ADJUDICATING CYBER ESPIONAGE CASES THROUGH THE WORLD TRADE ORGANIZATION'S DISPUTE SETTLEMENT SYSTEM

*Roshni Ranganathan**

Abstract

In 2013, United States received a report that revealed cyberattacks by the Chinese military on U.S. companies to steal their trade secrets in order to provide leverage to domestic Chinese companies. The legal recourse available to states in such circumstances is unclear and thus, requires some discussion. Stealing of trade secrets to provide some competitive advantage to one's own companies can be understood to mean commercial or economic cyber espionage. No international treaty governs economic espionage specifically but a basic protection to trade secrets[1] and other intellectual property is provided through the World Trade Organization's (WTO) Agreement on Trade

*Roshni Ranganathan is a fifth-year student at Gujarat National Law University, Gandhinagar. The author may be reached at roshniranganathan@gmail.com.

[1]TRIPS: Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organisation, Annex 1C, 1869 U.N.T.S. 299, 33 I.L.M. 1197 (1994), art. 39.2 [hereinafter 'TRIPS Agreement'].

Related Intellectual Property Rights (TRIPS)[2]*, which can be extended to protect the confidential data of the companies which gives them the trade advantage.*

Keeping this in mind, the author seeks to analyse the possibility of litigating commercial cyber espionage complaints through the WTO Dispute Settlement Body (DSB) as a ***TRIPS violation*** *and as* ***a non-violation complain****. These concepts are explained through the above* ***case study*** *of United States and China with respect to alleged acts of economic cyber espionage by China on U.S. By applying the relevant provisions of TRIPS and GATT 1994, the author will establish that among the few alternatives that are available to the United States for addressing and adjudicating commercial cyber espionage, WTO may not be the best forum for disputing data protection given the present system in existence. In order to serve as an adjudicatory forum, WTO must reconsider its existing mechanism to either modify TRIPS or formulate a new agreement that specifically addresses cyber espionage issues in trade.*

[2]TRIPS Agreement, art. 42.

I. INTRODUCTION

The modern global economy thrives on data. With an increase in the amount of data being collected and transferred on a daily basis, instances of cyber espionage are also on the rise.[3] One form of espionage is economic espionage which involves attempts by a state to covertly acquire trade secrets held by foreign private enterprises.[4] Protection against such espionage has been long considered by countries as important to national security and economic development.[5] With the advent of Internet, cyber economic espionage has become a growing concern among many countries.[6]

While countries like U.S. have their own national laws[7] governing cyber espionage, there is no international norm or treaty that addresses this issue at a global level.[8] In the absence of such a norm or treaty, some countries have entered into agreements with other countries to prevent theft of data from within their borders, such as the agreement entered into between U.K. and China to "not engage in commercially motivated cyber espionage."[9] However, such diplomatic agreements are not legally binding as they do not have the

[3]David J. Kappos and Pamela Passman, *Cyber Espionage is Reaching Crisis Level*, FORTUNE (December 12, 2015), http://fortune.com/2015/12/12/cybersecruity-amsc-cyber-espionage/, (last visited Feb. 18, 2018).
[4]David P. Fidler, *Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets through Cyber Technologies*, 17 INSIGHTS AMERICAN SOCIETY OF INT'L L 10 (2013), https://www.asil.org/insights/volume/17/issue/10/economic-cyber-espionage-and-international-law-controversies-involving.
[5]*Id.*
[6]David J. Kappos and Pamela Passman, *Cyber Espionage is Reaching Crisis Level*, FORTUNE (December 12, 2015) http://fortune.com/2015/12/12/cybersecruity-amsc-cyber-espionage/, (last visited Feb. 18, 2018).
[7]Economic Espionage Act, 18 U.S. Code § 1831 (1996).
[8]Matthew Dahl, *Agreements on Commercial Cyber Espionage: An Emerging Norm?*, LAWFARE (December 4, 2015) https://www.lawfareblog.com/agreements-commercial-cyber-espionage-emerging-norm, (last visited Oct. 2, 2017).
[9]*Id.*

sanction of a treaty. This article, therefore, looks into the viability of contesting cyber economic espionage at the WTO's Dispute Settlement Body as an alternative given that the states are bound by the decisions of the WTO Panel or Appellate Body[10] and the obligation to protect undisclosed information under TRIPS Agreement.[11]

Commercial cyber espionage, which is the focus of this article, specifically relates to a state's cyber activities to obtain trade secrets from foreign companies with the intent of providing competitive leverages to domestic companies.[12] For example, if companies belonging to State A carry on business in State B and have subsequently become targets of data theft by actors in State B, it compromises their competitiveness in State B and worldwide. Such acts amount to commercial cyber espionage.[13]

Although no international treaty governs economic espionage specifically, a basic protection to trade secrets[14] and other intellectual property is provided through World Trade Organization's (WTO) Agreement on Trade Related Intellectual Property Rights (TRIPS).[15] This Agreement can be extended to accord protection to the

[10]World Trade Organisation, *Dispute Settlement without recourse to Panels and the Appellate Body*, https://www.wto.org/english/tratop_e/dispu_e/disp_settlement_cbt_e/c8s1p1_e.htm, (last visited Feb. 17, 2018).
[11]TRIPS Agreement, art 39.
[12]Jack Goldsmith and Robert D. Williams, *The Chinese Hacking Indictments and the Frail "Norm" Against Commercial Espionage*, LAWFARE (November 30, 2017), https://www.lawfareblog.com/chinese-hacking-indictments-and-frail-norm-against-commercial-espionage, (last visited Feb. 18, 2018).
[13]Stuart S. Malawer, *Chinese Economic Cyber Espionage*, 1 GEORGETOWN J. ON INT'L AFFAIRS 1 (2015).
[14]TRIPS: Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organisation, Annex 1C, 1869 U.N.T.S. 299, 33 I.L.M. 1197 (1994), art. 39.2 [hereinafter 'TRIPS Agreement'].
[15]TRIPS Agreement, art. 42.

confidential data that provides the concerned company with a trade advantage.

