

# Research on the Standard of “National Security” in the U.S. Export Controls on Technologies and Analysis of Its WTO Obligations --Thinking Raised by U.S. Ban on Huawei

Zhenyuan Guo<sup>1</sup>

<sup>1</sup>*LL.M. of Melbourne Law School, The University of Melbourne, Australia*

**Abstract:** “National security” is an important factor for a country to decide on export control, but its standards in practice are rarely analyzed. The case of “U.S. Ban on Huawei” in the United States showed that the standards of “national security” in export control on technologies in the U.S has great generality and vagueness, even has become an excuse for political considerations. This paper starts with the development of U.S. export control system, on the basis of the analysis of its own legal system, combined with the “national security” and cases in the U.S. foreign investment laws, trying to research the standard of “national security” in the U.S. export control of technologies. Further, through the analysis of the “security exception” clause in the WTO system, the author proves that the practice of the United States in the case of “Huawei ban” and its attitude towards the export control of technologies has violated its WTO obligations.

**Key Words:** U.S. Export Controls on Technologies; Entity List; national security; GATT Article XXI

## I. INTRODUCTION

On May 17, 2019, the Bureau of Industry and Security (BIS, the sub-department under Ministry of Commerce of the United States, which responsible for export controls) has decided to add Huawei Technologies Co., Ltd (Huawei) and its non-U.S. affiliates to the Entity List, based on the *Export Administrations Regulations* (EAR). BIS believed that Huawei had been involved in activities contrary to the national security or foreign policy interests of the United States. This treatment was nearly a complete blockade,

namely that Huawei and its non-U.S. affiliates could never import any High-tech product components from any American companies. Just one year ago, the Trump’s administrations banned another Chinese High-tech company ZTE Co., Ltd (ZTE). Indeed, which cases are just epitomes of the U.S. export control of dual-use commodities and technologies. Until 2019, there are more than 1000 “Entities” lie in the Entity List<sup>1</sup>, which are subject to specific license requirements for the export, reexport and/or transfer (in-country) of specified items.

One of key factors that the BIS will consider in export control is the “national security”, but the real standard of “national security” is never clear. Neither the EAR and relevant regulations of the U.S. nor other official definitions has explained what the “national security” is, and also seldom scholars have researched this topic. Just focus on the cases of Huawei and ZTE, different circumstances in two cases has led to the same treatment, particularly when no evidence has shown that Huawei has violated the U.S. export control regulations and violated U.S. “national security”. So that a question has been raised that whether the issue of “national security” in export control is transparent and accountable and what is the real standard, or it is just an excuse of commercial or political considerations. For answering this question, in Part II, the cases of Huawei and ZTE will be discussed firstly

<sup>1</sup> Actually, the Entity List contains businesses, research institutions, government and private organizations, individuals, and other types of legal persons. See as ‘Entity List’ <<https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list>>.

as typical cases recently, to find the same and different circumstances between them, discussing why the standard of “national security” in the U.S. export control is seemed to be too mystical and contains a lot of commercial or political considerations. In Part III, this paper will try to find the meaning of “national security” in the U.S. export control regulations firstly; In the Part IV, in the light of the similar background and purpose of the U.S. export control regulations and foreign investment control regulations, the same concept of “national security” in the U.S. investment laws will be referred. In part V, this paper will try to clarify the common standards of “national security” both for export control and foreign investment control. In part VI, this paper will discuss whether the U.S. attitude and measures fit its WTO obligation—from GATT Article XXI about “national security”. The last part will be a conclusion

## II. THE CONFUSING STANDARD OF “NATIONAL SECURITY”: THINKING RAISED BY THE U.S BAN ON HUAWEI

Before Huawei, ZTE, another Chinese High-tech company that is also expertized at telecommunication technology and services, has been added to Entity List twice in 2016 and 2018, respectively. In view of the two companies are too similar in their country of origin (China), area of expertise (Telecom equipment maker) and the scale (no.1 of Huawei, no.4 of ZTE globally<sup>2</sup>), it could be easily imagined that the circumstance of the two case should be also quite similar, since they have received the same treatment (added to Entity List) with the same excuse (national security). Is that true? Unfortunately, no. The unclear standard of “national security” in the two cases has actually showed different measures.

The timeline of the two sanctions to ZTE is actually quite clear and it could be easily seen in what terms, ZTE has violated the U.S. “national security”. The first sanction was issued on March 7, 2016, the BIS decided to add ZTE to the Entity List, based on ZTE’s cooperation projects with Iran, North Korea, Syria and other embargoed countries, and

<sup>2</sup>‘Huawei Now World’s Largest Telecom Equipment-Maker - Caixin Global’ <<https://www.caixinglobal.com/2018-03-19/huawei-now-worlds-largest-telecom-equipment-maker-101223256.html>>.

accused ZTE of serious violations of the country’s export restrictions<sup>3</sup>. On March 24 the first sanction was provisionally removed, that the BIS gave ZTE a Temporary General License in the condition of several penalties and ZTE must remove the positions of senior executives who have participated in violations<sup>4</sup>. On March 2017, after four times of extension of validity of the Temporary General License<sup>5</sup>, and ZTE has acknowledged all alleged behaviors, the BIS formally removed ZTE from the Entity List with a fine of nearly \$ 2 billion and a probationary period of seven years<sup>6</sup>. Nevertheless, On April 15, 2018, the BIS announced to activate the suspended denial order to ZTE, because of 380 ZTE’s admitted violations of the U.S. laws, including pattern of deception, false statements, and repeated violations of the U.S. law<sup>7</sup>.

