguised recognition of the practice of trade protectionism.³² Therefore, the author believes that the WTO Panel or the Appellate Body should have some form of power to review the interpretation of self-judging clauses.

Among the cases before the International Court of Justice (ICJ), the United States once claimed that the escape clause based on "national security" in fact constituted a bar on the ICJ's jurisdiction, but this argument was rejected in the *Oil Platforms (Islamic Republic of Iran v. United States of America)* case by the ICJ. In that case, the ICJ rejected the United States' claim that security exceptions in the treaty indicated a limitation on the ICJ's jurisdiction. The Court concludes the actions carried out by United States forces cannot be justified as being measures necessary to protect the essential security interests of the United States, since those actions constituted recourse to armed force not qualifying, under international law on the question, as acts of self-defence. The ICJ explicitly referred to the previous case *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)* and held that the term "self-judging" indicates that the contracting party's substantive defenses should be considered.³³ It is worth noting that the security exceptions in the Treaty of Amity, Economic Relations and Consular Rights between the United States and Iran were not provided in the form of self-judging clauses.

During the Argentine financial crisis that began in 2001, the Argentine government invoked the emergency clauses in order to implement measures that deviated from its BIT obligations. In numerous investor-state arbitration proceedings, Argentina asserted that the relevant clauses should be interpreted as self-judging, that its determination of the existence of a state of emergency

³² *Ibid.*

³³ *Supra* n. 27.

was not subject to review by a tribunal, and that it did not involve any international responsibility. However, the tribunal found that the invocation of the clause needed to be reviewed, and it was then up to the tribunal to grant the state the latitude to determine the scope of application. Similar to the ICJ's decision, the investment tribunal distinguished between the concepts of "measures necessary for the protection of its essential security interests" and "measures which a state considers necessary for the protection of its essential security interests" and ruled that the former was not the essence of self-judging power.³⁴

It can, thus, be seen that the subjective standard gives WTO members self-judging power regarding security exceptions, while the objective standard limits the abuse of members' discretion. Therefore, this paper believes that a combination of subjective and objective criteria should be applied to determine a member's self-judging power.

B. Limits on the Abuse of Self-judging Clauses and the Principle of Good Faith

One of the original drafters of the GATT 1947, has stated as follows: "We gave a good deal of thought to the question of the security exception which we thought should be included in the Charter. We recognized that there was a great danger of having too wide an exception and we could not put it into the Charter, simply by saying: "by any member of measures relating to a member's security interests", because that would permit anything under the sun. Therefore we thought it well to draft provisions which would take care of real security interests and, at the same time, so far as we could, to limit the exception so as to prevent the adoption of protection for maintaining industries under every conceivable circumstance ... there must be some latitude here for security measures. It is really a question of balance. We have got to have some exceptions. We cannot make it too tight, because we cannot prohibit measures which are needed purely for security reasons. On the other hand, we cannot make it so broad that, under the guise of security, countries will put on measures which really have a commercial purpose".³⁵ For this reason, the key to

³⁴ See ICSID, *CMS v. Argentine Republic*, ICSID Case No. ARB/01/8, paras. 366-373.

³⁵ Analytical Index of the GATT, Article XXI, p. 600, https://www.wto.org/ENGLISH/res_e/booksp_e/gatt_ai_e/art21_e.pdf (Last Visited on May 14, 2022).

the interpretation of the national security exceptions is avoiding the abuse of security interest measures.³⁶

In the *Nicaragua* case, the ICJ's interpretation of the security exceptions in the Treaty of Friendship, Commerce and Navigation between the United States of America and the Republic of Nicaragua also reflected the requirement of review under self-judging clauses. The ICJ held that "whether a measure is necessary to protect the essential security interests of a party is not, as the Court has emphasized, purely a question for the subjective judgment of the party".³⁷ Although the ICJ did not specifically mention the criteria for review, it argued that the determination of the necessity and proportionality of national measures should be reviewed in a manner consistent with international law.³⁸