As things stand at present, there is a lack of clarity with respect to the actions that a victim state may take in case of commercial cyber espionage. The United States (U.S), for example, resorted to imposing unilateral trade sanctions on North Korea after a cyber attack by the latter state on Sony Pictures, an entertainment company based in U.S. A hacker group going by the name "Guardians of Peace" identified themselves as the perpetrators behind the attack where a great amount of confidential information of Sony Pictures, including employees' Social Security Number, e-mail address, etc. was leaked online.[16] The attack was attributed to North Korea and the purpose was to prevent them (Sony) from releasing the movie "Interview", which allegedly ridiculed the leader of North Korea, Kim Jong-Un.[17] In retaliation, United States imposed limited economic sanctions on North Korea. It was the first time a country had imposed economic and trade sanctions to counter destructive use of cyber space by another country.[18]

Resort to such unilateral measures by the U.S. highlights the lack of any international legal mechanism or other recourses available to states to deal with cyber activities by other state actors. This leads us to some important questions: How can a state protect its confidential data from being stolen by other state actors? And in case of theft of such data or attempt to steal, what recourse would the complaining state have?

[16]Gabi Siboni and David Siman-Tov, *Cyberspace Extortion: North Korea versus the United States*, 646INSS INSIGHT 1-3 (2014).
[17]*Id.*
[18]David E. Sanger and Michael S. Schmidt, *More Sanctions on North Korea After Sony*, N. Y. TIMES, March 1, 2015, http://www.nytimes.com/2015/01/03/us/in-response-to-sony-attack-us-levies-sanctionson-10-north-koreans.html, (last visited Sept. 28, 2017).

Given the current increase in cross border data flow among countries, there is a need for an international legal system to adjudicate cyber-espionage claims. With the above key questions in mind, this article will examine the viability of adjudicating disputes concerning cyber espionage (in particular, commercial cyber espionage) through WTO's dispute settlement system. For this purpose, the article is divided into four parts, namely:

Part I – Commercial Cyber Espionage by China on U.S. – A Case Study
Part II – TRIPS Violation Claims
Part III – Non-Violation Complaint under GATT
Part IV – Conclusion

Part I introduces the reader to the commercial cyber espionage launched by the Chinese Military on U.S. in 2013. Using this incident as the main case study, the article examines the options that would be available to U.S. (or another state in a similar position) if it were to pursue the matter through WTO's Dispute Settlement Body. These options, in the form of TRIPS violation claims and non-violation claims, have been analysed in detail in Part II & III. Part II discusses the various provisions under TRIPS that are violated by a state when it engages in espionage and analyses if the same were to apply to a case of commercial cyber espionage. Part III, on the other hand, examines whether an act of commercial cyber espionage could give rise to a non-violation complaint under GATT 1994. The article answers both the questions raised in these two parts in the negative. Through this, the author aims to prove that the present mechanism under which the WTO functions is insufficient to provide an effective remedy to a complaining state in the event of commercial cyber espionage. On that note, the article concludes in Part IV with thoughts on whether WTO should amend its existing covered agreements to include commercial cyber espionage as a violation or draft a new

agreement for activities in the cyber space altogether which would include commercial and trade related aspects.

II. COMMERCIAL CYBER ESPIONAGE BY CHINA ON U.S – A CASE STUDY

A. Background

Despite hundreds of billions of dollars being spent on cyber-security, the possibilities of cyber-attacks only seem to grow with time.[19] In 2013 at the Asia Society, U.S. National Security Advisor, Tom Donilon, highlighted the growing global concern with respect to cyber security. He stated:

> *"Cyber-security is not solely a national security concern or a concern of the U.S. government. Increasingly, U.S. businesses are speaking out about their serious concerns about the sophisticated, targeted theft of confidential business information and proprietary technologies through cyber intrusions emanating from China on an unprecedented scale…As the President said in the State of the Union, we will take action to protect our economy against cyber-threats."*[20]

His statement reflected the concern of the entire U.S. government regarding the alleged cyber espionage by the Chinese military, which was revealed through a report by a private company in February

[19]Craig Timberg, *A Flaw in the Design*. WASHINGTON POST https://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/ (May 31, 2015).

[20]Tom Donilon, *The Asia-Pacific in 2013*, (Remarks given to the Asia Society, White House Press Office, Washington, D.C., March 11, 2013).