Throughout the case of ZTE, it was actually reasonable and persuasive to penalty ZTE based on the reason of “national security”. Briefly, the U.S. law has clearly banned the export of U.S.-made products to Iran, North Korea, Syria and other embargoed countries in the U.S. export control laws, as those countries were designated as state sponsors of terrorism<sup>8</sup>. ZTE has purchased controlled items and reexported or through intermediary trading company for reexport to embargoed countries. What’s worse, some violations happened during the investigation and probationary period. Those pattern of

<sup>3</sup> ‘Federal Register: Additions to the Entity List’ <<https://www.federalregister.gov/documents/2016/03/08/2016-05104/additions-to-the-entity-list>>.

<sup>4</sup> ‘Temporary General License’, *Federal Register* (24 March 2016) <<https://www.federalregister.gov/documents/2016/03/24/2016-06689/temporary-general-license>>.

<sup>5</sup> The four extension was issued in Jun 28, 2016; Aug 19, 2016; Dec 11, 2016 and Feb 24, 2017, see as ‘Document Search Results for “ZTE”’, *Federal Register* <[https://www.federalregister.gov/documents/search?conditions%5BaGENCY\\_IDS%5D%5B%5D=54&conditions%5Bterm%5D=ZTE&order=oldest](https://www.federalregister.gov/documents/search?conditions%5BaGENCY_IDS%5D%5B%5D=54&conditions%5Bterm%5D=ZTE&order=oldest)>.

<sup>6</sup> ‘In the Matter of: Zhongxing Telecommunications Equipment Corporation ZTE Plaza, Keji Road South Hi-Tech Industrial Park Nanshan District, Shenzhen China; ZTE Kangxun Telecommunications Ltd. 2/3 Floor, Suite A, Zte Communication Mansion Keji (S) Road Hi-New Shenzhen, 518057 China Respondent’; Order Activating Suspended Denial Order Relating to Zhongxing Telecommunications Equipment Corporation and Zte Kangxun Telecommunications Ltd.’, *Federal Register* (23 April 2018) <<https://www.federalregister.gov/documents/2018/04/23/2018-08354/in-the-matter-of-zhongxing-telecommunications-equipment-corporation-zte-plaza-keji-road-south>>.

<sup>7</sup>Ibid.

<sup>8</sup>Ian F Fergusson and Paul K Kerr, *The U.S. Export Control System and the President’s Reform Initiative* (No R41916, Congressional Research Service, 2014), 4

deception, false statements, and repeated violations has further aggravated the U.S. government's dissatisfaction and has directly caused the second sanction.

So that what about Huawei? Did there were evidence that Huawei has purchased the U.S.-made products and reexported to embargoed countries or Huawei has cheated the U.S. government as what the ZTE has ever done? No, compared with very detailed accuse to ZTE<sup>9</sup>, in the decision of Huawei, the BIS was just able to use ambiguous descriptions to express that Huawei and its affiliates has been involved in activities contrary to the national security or foreign policy interests of the U.S. In the document of the decision, BIS cited Huawei's allegations in the U.S. District Court for the Eastern District of New York on 13 counts of violating the U.S. law. However, under the circumstance that those allegations were far away from a confirmed judgement, the amount of involved Huawei's non-U.S. affiliates has reached to exaggerated sixty-eight entities locates in twenty-six destinations<sup>10</sup>. In the light of the intensified trade-war between the U.S. and China, this sanction to Huawei was seemed not persuasive that such a wide scope of severe sanctions be made on the basis of such insufficient evidence. Accordingly, there are possible other subtle standards for BIS to consider "national security" in export control of dual-use commodities and technologies. And this paper will try to find these real standards of "national security" which hiding beneath the surface of the water in the following parts.

### III. FINDING FROM THE HISTORY AND FRAMEWORK OF US EXPORT CONTROL INTECHNOLOGIES

#### A. Historical development of US export control in technologies

The origin of the U.S. export control in technologies could date back from the Cold War era, when the western world tried to establish a multilateral system to control export and import of key goods and technologies to Soviet Union and its

<sup>9</sup> The BIS has listed each involved company and each export destination. See as 'Federal Register: Additions to the Entity List' (n 3). <<https://www.federalregister.gov/documents/2016/03/08/2016-05104/additions-to-the-entity-list>>.

<sup>10</sup> 'Federal Register: Addition of Entities to the Entity List' <<https://www.federalregister.gov/documents/2019/05/21/2019-10616/addition-of-entities-to-the-entity-list>>.

allies which could threaten the "national security" of the western world<sup>11</sup>. The original version of the U.S. export control was aiming to prevent the proliferation of arms technologies to the Eastern bloc states and other non-state actors, like international terrorist group<sup>12</sup>. At that time, the U.S. export control was mainly represented by *The Export Control Act* of 1949<sup>13</sup>, and the Mutual Defense Assistance Control Act in 1951<sup>14</sup>. Both acts have been consisted with the NATO' perspective to protect the political and territorial security of capitalist countries and restrict the Soviet countries' expansion<sup>15</sup>. There is no doubt that considerations of military and politics were obviously the key factors of "national security" in Cold War and the U.S. focused on the arms export control in governmental level. Until now, to prevent other states or non-state actors obtaining military capabilities that could threaten the U.S. national security, is still an important objective of the export control<sup>16</sup>.

From 1960s, the military-related technologies were broadly owned by private companies and these companies wanted to create more commercial interest by the technology<sup>17</sup>. In the light of the growing global trade, the U.S. government turned to focus on private sectors, to prevent those advanced technologies from being exported and used in wrong ways<sup>18</sup>. In that circumstance, *The Export Administration Act* (EAA) of 1969 was issued, aiming to find a balance between protecting

<sup>11</sup> Christopher F F. Corr, 'An Umbrella in a Hurricane: Cyber Technology and the December 2013 Amendment to the Wassenaar Arrangement' (2015) 13 *Northwestern Journal of Technology and Intellectual Property* 153., 159

<sup>12</sup> Fitzgerald DR, 'Leaving the Back Door Open: How Export Control Reform's Deregulation May Harm America's Security' (2014) 15 *North Carolina Journal of Law and Technology* 65., 68

<sup>13</sup> EAA of 1949 was closely connected with North Atlantic Treaty Organization (NATO) and Coordinating Committee for Multilateral Export Controls (COCOM). The NATO and COCOM were also established in 1949, and both organizations played roles in the export control of military products to Soviet Union and its allies.