As mentioned in the previous section, the core of achieving a balance between trade interests and national security lies in bringing into play the principle of good faith, and incorporating the interpretation of the principle of good faith in respect of performance of treaty obligations, into the interpretation of the necessity of taking actions to secure national security. Theoretically, the principle of good faith is not only a rule of interpretation, but also a substantive obligation on parties to implement and abide by a treaty. Article 26 of the VCLT states that "every treaty in force is binding upon the parties to it and must be performed by them in good faith". Although there is no clear definition of "good faith performance", any attempt to interpret a treaty in such a way as to take advantage of loopholes or ambiguities in the drafting process should not be considered as done in "good faith".³⁹

The national security exceptions must be understood as aiming to protect members' security interests. At the same time, a claim of necessity should be based on a substantial link between the measure and the objective. The determination of necessity requires an interpretation borrowed from Article XX(b) or

³⁶ *Ibid.*

³⁷ International Court of Justice, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Merits, Judgment, ICJ Rep. 1986, para. 282.

³⁸ Chiara Ragni, Standard of Review and the Margin of Appreciation before the International Court of Justice, In Lukasz Gruszczynski and Wouter Werner (eds.), *Deference in International Courts and Tribunals: Standard of Review and Margin of Appreciation*, Oxford University Press, 2014, p. 324.

³⁹ Jeff Waincymer, *WTO Litigation: Procedural Aspects of Formal Dispute Settlement*, Cameron May Press, 2002, p. 499.

XX(d) of the GATT 1994. Furthermore, “necessary” indicates the need for a member to demonstrate that there are no other measures that are less trade restrictive and can secure the same level of protection for that member.⁴⁰ In practice, in November, 1975, Sweden enforced global import quotas for specific raincoats, arguing that a significant decline in domestic production would constitute a substantial threat to Sweden’s economy and, thus, formed an integral part of its security policy.⁴¹ However, because the Swedish interpretation was not consistent with the principle of good faith, the GATT Committee’s decision held that Sweden’s alleged justification for the raincoat import ban constituted an abuse and misapplication of the security exceptions.⁴²

The principle of good faith pervades the interpretation and application of national security exceptions under Article XXI of the GATT 1994. Although members have the self-judging power to define concepts such as “necessity” and “essential security interests”, their invocation of the clauses should be consistent with the customary rules of treaty interpretation, i.e., upon an objective assessment, the measures implemented by the member must be shown to be necessary to protect their legitimate interests. Through the above analysis, this paper holds that the purpose of the security exceptions clause is to give members the right to take measures to protect their “essential security interests”. The specifics of the application of the security exceptions are embodied in the two “if the state considers” provisions: firstly, “the interests which it considers essential”; and secondly, “the measures which it considers necessary”.⁴³ Although members can define the relevant concepts and their own needs, they should, at least, satisfy the principle of good faith while interpreting a treaty and should not give too broad or too tight an interpretation of the phrases “essential security interests” or “emergency in international relations”. The above-mentioned state practices and treaty interpretations are relevant in this respect. As the Appellate Body has emphasized, an interpreter is not free to adopt a

40 *Supra* n. 21, pp. 452-453.

41 Council of Representatives, Report on Work Since the Thirtieth Session, L/4254 (November 25, 1975), pp. 17-18; Sweden – Import Restrictions on Certain Footwear, L/4250 (November 17, 1975), p. 2.

42 GATT, Minutes of Meeting Held in the Palais des Nations, Geneva, October 31, 1975, C/M/109, p. 8.

43 Peter Van Den Bossche, *The Law and Policy of the World Trade Organization: Text, Cases and Materials*, Cambridge University Press, 2013, p. 664.

reading that would result in reducing whole clauses or paragraphs of a treaty to redundancy or inutility.⁴⁴ When applying self-judging clauses as well, members should be consistent with the principle of good faith.

IV. CYBERSECURITY MAY CONSTITUTE “ESSENTIAL SECURITY INTEREST” UNDER THE WTO AGREEMENT

According to the mainstream view, as a reflection of national sovereignty, only WTO members have the power to define their “essential security interests”.⁴⁵ WTO members have the power to take actions to secure their respective security interests and that cannot be denied. However, the key issue is in determining how to balance the conflict between security interests and commercial interests. With regard to the definition of “national security”, different scholars have different arguments. Some scholars believe that the connotations of “national security” include state, sovereignty and international legal personality, and its definition should be based on the abovementioned three keywords. Some other scholars argue that the concept of “national security” is only concerned with protecting national sovereignty from any external, internal, traditional or non-traditional threats. Goodman, on the other hand, argues that human rights matters can also be matters concerning national security, and the violation of human rights obligations should empower members to invoke Article XXI to impose unilateral emergency sanctions on a state.⁴⁶ Furthermore, some scholars hold that members should be able to justify imposition of trade sanctions for reasons such as terrorism by invoking the security exceptions.⁴⁷ At the same time, some scholars have also tried to assert that the threat of climate change can also be a legitimate reason for invoking the security exceptions.⁴⁸ In this way, it can be seen that the concept of “essential security interests” has

⁴⁴ *Supra* n. 23.