2013.[21] The report stated that the Chinese military had employed cyber technology to steal trade secrets from foreign companies. It was speculated that this was to provide a competitive advantage to domestic Chinese companies as against those foreign companies. Therefore, the competitive advantage of U.S. companies in China *and worldwide* was compromised.[22]

B. Recourse Available to U.S

The existing legal instruments and policies on protection of intellectual property and trade secrets pre-date the advancement of the internet. The Uruguay Round Agreements,[23] which includes TRIPS, was concluded in 1995, when internet had just gained traction. Therefore, to successfully bring an international claim of cyber-espionage in trade against another state calls for creative application of the existing regime, which Prof. Malawer argues is available.[24]

The possible recourse that may be available to the United States is by approaching WTO under TRIPS Agreement or through Article 26 of DSU or by imposing unilateral sanctions on the opposite party (China) as it did in the case of North Korea.

[21]Mandiant, *APT1: Exposing One of China's Cyber Espionage Units* (Feb. 2013), http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf. (last visited Sept. 28, 2017).
[22]Stuart S. Malawer, *Chinese Economic Cyber Espionage*, 1 GEORGETOWN J. ON INT'L AFFAIRS 1(2015).
[23]*Final Act Embodying the Results of the Uruguay Round of Multilateral Trade Negotiations*, Apr. 15, 1994, 1867 U.N.T.S. 14, 33 I.L.M. 1143 (1994), https://www.wto.org/english/docs_e/legal_e/03-fa_e.htm., (last visited Sept. 30, 2017).
[24]Stuart S. Malawer, *Chinese Economic Cyber Espionage*, 1 GEORGETOWN J. ON INT'L AFFAIRS 2 (2015).

III. TRIPS VIOLATION CLAIMS

The TRIPS Agreement [hereinafter 'TRIPS'], does not explicitly provide for protection against economic cyber espionage for commercial or competitive advantages. However, it interesting to note whether and how the existing provisions of TRIPS may be creatively applied, especially in the U.S.-China case described above.

A. Preamble

The basic objective of TRIPS, reflected through its preamble, is "to reduce distortions and impediments to trade... taking into **account the need to promote effective and adequate protection of intellectual property rights**, and to ensure that measures and procedures to enforce intellectual property rights do not themselves become barriers to legitimate trade"[25] [*emphasis supplied*].

This text recognizes that lack of adequate protection to IP rights restricts trade[26] and leads to free rider problems.[27] Given that there are no specific laws governing the aspects of trade secret theft in the form of cyber espionage, the objective of TRIPS could come to its rescue. One can argue that if the underlying objective of TRIPS is to ensure adequate protection to IP, then the corollary is that it needs to be extended and applied to protect those IP aspects that were not envisaged at the time of negotiating the Agreement. However, such an argument fails to recognize the importance of the substantive provisions. While the objective of the TRIPS is correctly stated, it

[25]TRIPS Agreement, preamble.
[26]PETER VAN DEN BOSSCHE, THE LAW AND POLICY OF THE WORLD TRADE ORGANISATION 744 (2d ed. 2009).
[27]T. Cottier, *The Agreement on Trade Related Aspects of Intellectual Property Rights*, THE WORLD TRADE ORGANISATION: LEGAL, ECONOMIC AND POLITICAL ANALYSIS 1054 (Springer, 2005).

cannot be applied in isolation to include protection against commercial cyber espionage.

Therefore, it becomes important to understand the scope of application of the TRIPS Agreement as it currently exists.

B. Scope of Application

Article 1.2 of TRIPS provides that: "For the purposes of this Agreement, the term 'intellectual property' refers to all categories of IP that are the subject of Sections 1 through 7 of Part II." These subjects are:

a. Copyright and related rights;
b. Trademarks
c. GI
d. Industrial Design;
e. Patents
f. Layout-designs of ICs;
g. Protection of undisclosed information.

Plain reading of Article 1.2 implies that not all forms of IP rights are covered by TRIPS. However, these categories are not clear cut. In *U.S. – Section 211 Appropriations Act,* the Panel was faced with interpreting Article 2.1 of TRIPS in relation to 'trade names', which though not explicitly covered by the above-listed subjects, was covered under Article 1(2) of the Paris Convention. The Panel opined that the Paris Convention would not apply as the list of subjects from Sections 1-7 was exhaustive because Article 1.2 of TRIPS refers to 'all categories'.[28] The Appellate Body, however, differed on this. It held that the scope of application of TRIPS is "not limited to the categories indicated in each *title* but with other *subjects* as well"[29]

[28]Panel Report, *US – Section 211 Appropriations Act*, ¶ 8.26.
[29]Appellate Body Report, *US – Section 211 Appropriations Act*, ¶ 335.

implying that TRIPS also covers those IP rights in other conventions that incorporate the 'subject' of these Sections.[30]

In the present context, cyber espionage of trade secrets clearly falls within the last category, i.e. 'protection of undisclosed information'. However, should one argue that cyber espionage is not explicitly covered, the above interpretation by the Appellate Board widens the scope of the TRIPS Agreement to include several other aspects related to these subjects.

If trade secret protection against commercial cyber espionage is not covered by TRIPS, no remedy will lie in the WTO Dispute Settlement System. United States can successfully bring a claim against China only when it can prove that an obligation, like national treatment, for example, exists in relation to the IP right claimed.