<sup>14</sup> The Mutual Defense Assistance Control Act further prohibited U.S. economic assistance to Soviet Union's trade partners.

<sup>15</sup> Tamotsu Aoi, *Historical Background of Export Control Development in Selected Countries and Regions* (Center for Information on Security Trade Controls)., 7

<sup>16</sup> Ilenan Ros-Lehtinen, 'An Imperfect Balance: ITAR Exemptions, National Security, and U.S. Competitiveness' (2013) 1(2) *National Security Law Journal* 43., 43

<sup>17</sup> Hamed Alavi and Tatsiana KHamichonak, 'EU and US Export Control Regimes for Dual Use Goods: An Overview of Existing Frameworks' (2017) 17 *Romanian Journal of European Affairs* 59., 67

<sup>18</sup> Since that time, the U.S. government thought the procurement of existing and mature military technologies was beneficial, so that R&D by private sectors were encouraged. See as Ibid.

the U.S. national security and facilitating the U.S. international trade in technologies<sup>19</sup>. After several revisions, the EAA has been completely rewritten in 1979, and this version has become the basis of the export control even in the U.S. today<sup>20</sup>. The EAA formally authorized the President to control the exports of dual-use products and technologies<sup>21</sup>, and allocated the Department of Commerce to implement this power<sup>22</sup>. Based on EAA, the *Export Administrations Regulations*<sup>23</sup> (EAR) in very detailed regulations rules the Department of Commerce's power to manage the export and re-export of dual-use products and technology<sup>24</sup>. In addition, the *International Emergency Economic Powers Act* (IEEPA) of 1977 has also authorized the President to block transactions and freeze assets to any states, entities or individual if there is an unusual and extraordinary threat to the national security, foreign policy, or economy of the United States<sup>25</sup>. All of acts and regulations above substantially constitute current export control on High-tech products of the U.S. currently. Meanwhile, the U.S. government has actually clarified the boundary of the export control between arms and technologies. For instance, the *Arms Export Control Act* (AECA) and related *International Traffic in Arms Regulations* (ITAR) specifically concentrate the export control of arms products and services. Briefly, the U.S. has applied two overlapping management system for the export control of defense products and technologies<sup>26</sup>.

From the overall historical development of the U.S. export control, it could be seen that though the export control of arms and technologies are separated now, but their origins were based on the export control of military technology and products during the Cold War. There were two main reason

for the independence of export control of technologies. On the one hand, high-tech technology has been broadly owned by the private sector, and these dual-use products have the possibility of being used for military purposes. On the other hand, based on the commercial value of dual-use technology, the U.S. need to seek balance between export control and international trade<sup>27</sup>. So that, at least, it could be clear that one of the standards of "national security" for the U.S. export control of dual-use products is the same as its original version half century ago—the threat to national security at the military level.

## B. Current framework of US export control in technologies

### 1. Purposes of EAA and EAR

As discussed above, current US export control in dual-use products is mainly based on the EAR, which actually implements the EAA<sup>28</sup>. In view of EAA and EAR, there are three main purposes. The first purpose has inherited from export control in arms, to prevent the proliferation of weapons of mass destruction and the improvement of other countries' military capacity which would play detrimental role to the national security of the U.S.; the second purpose is to be coordinated with the foreign policy and declared international obligations, be coordinate with other multilateral control arrangement, including Nuclear Suppliers Group, the Australia Group, and the Missile Technology Control Regime, etc.; the last purpose is to protect the domestic economy, prevent certain commodities in short supply or serious inflation.<sup>29</sup>

These three purposes represent three different dimensions of concern, the national security in military level, the international obligations in multilateral control arrangement, and the national security in economy. In the light of those multilateral control arrangements are also aiming to regulate export and import of core arms technologies, such nuclear, missile, biological and chemical weapons, etc.<sup>30</sup> So that in

<sup>19</sup>Dvorin SM, 'The Export Administration Act of 1979: An Examination of Foreign Availability of Controlled Goods and Technologies' [1980] *Northwestern Journal of International Law & Business* 179., 194

<sup>20</sup>Aoi (n 15)., 9

<sup>21</sup>The "dual-use" is now officially defined as "has civil applications as well as terrorism and military or weapons of mass destruction (WMD)-related applications" and see as CFR/EAR §730.3

<sup>22</sup>SM (n 19)., 68

<sup>23</sup>EAR is a set of regulations of Electronic Code of Federal Regulation (e-CFR) §730-774

<sup>24</sup>Alavi and KHamichonak (n 17)., 68

<sup>25</sup>Aoi (n 15)., 9

<sup>26</sup>Belay Seyoum, 'National Security Export Control Regimes: Determinants and Effects on International Business' (2017) 59(6) *Thunderbird International Business Review* 693., 694

<sup>27</sup>Alavi and KHamichonak (n 17)., 67

<sup>28</sup>Ibid., 68

<sup>29</sup>*Export Administration Act Of 1979*, 50 USC app. 2402, s 3. (2).; *Export Administration Regulations* CFR §730.3

<sup>30</sup>Felicity Vabulas and Duncan Snidal, 'Organization without Delegation: Informal Intergovernmental Organizations (IIGOs) and the Spectrum of

terms of considerations of national security, the first and second purposes are both concentrating on military threat in essence. Meanwhile, the third purpose of national economic security is seemed comparatively specific. As the statements of “serious inflationary impact of foreign demand” in section 3. (2). (C) of EAA, and “protect the United States from the adverse impact of the unrestricted export of commodities in short supply” in CFR §730.3 of EAR, the standards for national economic security is seemed to be very conservative and defensive. Is that true? Perhaps not.