⁴⁵ *Supra* n. 19, p. 139.

⁴⁶ Ryan Goodman, Norms and National Security: The WTO as a Catalyst for Inquiry, *Chicago Journal of International Law*, Vol. 2, No. 1, 2001, p. 101.

⁴⁷ Eric J. Lobsinger, Diminishing Borders in Trade and Terrorism: An Examination of Regional Applicability of GATT Article XXI National Security Trade Sanctions, *ILSA Journal of International and Comparative Law*, Vol. 13, 2006, p. 99.

⁴⁸ Felicity Deane, The WTO, the National Security Exception and Climate Change, *Carbon and Climate Law Review*, Vol. 2, 2012, p. 149.

been widely discussed and debated.

There is no authoritative definition of “national security” in relation to the Internet either. For example, Australia has asserted that Huawei’s information technology products would pose a challenge to its national security, while the United Kingdom and New Zealand have argued that there is no need to ban Huawei from supplying equipment for critical infrastructure projects.⁴⁹ Specifically, the US argues that because Huawei has not provided clear and complete information explaining the company’s relationship with the Chinese government, has not answered questions about its financial independence from the Chinese government, and has not responded in detail about its affiliation with the Chinese military and intelligence agencies, the US considers Huawei’s products to be insecure.⁵⁰ In contrast, the British government finally approved Huawei’s participation in the country’s broadband project because its investigation and hearings did not uncover evidence supporting the charges against Huawei.⁵¹

In the case of a threat to cybersecurity, Article XXI(b) of the GATT 1994, and Article 23(1) of the Government Procurement Agreement (GPA) are the most relevant exception clauses.⁵² The core issue in resolving the disagreements regarding application of security exceptions in the GATT 1994, is that, in the context of an “emergency in international relations” caused by cyber espionage, a member is able to take “actions which it considers necessary” for the protection of its “essential security interests”.

National security interests obviously consist of military and defense interests. In contemporary times, the purview has expanded to include the protection of civil communications infrastructure, environmental security, and financial and fiscal interests.⁵³ However, national security interests should be recognized

49 BMI-TechKnowledge Group, Which Way for Huawei? To Ban or Not to Ban, <http://www.bmi-t.co.za/content/which-way-huawei-ban-or-not-ban> (Last Visited on November 16, 2022).

50 The US House of Representatives and the House Permanent Select Committee on Intelligence (HPSCI), Investigative Report on the US National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE (112th Congress), [https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20\(FINAL\).pdf](https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf) (Last Visited on June 11, 2022), pp. 11-34.

51 *Supra* n. 15, p. 471.

52 *Supra* n. 15, p. 458.

53 Eric Pickett and Michael Lux, Embargo as a Trade Defense against an Embargo: The WTO Compatibility of the Russian Ban on Imports from the EU, *Global Trade and Customs Journal*, Vol. 10, 2015, p. 28.

in any case. As one of the original drafters of the national security exceptions in the GATT has stated, security interests include all matters under the sun, unless there is a restrictive provision.⁵⁴

In its National Cybersecurity Strategy Guide (NCSG), the International Telecommunication Union (ITU) has noted that “information security” does not necessarily fall within the scope of “national security” at the technical level, and that confusion between the two terms may lead to misconceptions about security or baseless concerns over risks in cyberspace.⁵⁵ However, it is important to distinguish between cybersecurity and information security. Information security is concerned only with the confidentiality of information and sources/identities, and its emphasis is on privacy and authorized access. Traditionally, most computer systems used to be stand-alone units and unlikely to be transferred across borders. Information security is primarily about avoiding non-consensual and unauthorized access to, modification of, or destruction of, computers, networks, programs, and data.⁵⁶ Steps to ensure cybersecurity are a logical corollary of safeguarding national security, with its emphasis on securing critical digital infrastructure and its functions.⁵⁷ Thus, cybersecurity is an inseparable element of national security.