C. National Treatment Principle – Article 3

National treatment is one of the major principles in international trade law[31] and intellectual property.[32] It reads as follows:

> *"Article 3*
>
> *National Treatment*
>
> *1. Each Member shall accord to the nationals of other Members treatment no less favourable than that it accords to its own nationals with regard to the protection of intellectual property, subject to the exceptions already provided in,*

[30]PETER VAN DEN BOSSCHE, THE LAW AND POLICY OF THE WORLD TRADE ORGANISATION, 751 (2d ed. 2009).
[31]M. MATSUSHITA & T. F. SCHOENBAUM & P. C. MAVROIDIS, THE WORLD TRADE ORGANISATION: LAW, PRACTICE, AND POLICY, 233 (2nd ed. 2006).
[32]F. H. Reichman, *Universal Minimum Standards of Intellectual Property Protection under the TRIPS Component of WTO Agreement*, 29 INT'L L.J. 2, 345, 347 (1995).

> *respectively, the Paris Convention (1967), the Berne Convention (1971), the Rome Convention or the Treaty on Intellectual Property in Respect of Integrated Circuits. In respect of performers, producers of phonograms and broadcasting organizations, this obligation only applies in respect of the rights provided under this Agreement. Any Member availing itself of the possibilities provided in Article 6 of the Berne Convention (1971) or paragraph 1(b) of Article 16 of the Rome Convention shall make a notification as foreseen in those provisions to the Council for TRIPS.*
>
> *2. Members may avail themselves of the exceptions permitted under paragraph 1 in relation to judicial and administrative procedures, including the designation of an address for service or the appointment of an agent within the jurisdiction of a Member, only where such exceptions are necessary to secure compliance with laws and regulations which are not inconsistent with the provisions of this Agreement and where such practices are not applied in a manner which would constitute a disguised restriction on trade."*

The main objective of this provision[33] is to eliminate discrimination between a foreign person and a national with respect to protection of intellectual property.[34] The relevant question then is whether this protection extends to prevent a member state from (unlawfully) procuring the trade secrets and other IP information from foreign firms *within its territory* and then pass on such information to its nationals/domestic firms? The answer to this is in the affirmative as is

[33]TRIPS Agreement, art. 3 – "Each Member shall accord to the nationals of other members treatment no less favorable than that it accords to its own nationals with regard to the protection of intellectual property."
[34]M. Matsushita & T. F. Schoenbaum & P. C. Mavroidis, *supra* note 32, at 233 (2nd ed. 2006).

clear from a plain reading of the provision. However, this protection is territorial in nature.[35]

Given that the treatment of foreign IP is dependent on the extent of rights and protection granted to a national under the domestic law, this provision does not extend the obligation of the member state to firms outside its territory. In other words, if a member state secures trade secrets of a foreign firm (that is not situated within its territory) in order to provide benefits to its domestic firms from such secrets, the member state to which the foreign firm belongs cannot claim national treatment violation. Some scholars disagree on this point.[36] They claim that if the effects and benefits of the stolen information accrue to the intruding state, then such actions are also reasonably included within the language of Article III.[37] That is to say, if it can be proved that Chinese firms benefitted from the stolen information or the effects of such theft accrued to China, then U.S. can claim violation of national treatment principle under TRIPS. However, there is nothing provided in the WTO Agreement or in the TRIPS Agreement that extends the obligation of a member state to protect the confidential information of companies outside its territory.[38] More generally, even international law does not prohibit economic espionage either through treaty or customary international law.[39]

[35]Loewenheim U, *The Principle of National Treatment in the International Conventions Protecting Intellectual Property*, In: Pyrmont W.P.W., Adelman M.J., Brauneis R., Drexl J., Nack R. (eds) *Patents and Technological Progress in a Globalized World*, MPI STUDIES ON INTELLECTUAL PROPERTY, COMPETITION AND TAX LAW, 6 (Springer, Berlin, Heidelberg 2009).

[36]Stuart S. Malawer, *Chinese Economic Cyber Espionage*, 1 GEORGETOWN J. ON INT'L AFFAIRS 4, 5 (2015) [hereinafter 'Malawer'].

[37]*Id.*

[38]David P. Fidler, *Why the WTO is not an Appropriate Venue for Addressing Economic Cyber Espionage*, *Arms Control Law* (Feb. 11, 2013), https://armscontrollaw.com/2013/02/11/why-the-wto-is-not-an-appropriate-venue-for-addressing-economic-cyber-espionage/, (last visited Feb. 18, 2018).

[39]Simon Chesterman, *The Spy Who Came in from the Cold War: Intelligence and International Law*, 27 MICH. J. INT'L L. 1071 (2006).

Therefore, under the existing jurisprudence on WTO and TRIPS, national treatment principle is territorial in nature.

Another issue with claiming national treatment violation as a result of cyber economic espionage is discharging of burden of proof by the complaining party. The problem of attribution is common across all cyber espionage cases, i.e. pinning responsibility on the perpetrator of the attack.[40] If a state is unable to discharge this burden sufficiently, then it is argued that the chances of succeeding in a case of commercial cyber espionage are low. In case of the Chinese cyber espionage on U.S., the latter state relied on reports that were released by a private company while attributing the attack to China.[41] In the absence of any other proof or empirical data, this report alone may not suffice in establishing responsibility on China for the attack.[42] Therefore, a complaint by U.S. alleging violation of national treatment principle by China will not succeed for economic cyber espionage cases.