## 2. Scope of application and classifications

§734.3 of EAR evidently illustrates its ambitiousness in the scope of application, the influencing factors of general prohibitions and the classifications. From its exhaustive statement, all items in the US, including in a U.S. Foreign trade Zone, all U.S. origin items, even all foreign-made commodities that are “bundled” with controlled U.S.-origin commodities or software, and certain commodities produced outside the U.S. that is a direct product of the U.S.-origin technology or software, etc. are subject to EAR<sup>31</sup>. The EAR further regulates ten general prohibitions<sup>32</sup> with five types of factors to determine the applicability of the general prohibitions: classification; destination; end-user; end-use and conduct<sup>33</sup>. Afterwards, the EAR establishes a Commerce Control List (CCL), which lists items that are subject to the export control of BIS, such as commodities, technologies and software<sup>34</sup>. In detail, the CCL divides ten categories<sup>35</sup> and five

groups<sup>36</sup> of items with certain serial numbers. Also, the CCL sets each controlled category an Export Control Classification Numbers (ECCN) to describe the reason for control<sup>37</sup>.

It could be easily seen that the EAR is actually quite ambitious and offensive but not conservative. Firstly, the scope of application of EAR and its CCL has virtually covered all the goods and its relevant technologies which originate in the U.S. What’s more, as long as be “bundled” with controlled U.S.-origin commodities or software, even foreign-made commodities will be controlled<sup>38</sup>. Further, “end-use”<sup>39</sup> and “end-user”<sup>40</sup> are “killer factors” to determine the applicability of control, which means even the commodity is not on the CCL, it could still be restricted as long as the commodity be regarded to be utilized for a military end-use or exported to an entity involved in proliferation or an entity is believed to be involved in weapons proliferation<sup>41</sup>. In accordance with such ambitious EAR’s attitude with national economic security, it could be imagined that, the consideration of national economic security ought to be the key standard of “national security”, though it can’t find more about the detail from text materials of EAR.

It also worth noting that, the “NS” (National Security) is appeared as an independent and parallel reason amongst all the fourteen ECCNs. In consideration of others of ECCN are all clear and straight statement, such as “AT” (Anti-Terrorism), “CC” (Crime Control), “MT” (Missile Convention), “NP” (Nuclear Nonproliferation) and “SS” (Short Supply), etc. The “national security” here is still seemed to be a conceptual and principled “fallback provision” with no actual standards and conditions and needs to be further defined.

---

Intergovernmental Arrangements’ (2013) 8(2) *The Review of International Organizations* 193., 199

<sup>31</sup> Of course, arms products and technologies are not subject to EAR, but to other arms export control regulations such as ITAR and NRC. See as §734.3. (b) of EAR

<sup>32</sup> In detail, the ten prohibition are the following: 1) Export and reexport of controlled items to listed countries; 2) Reexport and export from abroad of foreign-made items incorporating more than *a de minimis* amount of controlled US content; 3) Reexport and export from abroad of the foreign-produced direct product of US technology and software; 4) Engaging in actions prohibited by a denial order; 5) Export or reexport to prohibited end-users or end-users; 6) Export or re-export to embargoed destinations; 7) Support of Proliferation Activities; 8) In transit shipments and items to be unladen from vessels or aircraft; 9) Violation of any order, terms, and conditions; 10) Proceeding with transactions with knowledge that a violation has occurred or is about to occur.

<sup>33</sup> EAR, §736.2. (a)

<sup>34</sup> Ian F Fergusson and Paul K Kerr, *The U.S. Export Control System and the President’s Reform Initiative* (No R41916, Congressional Research Service, 2014), 3

<sup>35</sup> The ten categories are: 0) nuclear materials, facilities and equipment; 2)

---

chemicals, microorganisms and toxins; 3) materials processing; 4) electronics; 5) computers, 6) telecommunications and information security; 7) lasers and sensors; 8) navigation and avionics; 9) marine; 10) aerospace and propulsion. See as §738.2 (a) of EAR

<sup>36</sup> Five groups are divided into: A) Equipment, Assemblies and Components, B) Test, Inspection and Production Equipment, C) Materials, D) Software, E) Technology, see as §738.2 (b) of EAR

<sup>37</sup> §738.2. (d) of EAR

<sup>38</sup> §734.3. (b) of EAR

<sup>39</sup> End use refers to the actual and final use of exported or re-exported items.

<sup>40</sup> End user refers to the importer who accepts and eventually uses the export or re-export items

<sup>41</sup> Fergusson and Kerr (n 8), 4

#### IV. “NATIONAL SECURITY” IN THE U.S. FOREIGN INVESTMENT LAWS

##### A. Consistency of BIS and CFIUS on “national security”

For further clarifying the standard of “national security” in the U.S. export control on dual-use products and technologies, the same concept in the U.S. investment foreign investment laws could be referred. The history of the U.S. foreign investment laws could also date back from the WWI, WWII and Cold War, that the U.S has set a series of laws to control the foreign direct investment (FDI) in the state of war or emergency to maintain the U.S. economic order and national security<sup>42</sup>. In 1970s, the same period with the announcement of EAA of 1979, the current authority of the U.S. foreign investment control has been established in 1975—the Committee on Foreign Investment in the United States (CFIUS)<sup>43</sup>. The CFIUS was initiated to collecting information about the potential risks in foreign investment and reporting them to the Congress<sup>44</sup>. With the successive enactments of several amendments and laws, especially the *Foreign Investment and National security Act* of 2007 (FINSAs)<sup>45</sup>, the CFIUS acquired the contemporary power in investigation of foreign investment<sup>46</sup>. Briefly, CFIUS could review any covered transactions whenever there is any possible impact upon national security<sup>47</sup>. From the concise history and function of CFIUS, it could be seen that the U.S. foreign investment laws have nearly developed in the same time with export control regulations and also aimed to deal with the potential risks in national security, military and economic<sup>48</sup>. Therefore, upon