Cybersecurity is not just a matter of information security, but is more closely related to national policy, as illegal use of the Internet can prevent the continuation of normal economic, public health and national security activities.⁵⁸ At present, all countries possess or store sensitive information on computers and transmit data to other computers via electronic networks. At the same time, numerous unauthorized hackers engage in regular intrusion, theft and distortion of sensitive government information.⁵⁹ For this reason, the above-mentioned threats, when sufficiently serious, can jeopardize the stability of a country’s economy and sovereignty and, therefore, constitute a direct

⁵⁴ *Ibid.*

⁵⁵ ITU, National Cybersecurity Guide, <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf> (Last Visited on November 16, 2022).

⁵⁶ *Supra* n. 55.

⁵⁷ *Supra* n. 15, p. 469.

⁵⁸ *Supra* n. 55.

⁵⁹ ITU, Global Cybersecurity Index and Cyberwellness Profiles, http://www.itu.int/dms_pub/itu-d/oph/str/D-STR-SECU-2015-PDF-E.pdf (Last Visited on November 16, 2022).

threat to national security.⁶⁰

The Internet represents crucial national security interests as well as threats to those interests. Even the US research institutions have declared that the failure of the United States to take steps to ensure cybersecurity is the most pressing challenge to US national security.⁶¹ The US has clearly stated that cyber-attacks pose a significant threat to its domestic cellular network, power companies, electronic commerce, etc.⁶²

By its very nature, the Internet cannot exist in a “zero risk” space. For example, software insecurity is inherent. As technical experts say, software insecurity and vulnerability exist at all stages of software development.⁶³ The key question, then, is in respect of the level of risk which will be considered to constitute a threat to “essential security interests”. Undoubtedly, cybersecurity measures for curtailment of a certain level of risk will constitute an “essential security interest” under Article XXI of the GATT 1994.

V. CYBERSECURITY RISKS MAY CONSTITUTE AN “EMERGENCY IN INTERNATIONAL RELATIONS” UNDER ARTICLE XXI OF THE GATT 1994

An “emergency in international relations” is one of the pre-conditions for invoking the security exceptions. Up till now, there has been no uniform understanding of the phrase in the international community. In November, 1975, Sweden enforced global import quotas for specific raincoats, claiming that a significant decline in domestic production would pose a substantial threat to Sweden’s economic situation and that it was, thus, an integral part of its security policy.⁶⁴ This claim has led to extensive controversy over the definition of “emergency in international relations”.

⁶⁰ *Supra* n. 15, p. 470.

⁶¹ CSIS Commission on Cybersecurity, *Securing Cyberspace for the 44th Presidency*, Washington DC, 2008.

⁶² *Ibid.*

⁶³ Richard Clarke et al., *Cyber War: The Next Threat to National Security and What to Do about It*, Harper Collins Publishers, 2012, pp. 69-102.

⁶⁴ *Supra* n. 41.

The controversies over the meaning of the phrase “emergency in international relations” include the issue of whether or not the term falls within a member’s self-judging powers. Hannes argues that while WTO members are free to define what measures are necessary for the protection of their respective “essential security interests”, the Panel and the Appellate Body must be empowered to review, in good faith, the determination made regarding existence of a state of “war and other emergency in international relations”.⁶⁵ In other words, through the judicial review of the security exceptions in Article XXI(b) by the Panel and the Appellate Body, the possibility of abuse of the security exceptions by the members will be considerably limited. In essence, this view advocates that when applying national security exceptions: firstly, with regard to subject-matters, members have the right to decide what matters conform to the definition of national security exceptions, which is a subjective standard; and secondly, with regard to timing, it is up to the Dispute Settlement Body (DSB) to decide when a member can invoke the national security exceptions, which is an objective scrutiny.⁶⁶

It goes without saying that the definition of “emergency in international relations” is important and determines the scope of application of security exceptions. In Article XXI(b)(iii) of the GATT 1994, the phrase “if the state considers” does not change the definition of “emergency in international relations”. In other words, interpretation of the definition of “emergency in international relations” goes beyond the scope of members’ self-judging power.⁶⁷

Today, we live in a computerized world. Computers and their related devices play a fundamental role in all business activities, in public life and in private life. We live not only in a computerized world, but also in the Internet era, which is characterized by the fact that almost all matters can be controlled remotely via the Internet or other network types.⁶⁸

In December, 2010, a computer malware in the nature of a “worm” infected numerous industrial automation instruments around the world. Although the

⁶⁵ *Supra* n. 18, pp. 446-447.