D. Protection of Undisclosed Information – Article 39

Article 39 of TRIPS imposes an obligation on the member states to protect undisclosed information of natural and legal persons. Paragraph 1 of Article 39 imposes an obligation on the member

[40]C Fred Bergsten, *Bridging the Pacific: toward free trade and investment between China and the United States*; Gary Clyde Hufbauer; Sean Miner, 356 (Washington, District of Columbia: Peterson Institute for International Economics, 2014).
[41]Mandiant, *APT1: Exposing One of China's Cyber Espionage Units* (Feb. 2013), http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf. (last visited Sept. 28, 2017).
[42]C Fred Bergsten, B*ridging the Pacific : toward free trade and investment between China and the United States*; Gary Clyde Hufbauer; Sean Miner, 356 (Washington, District of Columbia : Peterson Institute for International Economics, 2014); David P. Fidler, *Why the WTO is not an Appropriate Venue for Addressing Economic Cyber Espionage*, Arms Control Law (Feb. 11, 2013), https://armscontrollaw.com/2013/02/11/why-the-wto-is-not-an-appropriate-venue-for-addressing-economic-cyber-espionage/, (last visited Feb. 18, 2018).

states; paragraph 2 provides a right of protection of undisclosed information against disclosure to natural and legal persons (read with Article 39.1) and paragraph 3 deals with data submitted to government or their agencies.

The protection under Article 39.2 is from disclosures done "in a manner contrary to honest commercial practices"[43] the meaning of which is clarified in the footnote to the provision.[44] It includes breach of contract, breach of confidence, inducement to breach, and acquisition by parties who knew such practices were being employed to acquire such information. Commercial cyber espionage will fall within "breach of confidence" as the confidential information in such cases is obtained without the knowledge of the owner and used without his/her express or implied consent.[45]

The meaning of "honest commercial practices" was further espoused by the Appellate Body in *US – Hot Rolled Steel* case where it stated:

> *"The word 'honest' which qualifies the word 'practices', indicates that... the 'practices' must conform to the dictates of the basic principles of good faith and fundamental fairness."*[46]

This obligation will be breached by any state (China, in the present case) that acquires trade secrets in a clandestine manner[47] in order to

[43]TRIPS Agreement, art. 39.2.
[44]TRIPS Agreement, Note to art. 39: "For the purpose of this provision, "a manner contrary to honest commercial practices" shall mean at least practices such as breach of contract, breach of confidence and inducement to breach, and includes the acquisition of undisclosed information by third parties who knew, or were grossly negligent in failing to know, that such practices were involved in the acquisition"
[45]Saltman Engineering v. Campbell Engineering, (1948) 65 RPC 203 (CA).
[46]Appellate Body Report, *US – Hot Rolled Steel,* ¶ 193.
[47]Commonwealth v. John Fairfax & Sons Ltd., (1980) 147 CLR 39, 50.

secure some competitive/commercial advantage to its national companies.[48]

The main task of the complaining state would then be to prove that the information so acquired falls within the parameters of "undisclosed information" as laid down in Article 39.2(a) to (c). These parameters stipulate that the information should be:

> a) Should have been kept a secret through reasonable steps taken by the person in control of the information.[49]
> b) Should have a commercial value attributable to its secrecy;[50]
> c) A secret that is not generally known or readily accessible to the persons who normally deal with this kind of information;[51]

The problem in determining 'reasonable steps' taken to protect the information in case of a digitally protected data is that the complaining party may have to reveal the security mechanisms in place to protect the data which could make the data vulnerable to new attacks. However, unlike domestic dispute settlement bodies, the WTO Panel understands the need for additional protection of business information submitted to Panels.[52] In *Canada – Aircraft* and *Brazil – Aircraft*, the confidential information was to be stored in a locked room at the premises of the relevant Geneva missions, with

[48]Jack Goldsmith and Robert D. Williams, *The Chinese Hacking Indictments and the Frail "Norm" Against Commercial Espionage*, LAWFARE, November 30, 2017, https://www.lawfareblog.com/chinese-hacking-indictments-and-frail-norm-against-commercial-espionage, (last visited Feb. 18, 2018).
[49]TRIPS Agreement, art. 39.2(c).
[50]TRIPS Agreement, art. 39.2(b).
[51]TRIPS Agreement, art. 39.2(a).
[52]PETER VAN DEN BOSSCHE, THE LAW AND POLICY OF THE WORLD TRADE ORGANISATION 284 (2d ed. 2009).

restrictions imposed on access.[53] Special procedures were adopted to govern this information which *inter alia* provided for destruction of the confidential information upon completion of the proceedings. Despite this, Canada refused to submit the confidential information, citing reasons of inadequate protection. The Appellate Body, however, stressed that refusal to provide information shall not be the only determining criteria to draw inferences.[54]

In the context of commercial cyber espionage, when the confidential information is stored digitally, adopting such special procedures and ensuring that they remain confidential becomes difficult. In order to overcome this difficulty, the Procedures Governing Business Confidential Information needs to be amended to suit the needs of the digital age.

Secondly, the information so revealed should have a commercial value.[55] Interpretation of "undisclosed information" under Article 39 encompasses 'company secrets' as well.[56] Private information is not covered given the distinction between confidential information and trade secrets.[57] To claim protection under Article 39, it must be proved that the information affects the competitive advantage of the national.[58] In the context of commercial espionage, this implies that cyber attacks like that on *Sony*are outside the scope of litigation through WTO. In case of economic espionage by the Chinese military, it needs to be proved that the information that was disclosed

[53]Panel Report, *Canad – Aircraft*, Annex 1; Panel Report, *Brazil – Aircraft*, Annex 1.