<sup>42</sup> Such as *Trading with the Enemy Act* of 1917 during WWI, *National Security Act* of 1947 during WWII, *Defense Production Act* of 1950 and *The National Emergencies Act* of 1976 during the Cold War

<sup>43</sup> Christopher M Tipler, ‘Defining “National Security”: Resolving Ambiguity in the CFIUS Regulations’ (2014) 35 *University of Pennsylvania Journal of International Law* 62., 1226

<sup>44</sup> Joshua C Zive, ‘Unreasonable Delays: CFIUS Reviews of Energy Transactions’ (2013) 3 *Harvard Business Law Review* 169., 170

<sup>45</sup> i.e., 1988 Exon-Florio Amendment, 1993 Byrd Amendment and the most important, *Foreign Investment and National security Act* of 2007 (FINSAs)

<sup>46</sup> Jingli Jiang and Gen Li, ‘CFIUS: For National Security Investigation or for Political Scrutiny’ (2013) 9 *Texas Journal of Oil, Gas, and Energy Law* 67., 70

<sup>47</sup> Michael V Seitzinger, *Foreign Investment in the United States: Major Federal Statutory Restrictions* (No RL331003, Congressional Research Service, 2013), 14

<sup>48</sup> Actually, before Exon-Florio Amendment of 1988, the CFIUS was short of enforcement power, and the U.S. relied on other regulatory mechanism to protect the national security, including the export controls such as ITAR and

their same perspective, the connotation of the “national security” in the U.S. foreign investment laws could be referential to that of export control regulations, and this paper will mainly focus on economic “national security”.

##### B. How does CFIUS rule the national security

CFIUS concentrates on the review raised by national security concerns, however, there is also none of definition of what the “national security” is, but limited guidance to interpret it<sup>49</sup>. Which was highly because of the rapid evolvement of the concept of “national security” in response to the concerns with the national defense and economic security with a series of events<sup>50</sup>. In detail, the FINSAs has listed 11 factors of national security<sup>51</sup> and further let CFIUS to publish a guidance to interpret them in Federal Register<sup>52</sup>.

##### 1. Factors to national security

The FINSAs lists a board range of factors for the CFIUS to consider the “national security” of a transaction in §721(f), in which the majority of these factors could be regarded as be consistent with three purposes of EAR and EAA<sup>53</sup>. Namely, amongst 11 factors, (1) - (3) are concern with the maintenance and promotion of national defense capacity<sup>54</sup>; (4) and (9) show the consistency with foreign policy interests and obligations, especially the EAA of 1979 is particularly

EAA. See Susan W Liebler and William H Lash III, ‘Exon-Florio: Harbinger of Economic Nationalism’ (1993) 16 *Cato Review of Business and Government* 44., 44-45

<sup>49</sup> 50 U.S.C §2170 (b)

<sup>50</sup> i.e., 9/11 and the proposed CNOOC and DPW transactions have raised the concern of national security intensively. See as, Mendenhall James and Baker Stewart, ‘Economic Politics and National Security: A CFIUS Case Study’ in *American Society of International Law. Proceedings of the Annual Meeting* (Cambridge University Press, 2008), 249

<sup>51</sup> *Foreign Investment and National security Act* of 2007, §721(f)

<sup>52</sup> ‘Guidance Concerning the National Security Review Conducted by the Committee on Foreign Investment in the United States’ (2008) 73 (No. 236) *Federal Register* 74567.

<sup>53</sup> As concluded above: The first purpose is to prevent the proliferation of weapons of mass destruction; The second purpose is to be coordinated with the foreign policy and declared international obligations, be coordinate with other multilateral control arrangement; the last purpose is to protect the domestic economy, prevent certain commodities in short supply or serious inflation.

<sup>54</sup> FINSAs §721(f), (1) domestic production needed for projected national defense requirements, (2) the capability and capacity of domestic industries to meet national defense requirements, including the availability of human resources, products, technology, materials, and other supplies and services, (3) the control of domestic industries and commercial activity by foreign citizens as it affects the capability and capacity of the United States to meet the requirements of national security.

mentioned<sup>55</sup>; (10) also expresses the concern about the long-term requirements for sources of energy and other critical resources and material<sup>56</sup>; (11) is a general “fallback provision” in case of particular situation<sup>57</sup>. Apart from those factors which are consistent with purposes of the U.S. export control regulations, others of factors are comparatively unique and worthy of mention. (5)-(7) focus on the U.S. capacity in international technological leaderships and the potential national security-related effects on the U.S. infrastructure and technologies<sup>58</sup>; (8) specially expressed the concern with foreign government-controlled transactions<sup>59</sup>.

## 2. Guidance concerning the national security review

The guidance was issued for “regarding the types of transactions that CFIUS has reviewed and that have presented national security considerations<sup>60</sup>”. However, this guidance was designed to be “necessarily” and “does not purport to describe all national security considerations that CFIUS may identify and analyze in reviewing a transaction”. Accordingly, this guidance has no “binding power” but works as “reference only” to assist CFIUS to determine whether a transaction is involved in national security issues<sup>61</sup>. Two categories of

transactions that will be involved in national security concerns are mentioned in this guidance: (1) “those raising concerns due to the nature of the U.S. business over which foreign control is being acquired”, and (2) “those raising concerns due to the nature of the foreign person who acquires control over the U.S. business”.<sup>62</sup> Unlike categories of specific industries and products in EAR for export control, the guidance only provides very general and conceptual subcategories<sup>63</sup>.