⁶⁶ *Supra* n. 29, p. 1287.

⁶⁷ Dapo Akande and Sope Williams, International Adjudication on National Security Issues: What Role for the WTO, *Virginia Journal of International Law*, Vol. 43, 2003, p. 399.

⁶⁸ Georg Kerschischnig, *Cyberthreats and International Law*, Eleven International Publishing, 2012, p. 5.

worm did not affect the systems too much, it could send commands regarding operation of the systems through the networks. The worm reportedly invaded the processing systems of Iranian facilities in Bushehr and Natanz, took control and executed commands for self-destruction.⁶⁹ Undoubtedly, this cyber-attack demonstrates the clear and present danger of cross-border terrorists, criminal elements and other actors in cyberspace, difficult to identify/locate, posing a threat to national security via the Internet.

With the increasingly strategic role and use of the Internet, non-state actors can affect information security, cybersecurity and national security by means of digital networks. Bryan even goes so far as to say that cyber-attacks are increasing and that they have become a new type of technological warfare.⁷⁰ In practice, cyber warfare is unanimously regarded as a new form of warfare. For example, in 2007, the Estonian political party, government, banks and media websites suffered a three-week-long downtime due to a cyber-attack. Russian hackers are believed to have been the masterminds of this cyber-attack, which resulted in huge losses to the Estonian government.⁷¹

According to the Dispute Settlement Panel (DSP) and the Appellate Body, the Internet itself is a neutral medium, and that there is no difference between warfare in the physical world and warfare in the virtual world. In other words, cyberwarfare is warfare, or at least constitutes a form of national emergency for which the security exceptions clause can be invoked.⁷²

The concepts of “essential security interests” and “emergency in international relations” are mutually related, and the Panel should be able to conduct an objective scrutiny of claims regarding existence of an “emergency in international relations”. In other words, the phrase “if a state considers” is associated, at best, with “necessary for the protection of its essential security interests”. Subsequently, although Article XXI(b) of the GATT 1994, is broad, it

69 Ron Rosenbaum, The Triumph of Hacker Culture, http://www.slate.com/articles/life/the_spectator/2011/01/the_triumph_of_hacker_culture.htm (Last Visited on December 20, 2022); Fredrik Erixon and Hosuk Lee-Makiyama, Digital Authoritarianism: Human Rights, Geopolitics and Commerce, ECIPE Occasional Paper, No. 5, 2011, p. 10.

70 Brian M. Mazanec, Why International Order in Cyberspace Is Not Inevitable, *Strategic Studies Quarterly*, 2015, pp. 78-80.

71 *Ibid.*

72 Claire Oakes Finkelstein and Kevin H. Govern, Introduction: Cyber and the Changing Face of War, Pennsylvania Legal Scholarship Repository Paper, No. 1566, 2015, pp. x-xx.

leaves room for institutional interpretation by the Panel and the Appellate Body as well as self-interpretation by the members.⁷³

VI. CONCLUSION

The WTO legal framework is a system of multiple agreements. Any issue may be the subject of provisions of different agreements or different provisions of the same agreement. In contrast to the general exception clause, the security exceptions clause is considered a “gentleman’s provision” and WTO members are committed to avoiding invoking it. However, an analysis of the security exceptions helps to provide a deeper understanding of the way the Internet regulations are applied.

Through the analytical framework of the law of treaties, the core issue of the interpretation and application of security exceptions is to determine the “self-judging” nature of the security exceptions, and to define the concepts of “essential security interests” and “emergency in international relations” in a reasonable manner. Specifically, although the security exceptions entitle a member to assert both essential security interests and necessities, the principle of good faith should be followed in the application and interpretation of the clause. According to the law of treaties, cybersecurity may constitute “essential security interests” under Article XXI of GATT 1994, while cybersecurity threats may constitute an “emergency in international relations” under Article XXI of GATT 1994.

⁷³ *Supra* n.15, p. 464.