[54]Appellate Body Report, *Canda – Aircraft*, paras. 204-5; Panel Report, *US – Upland Cotton*, ⁋⁋. 7.20-7.42, 7.609-7.633.

[55]TRIPS Agreement, art. 39.2(b).

[56]M. BLAKENEY, TRADE RELATED ASPECTS OF INTELLECTUAL PROPERTY RIGHTS: A CONCISE GIDE TO THE TRIPS AGREEMENT, 103 (1996).

[57]Faccenda Chicken Ltd v. Fowler, [1986] 1 All ER 617.

[58]WTO – TRADE RELATED ASPECTS OF INTELLECTUAL PROPERTY RIGHTS 635 (Peter Tobias Stoll, Jan Busche and Katrin Arend eds., Max Planck Institute for Comparative Public International Law 2008).

was indeed used to provide the domestic companies with a trade advantage over foreign companies, i.e. U.S. Companies. However, in the absence of any WTO jurisprudence in this regard, it is unclear whether threatening the foreign firm with its confidential information, in order to gain some trade/commercial leverage, would amount to 'acts contrary to honest commercial practices.'

The third parameter is that of 'ready accessibility'. The impugned information should be a secret that is not generally known or readily accessible to the persons who normally deal with this kind of information.[59] This aspect of 'ready accessibility' has been subject to various national interpretations. In case of U.S., the information is considered secret if it requires "considerable difficulties" to access it.[60] In Germany, on the other hand, the time and "effort", and the obstacles in place to prevent disclosure are considered to determine accessibility.[61] The kind of interpretation to be applied to any case would depend on the facts and circumstances of each case.

Even if the state is able to prove the above requirements with respect to the information in question, the problem of territoriality, as seen in case of national treatment, re-surfaces.[62] Scholars argue that the use of the words 'possibility of preventing' in Article 39.2[63] implies that it

[59]TRIPS Agreement, art. 39.2(a).
[60]M. MATSUSHITA & T. F. SCHOENBAUM & P. C. MAVROIDIS, THE WORLD TRADE ORGANISATION: LAW, PRACTICE, AND POLICY, 246 (2nd ed. 2006).
[61]*Id.*
[62]*Supra* Part II, 2.3; C. CORREA & A. YUSUF, INTELLECTUAL PROPERTY AND INTERNATIONAL TRADE: THE TRIPS AGREEMENT 370 (1998).
[63]TRIPS Agreement, art. 39.2: "2. Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices so long as such information:
(a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;
(b) has commercial value because it is secret; and

does not provide a right to a legal claim to the nationals but rather obliges the member states to "provide legal instruments to their nationals to enable them to prevent infringements."[64] This means that Article 39.2 does not grant any exclusive right of protection at an international level[65] but only imposes an obligation on the member states to implement mechanisms that meet the minimum standards which can be done by enacting national laws to that effect.[66] Therefore, in order to successfully prove Article 39 violation, the complainant state must prove that the member state complained of has not met its obligation under TRIPS.

The kinds of obligation recognized under the TRIPS for this purpose are obligation to protect against disclosure and against unfair commercial use.[67] In case of commercial cyber espionage, it becomes important to prove that the confidential data was used for commercial advantage.[68] In the Chinese military attack on U.S., the reports were released by a private company[69] with no concrete evidence to establish that the data has been used by China to provide competitive advantage to the Chinese firms.

(c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret."

[64]C. CORREA & A. YUSUF, INTELLECTUAL PROPERTY AND INTERNATIONAL TRADE: THE TRIPS AGREEMENT 370 (1998).

[65]World Health Organisation, Protection of Data Submitted for the Registration of Pharmaceuticals: Implementing the Standards of the TRIPS Agreement (2002), § 6.

[66]C. CORREA & A. YUSUF, INTELLECTUAL PROPERTY AND INTERNATIONAL TRADE: THE TRIPS AGREEMENT 370 (1998).

[67]*Id.*

[68]Jack Goldsmith and Robert D. Williams, *The Chinese Hacking Indictments and the Frail "Norm" Against Commercial Espionage*, LAWFARE, November 30, 2017, https://www.lawfareblog.com/chinese-hacking-indictments-and-frail-norm-against-commercial-espionage, (last visited Feb. 18, 2018).

[69]Mandiant, *APT1: Exposing One of China's Cyber Espionage Units* (Feb. 2013), http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf. (last visited Sept. 28, 2017).

Therefore, an action may lie at WTO under TRIPS for acts of commercial cyber espionage only if the foreign firm is within the territory of the violating state and if the complaining state can prove that the information qualifies as 'undisclosed' as required by Article 39. It will be very difficult to provide a remedy at WTO in case the company operates outside the territory of the violating state for reasons explained above.[70]

IV. NON-VIOLATION COMPLAINT UNDER GATT

Filing a non-violation complaint is another avenue that a state can explore. According to the non-violation principle, the member state can approach the Dispute Settlement Body without there being any agreement with the other state complained of. The principle of non-violation is laid down in Article 26.1 of Dispute Settlement Understanding and Article 64.1 of TRIPS. However, currently there is a moratorium (temporary ban) on non-violation complaints on intellectual property claims under TRIPS.[71] Initially this period was for five years (that is, 1995-1999). It has been extended since then.[72] Although there have been arguments from countries like U.S. and Switzerland to make non-violation claim applicable under TRIPS, the majority of the member states either wanted to impose a complete ban on non-violation complaints in respect of IP or extend the moratorium. At the 11th Ministerial Conference in Buenos Aires in December 2017 the member states agreed to once again extend the