The first category including certain circumstances that CFIUS will review a transaction in four subcategories: (a) contractors or suppliers to the U.S. government; (b) products or services of the U.S. businesses may have implications for U.S. national security; (c) companies involve critical infrastructure and (d) production of certain types of advanced technologies<sup>64</sup>. Finally, the guidance notes that transactions should be reviewed by CFIUS are generally related to “technology, goods, software, or services that are subject to U.S. export controls”<sup>65</sup>. The second category highlights the risks by foreign government-controlled transactions, particularly when “contracts between the U.S. business and U.S. Government agencies for goods and services relevant to national security”<sup>66</sup>. This category specifically raises two major concerns, (a) foreign government-controlled transactions and (b) exceptional corporate reorganization that the foreign person acquires control of a U.S. business<sup>67</sup>. When considering a foreign government-controlled transaction, the guidance lists several factors to help identify whether there are national security risks<sup>68</sup>. The guidance did not provide clear explanation about the concern of exceptional corporate corporation, but just expresses that “CFIUS considers all

<sup>55</sup> Ibid, (4) the potential effects of the proposed or pending transaction on sales of military goods, equipment, or technology to any country— (A) identified by the Secretary of State— (i) under section (j) of the Export Administration Act of 1979 [section 2405(j) of this Appendix], as a country that supports terrorism..., (9) as appropriate, and particularly with respect to transactions requiring an investigation under subsection (b)(1)(B), a review of the current assessment of— (A) the adherence of the subject country to nonproliferation control regimes, including treaties and multilateral supply guidelines...

<sup>56</sup> Ibid, (10) the long-term projection of United States requirements for sources of energy and other critical resources and material

<sup>57</sup> Ibid, (11) such other factors as the President or the Committee may determine to be appropriate, generally or in connection with a specific review or investigation.

<sup>58</sup> Ibid, (5) the potential effects of the proposed or pending transaction on United States international technological leadership in areas affecting United States national security; (6) the potential national security-related effects on United States critical infrastructure, including major energy assets; (7) the potential national security-related effects on United States critical technologies;

<sup>59</sup> Ibid, (8) whether the covered transaction is a foreign government-controlled transaction, as determined under subsection (b)(1)(B);  
<sup>60</sup> Guidance Concerning the National Security Review Conducted by the Committee on Foreign Investment in the United States’ (n 52), 74568

<sup>61</sup> Specifically, the guidance clearly expressed as: “this discussion does not provide comprehensive guidance on all types of covered transactions that have presented national security considerations”; “...does not mean that CFIUS will necessarily determine that the transaction poses national security risk...does not identify the types of transactions that pose national security risk, and it should not be used for that purpose.” “...should not be interpreted to suggest that the U.S. Government encourages or discourages the types of

transactions described in this section”. See as Ibid., 74570

<sup>62</sup> Ibid.

<sup>63</sup> Tipler (n 43), 1243

<sup>64</sup> Guidance Concerning the National Security Review Conducted by the Committee on Foreign Investment in the United States’ (n 52), 74570; see also Tipler (n 43), 1243-1244

<sup>65</sup> Guidance Concerning the National Security Review Conducted by the Committee on Foreign Investment in the United States’ (n 52), 74571

<sup>66</sup> Ibid.

<sup>67</sup> Ibid.

<sup>68</sup> Those factors are: “whether governance structures are in place to ensure independence; the degree of transparency and disclosure of the purpose, investment objectives, institutional arrangements, and financial information of the investor; and the degree to which the investor complies with applicable regulatory and disclosure requirements of the countries in which they invest.” See as Ibid.

relevant national security factor”<sup>69</sup>. In the end, the guidance restates that it is not “binding” for CFIUS to identify national security in a covered transaction but just “referential”<sup>70</sup>.

#### V. COMMON STANDARDS OF “NATIONAL SECURITY” WITH CASE STUDIES—BOTH FOR BIS AND CFIUS

As introduced above, factors of “national security” in the U.S. export control regulations and foreign investment laws are virtually general and vague. However, with several typical cases, the common standard of “national security” both for BIS and CFIUS could be found, particularly the national security with economic concern. In the light of this paper focus on “national security” itself, so that the effects from Congress or BIS/CFIUS will not be particularly distinguished.

##### A. Foreign government related transactions and entities related to critical infrastructure and strategic assets

The first vital case from China National Offshore Oil Corporation’s (CNOOC, a powerful Chinese SOE) bid of California-based energy company, Unocal in 2005. This bid caused great controversy in the U.S, even been considered as “one of the of the most politically charged merger battles in U.S. history”<sup>71</sup> In the view of Senator Dorgan, the major concerns to reject this acquisition were as follows: oil and gas are strategic resources of the U.S; CNOOC is a SOE and be controlled by Chinese government; the possibility that the strategic resources of Unocal would be allocated to China.<sup>72</sup> Besides, the CNOOC’s proposal was heavily subsidized by Chinese Stated-owned companies and banks, which has led to the Congress thought this transaction was led by Chinese government rather than a complete commercial activity<sup>73</sup>, accordingly, CNOOC was believed to has unfair market advantages<sup>74</sup>. Besides, U.S. government also worried about

dual-use technologies of deep-sea exploration and drilling owned by Unocal would be transferred into the hands of Chinese government which could improve the capacity of Chinese military<sup>75</sup>. Similar concerns could also be found from other prohibited transactions such as DP world’s bid for P&O<sup>76</sup> and Anshan Iron & Steel Group Corp.’s proposed investment to Steel Development Co.<sup>77</sup>.

The entity with foreign government background is also an essential factor for BIS in export control. For instance, until 2019, amongst 106 entities from mainland China on the Entity List, about half of them have government background (3 national laboratory, 6 universities, 8 SOEs, 20 individuals and 22 scientific institutions with government background)<sup>78</sup>. From the entities raised above, another equally apparent factor—the classification could be easily found. In detail, 15 of entities are involved in aerospace field, 20 of entities are involved in computer science and electronic technology. Besides, there are also tens of entities are involved in nuclear, optics and energy.<sup>79</sup> It is obvious that the U.S. government is worrying about the critical infrastructure, strategic assets, sensitive and advanced products and technologies be acquired by China and improve Chinese military capacity<sup>80</sup>, through every possible SOEs and any kinds of government-background institutions. In CFIUS, this concern is reflected in the prevention of investment and acquisitions carried out by government-related companies. In BIS, this concern is reflected in the export control to government-related entities.

<sup>69</sup>Ibid.

<sup>70</sup> In the conclusion of the guidance, it states that “CFIUS does not issue advisory opinions as to whether a covered transaction raises national security considerations” and “This guidance may provide assistance to parties as they consider whether to file a voluntary notice with CFIUS”. See as Ibid., 74572

<sup>71</sup>Joshua W. Casselman, ‘China’s Latest Threat to the United States: The Failed CNOOC-Unocal Merger and Its Implications for Exon-Florio and CFIU’ (2007) 17 *Indiana International & Comparative Law Review* 155., 162

<sup>72</sup>Ibid., 163

<sup>73</sup>C Richard D’Amato, ‘National Security Dimensions of the Possible Acquisition of UNOCAL by CNOOC and the Role of CFIUS’ (at the U.S.-China Economic and Security Review Commission, 13 July 2005), 2

<sup>74</sup>Casselman (n 72), 166

<sup>75</sup>D’Amato (n 73), 4

<sup>76</sup>Deborah M Mostaghel, ‘Dubai Ports World Under Exon-Florio: A Threat to National Security or a Tempest in a Seaport?’ (2007) 70 *Albany Law Review* 583., 606

<sup>77</sup>Palmer D., ‘U.S. Lawmakers Cheer as China Steel Firm Backs out’, *Reuters* (19 August 2010) <<https://www.reuters.com/article/us-usa-china-trade/u-s-lawmakers-cheer-as-china-steel-firm-backs-out-idUSTRE67I40C20100819>>.

<sup>78</sup> 3 national laboratories are three National Supercomputing Center in Changsha, Guangzhou and Tianjin; 5 universities are public universities which are good at science, nuclear, computer and communications; SOEs and scientific institutions are also related to high-tech, including space, nuclear, computer and communications, etc. Individuals are basically the person in charge of SOEs and institutions above. See as ‘Entity List’ (n 1).

<sup>79</sup>Ibid.

<sup>80</sup>Hugo Meijer, *Trading with the Enemy: The Making of US Export Control Policy toward the People’s Republic of China* (Oxford University Press, 2016), 237



### B. Communication sector-related transaction

High technology is a frequent field that the CFIUS will review, and BIS has paid special attention recently, especially the telecommunication sector. Huawei has a checked history by CFIUS from its proposed acquisitions of two U.S. technology companies 3Com and 3leaf in 2008 and 2011, respectively<sup>81</sup>. In the failed acquisition of 3Com, Washington worried about national security because of the 3Com was a supplier to the U.S. military<sup>82</sup>. And in the case of 3Leaf, the transaction by Huawei was subject to several concerns, namely: the “close connections with the Chinese military”, because although Huawei is a completely private company, its founders have experience in serving the PLA; “disputes over the intellectual property rights”; the “allegations of financial support from the Chinese government”; and the suspicion of Chinese companies’ penetration of the U.S. telecommunication market, as telecommunication sector are special for national security<sup>83</sup>. Particularly, the Congress mentioned that “China has the means, opportunity, and motive to use telecommunications companies for malicious purpose”, and highlighted that priority of protection of critical infrastructure (telecommunication).<sup>84</sup>

There is no doubt that BIS has also paid great attention in communication sectors, such as the severe sanctions towards Huawei and ZTE. As introduced, from the reasons raised by BIS, the U.S. government believed that Huawei and ZTE has export controlled products to embargoed countries, like Iran, so that both companies were added into the Entity List. However, as the question has been posed above, there were no evidence that Huawei has violated the EAR, but Huawei has been even punished heavier. In that circumstances, this question can actually be answered by what the CFIUS emphases on telecommunication sector. Specifically, the

Congress has highlighted that the communication sector is unique for national security and Chinese companies’ penetration of the U.S telecommunication market<sup>85</sup>. Which is quite unusual that because in this statement, the U.S. has completely rejected the fair competition of Chinese telecom companies. Indeed, though Huawei and ZTE has been leading 5G equipment suppliers all over the world, the U.S. government has insisted a complete blockade, to prevent the entrance of Chinese 5G equipment into the U.S.<sup>86</sup>

In accordance with concerns above, the Congress actually held such a presumption that there will be a highly possible essential threat to the U.S. national security, as long as the powerful Chinese companies seeking to acquire sensitive U.S. assets, such as telecommunication sector<sup>87</sup>. For instance, on February, 2018, the U.S. Federal Communications Commission (FCC) has issued a proposed rule of “protecting against national security threats to the communications supply chain”.<sup>88</sup> In this document, FCC restates that security of America’s communications networks is an “critical element” of the U.S. national security, therefore, foreign equipment providers with potential risks should not be permitted to enter the telecommunications supply chain in the U.S.<sup>89</sup>

### C. U.S. capacity in international technological leaderships

The U.S. concern with telecommunication sector actually reflects another important but rarely mentioned concern—the U.S. international leadership in technologies, as described in FINSA<sup>90</sup>. The U.S. was known for its leading telecommunications powers over a century, but this leadership

<sup>85</sup>Ibid.