[70]*Supra* Part II, 2.3, 2.4.
[71]*TRIPS: 'Non-Violation' Complaints (Article 64.2)*, WORLD TRADE ORGANISATION, https://www.wto.org/english/tratop_e/trips_e/nonviolation_background_e.htm, (last visited Oct. 2, 2017).
[72]WTO: 2015 News Item, Intellectual Property: Formal Meeting, WTO website, November 23, 2015.

moratorium until the 12th Ministerial Conference in 2019.[73] Till then, the members are not permitted to initiate any non-violation complaints under TRIPS.[74]

If the State party wishes to approach the Panel under Article 26.1 of DSU instead of Article 64 of TRIPS, then it (the complaining party) needs to satisfy the three part structure set out by the Panel in *Japan – Film* case-

a) the application of a "measure"

b) the identification of a benefit owing to the complainant under some WTO agreement; and

c) a demonstration that the measure has nullified or impaired that benefit.[75]

Going by the interpretation, it is debateable if acts of commercial cyber espionage constitute a 'measure' for the purpose of non-violation claims. Whether or not "benefits" were owed to the complainant varies with facts and circumstances of the case. For example, if State X collects confidential information from foreign companies within its territory to provide certain commercial advantages to the domestic companies, there could be impairment of benefits. However, when the foreign company do not operate with or within the territory,[76] there are generally no benefits promised by State X to such companies. Does that imply that no obligation is owed by State X to such a company? Under GATT 1994, at least, no such

[73]*TRIPS: 'Non-Violation' Complaints (Article 64.2),* WORLD TRADE ORGANISATION,https://www.wto.org/english/tratop_e/trips_e/nonviolation_e.htm, (last visited Feb. 28, 2018).
[74]*Id.*
[75]Panel Report, *Japan – Film.*
[76]"with" includes export-import activities with that state and "within" includes establishing a physical presence in that territory.

obligation can be traced to State X in the absence of any 'benefits' promised to the complainant state.

Further, under Article 26.1(b) of DSU, the Appellate Body does not require the 'measure' to be withdrawn by the state complained of in case it nullifies or impairs the benefits, but can only*recommend* the parties to make a 'mutually satisfactory agreement'.[77] This means that the member state complained of does not have an obligation to withdraw or discontinue the measure involving cyber espionage. The WTO can merely recommend China and U.S. to reach a mutually satisfactory agreement. This will not be a satisfactory remedy for cyber espionage cases as it does not stop the violating state from stealing confidential information. It is probably in this light that U.S. and China entered into an agreement to refrain from carrying on any cyber-related theft of confidential information.[78]

At the time when this incident came to light, many cyber-security experts discussed that U.S. could claim national security exception under Article XXI of GATT, 1994 and subsequently impose unilateral sanctions on China.[79] However, there has been no case till date in the WTO where the parties have claimed this exception.[80] Therefore, it is difficult to ascertain if such a strategy would succeed.

[77]GATT 1994:General Agreement on Tariffs and Trade 1994, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organisation, Annex 1A, 1867 U.N.T.S. 187, 33 I.L.M. 1153 (1994), art. 26.1(b) [*hereinafter* 'GATT 1994'].
[78]James Andrew Lewis, *The US Really Does Want to Constrain Commercial Espionage: Why does Nobody Believe It?*, LAWFARE, July 1, 2016, https://www.lawfareblog.com/us-really-does-want-constrain-commercial-espionage-why-does-nobody-believe-it, (last visited Oct. 2, 2017).
[79]James Andrew Lewis, Center for Strategic and International Studies, Conflict and Negotiation in Cyberspace 50 (Feb. 2013).
[80]Malawer, *supra* note 36.

V. CONCLUSION

The U.S-China cyber economic espionage dispute amplifies the absence of any straightforward or uniform adjudication process for a state to undertake in case of such an occurrence. Through the above analysis, this article proves that an action by the U.S against China at WTO would not have been successful. Considering these difficulties in adjudicating the matter at WTO at present, U.S. probably availed the right alternative by entering into an agreement with China in September 2015 (also known as Xi-Obama Agreement) to not engage in economic cyber espionage activities against each other.[81]

The agreement states:

> *"that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."*[82]

Subsequently, China entered into a similar agreement with United Kingdom as well.[83] Not long after, a G-20 communiqué extended the Xi-Obama agreement to 18 other countries.[84] In the absence of any

[81] Matthew Dahl, *Agreements on Commercial Cyber Espionage: An Emerging Norm?* LAWFARE https://www.lawfareblog.com/agreements-commercial-cyber-espionage-emerging-norm.

[82]James Andrew Lewis, *The US Really Does Want to Constrain Commercial Espionage: Why does Nobody Believe It?*, LAWFARE, July 1, 2016, https://www.lawfareblog.com/us-really-does-want-constrain-commercial-espionage-why-does-nobody-believe-it, (last visited Oct. 2, 2017).

[83]Matthew Dahl, *Agreements on Commercial Cyber Espionage: An Emerging Norm?*, LAWFARE, December 4, 2015, https://www.lawfareblog.com/agreements-commercial-cyber-espionage-emerging-norm, (last visited Oct. 2, 2017).

[84]Martin Libicki , *The Coming of Cyber Espionage Norms*, NATO CCD COE PUBLICATION, Tallinn 1, https://ccdcoe.org/sites/default/files/multimedia/pdf/Art%2001%20The%20Coming%20of%20Cyber%20Espi nage%20Norms.pdf, (last visited Feb. 20, 2018).

international law on cyber espionage, many scholars acknowledged this trend as an emerging norm in international law.[85] In other words, the practice of entering into agreements with other states to prevent economic cyber espionage was becoming increasingly recognized and accepted in the international community.[86] If such a practice attains the status of an international norm, then no derogation from the same would be permissible.[87] It received sufficient support at the G-20 Summit in November 2015 to be recognized as an international norm according to international law experts.[88] However, in practice, such diplomatic agreements go only so far as to enforce a legal order on cyber espionage. They as are not binding on the parties as they are not treaties drafted with the constitutional assent of the Senate.[89] Hence, ensuring compliance will be a task for these states. For instance, two years after the Xi-Obama Agreement, three Chinese individuals from a Chinese cyber-security firm were caught hacking into the computer systems of a few U.S. companies for commercial gain.[90] Therefore,

[85]Matthew Dahl, *Agreements on Commercial Cyber Espionage: An Emerging Norm?*, LAWFARE, December 4, 2015, https://www.lawfareblog.com/agreements-commercial-cyber-espionage-emerging-norm, last visited Oct. 2, 2017; Buchan, R.J. *The International Legal Regulation of Cyber Espionage: Legal, Policy and Industry Perspectives*, NATO CCD COE PUBLICATIONS, Tallinn, 65-86, http://eprints.whiterose.ac.uk/98791/10/Russell_The%20International%20Legal%20Regulation%20of%20Cyber%20Espionage%20_comments%20combined.pdf, (last visited Feb. 18, 2018).

[86]Martin Libicki , *The Coming of Cyber Espionage Norms*, NATO CCD COE PUBLICATION, Tallinn 1, https://ccdcoe.org/sites/default/files/multimedia/pdf/Art%2001%20The%20Coming%20of%20Cyber%20Espionage%20Norms.pdf, (last visited Feb. 20, 2018).

[87]*Id.*

[88]Jack Goldsmith and Robert D. Williams, *The Chinese Hacking Indictments and the Frail "Norm" Against Commercial Espionage*, LAWFARE, November 30, 2017, https://www.lawfareblog.com/chinese-hacking-indictments-and-frail-norm-against-commercial-espionage, (last visited Feb. 18, 2018).

[89]Matthew Dahl, *Agreements on Commercial Cyber Espionage: An Emerging Norm?*, LAWFARE, December 4, 2015, https://www.lawfareblog.com/agreements-commercial-cyber-espionage-emerging-norm, (last visited Oct. 2, 2017).

[90]Jack Goldsmith and Robert D. Williams, *The Chinese Hacking Indictments and the Frail "Norm" Against Commercial Espionage*, LAWFARE, November 30, 2017,

entering into commercial cyber espionage agreements does not solve the problem for states.

It also depends on the drafting of the agreement. The Xi-Obama agreement was criticized for the specificity of the agreement[91] the loopholes of which can be interpreted to one's advantage. This is similar to how China, through its national security defense to the recent cyber-attack, took advantage of the loopholes in the Xi-Obama Agreement.[92] In case a state seeks to enter into commercial cyber espionage agreements in the future, the parties should clearly lay down the activities that constitute a violation and those that do not. In the absence of such clarity, such agreements would not serve the purpose.

An alternative to tackle this issue is by expanding the application of TRIPS Agreement to specifically address cyber espionage for trade and commercial purposes. This would involve detailed discussions of all the WTO members to find solutions to the above discussed problems in the TRIPS Agreement as it exists currently (such as territorial limitation under National Treatment principle, ambiguity over whether commercial cyber espionage constitutes breach of confidence, etc).

Another avenue could be to pursue a general diplomatic conference outside WTO to address a wide range of issues with respect to cyber espionage including trade and commercial aspects. Such a conference

https://www.lawfareblog.com/chinese-hacking-indictments-and-frail-norm-against-commercial-espionage, (last visited Feb. 18, 2018).

[91]James Andrew Lewis, *The US Really Does Want to Constrain Commercial Espionage: Why does Nobody Believe It?*, LAWFARE, July 1, 2016, https://www.lawfareblog.com/us-really-does-want-constrain-commercial-espionage-why-does-nobody-believe-it, (last visited Oct. 2, 2017).

[92]Jack Goldsmith and Robert D. Williams, *The Chinese Hacking Indictments and the Frail "Norm" Against Commercial Espionage*, LAWFARE, November 30, 2017, https://www.lawfareblog.com/chinese-hacking-indictments-and-frail-norm-against-commercial-espionage, (last visited Feb. 18, 2018).

would be similar to the naval disarmament conferences during the inter-war period where members of the League of Nations took an initiative to actualize the ideology of disarmament.[93] Until the time such an activity is undertaken, there seems very little success of adjudicating a commercial cyber espionage issue at the WTO.

[93]Stuart Malawer, *Cyber Warfare: Law and Policy Proposals for U.S. and Global Governance*, 58 Virginia Lawyer 28 (Feb. 2010).