<sup>86</sup>Iris Deng and Yingzhi Yang, ‘US Ban on Huawei’s 5G Technology Could Be a Blessing in Disguise for the Chinese Brand, Say PR Experts | South China Morning Post’, *South China Morning Post* (25 February 2019) <<https://www.scmp.com/tech/big-tech/article/2187622/us-ban-huaweis-5g-technology-could-be-blessing-disguise-chinese-brand>>.

<sup>87</sup>Feldman (n 81), 311

<sup>88</sup>Federal Communications Commission., ‘Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs’ (2 May 2018) <<https://www.federalregister.gov/documents/2018/05/02/2018-09090/protecting-against-national-security-threats-to-the-communications-supply-chain-through-fcc-programs>>.

<sup>89</sup>Ibid.

<sup>90</sup>Above (n) 59, FINSA §721(f), (5) “the potential effects of the proposed or pending transaction on United States international technological leadership in areas affecting United States national security”

<sup>81</sup>Mark Feldman, ‘China’s Outbound Foreign Direct Investment: The US Experience’ (2017) 13 *International Journal of Public Policy* 304., 310

<sup>82</sup>Steven R Weisman, ‘Sale of 3Com to Huawei Is Derailed by U.S. Security Concerns’, *The New York Times* (online at 21 February 2008) <<https://www.nytimes.com/2008/02/21/business/worldbusiness/21iht-3com.1.10258216.html>>.

<sup>83</sup>Mike Rogers, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE* (No 112th Congress, U.S. House of Representatives, 8 October 2012), 11-34

<sup>84</sup>Ibid. 2

has collapsed since the emergence of 4G.<sup>91</sup> On the contrary, Chinese companies has taken the lead position on telecommunication sector, especially in the coming 5G revolution<sup>92</sup>. The telecommunication sector, a data-driven industry is “winner take most”<sup>93</sup>. That the U.S government believed the lose in the race of 5G will “forever reduce the economic and societal gains from leading the world in technology”<sup>94</sup>.

Indeed, the blockade towards Chinese telecommunication companies recently could nearly be corresponded with the “semiconductor war” between Japan and the U.S. more than 30 years ago. In 1980s, the Japanese companies occupied more than half global market share of semiconductor, and almost replaced the traditional international leading position by U.S. companies<sup>95</sup>. In 1980s, the semiconductor industry was seen as foundation of electronic revolution and also the “strategic industry” for “national security”<sup>96</sup>. To reduce the capacity of Japanese companies and protect the strengthen and market share of domestic companies, the U.S. government has applied several measures to defeat Japan, in terms of exchange rate agreements, bilateral measures and WTO framework, etc.<sup>97</sup>

Telecommunication industry, especially 5G and relevant technologies are “strategic assets” in the new generation, just like the semiconductor industry 30 years before. With the emergence of China-US trade war recent years and “specific” treatments towards Chinese powerful telecommunication companies, it is highly possible that the U.S is likely to repeat

what has been done 30 years ago. As a evidence recently, the U.S. Commerce Committee has held a hearing titled “Winning the Race to 5G and the Era of Technology Innovation in the United States”, aiming to discuss what policies are required to accelerate the deployment of 5G to keep America “competitive on the international stage”<sup>98</sup>. Also, just one month before the sanction to Huawei, as President Trump’s speech in April, 2019, the U.S. government “cannot allow any other country to out-compete the United States in this powerful industry of the future” and “the race to 5G is a race America must win”<sup>99</sup>. Therefore, the maintenance and promotion of U.S. international technology leadership should be an essential factor which hides behind the “national security”, and the “5Gcompetition” between U.S and China is a concentrated manifestation of this concern. Such concern has led Chinese telecommunication companies to be blocked from the U.S. market and be added into Entity List.

## VI. DOES U.S FIT ITS WTO OBLIGATIONS?

### A. Article XXI of GATT—An essential exception for national security

WTO framework is the common legal basis of the international trade, and the “national security” is actually closely linked to WTO rules<sup>100</sup>. Current WTO regulations has incorporated by references the GATT.<sup>101</sup> GATT free trade regime was designed to handle “technical” problems in transactional trade, especially the imports or exports of goods.<sup>102</sup> One of the basic functions of GATT was for sovereignty member states to negotiate with certain rights and obligations in the international trade<sup>103</sup>. The conflicts

<sup>91</sup>Zen Soo, ‘How US Went from Telecoms Leader to 5G Also-Ran without Challenger to China’s Huawei’, *South China Morning Post* (2 April 2019) <<https://www.scmp.com/tech/enterprises/article/3004325/how-us-went-telecoms-leader-5g-also-ran-without-challenger-chinas>>.

<sup>92</sup> Chinese companies account for 34% of worldwide applications for major patents related to 5G, but U.S. companies only take up 14%, see as AKITO TANAKA, ‘China in Pole Position for 5G Era with a Third of Key Patents’, *Nikkei Asian Review* (3 May 2019) <<https://asia.nikkei.com/Spotlight/5G-networks/China-in-pole-position-for-5G-era-with-a-third-of-key-patents>>.

<sup>93</sup>Dan Ciuriak, ‘The US-China Trade War: Technological Roots and WTO Responses’ (2019) *SSRN Electronic Journal*, 2

<sup>94</sup>Soo (n 91).

<sup>95</sup>Bryan Johnson, *The U.S.-Japan Semiconductor Agreement: Keeping Up the Managed Trade Agenda* (No 805, The Heritage Foundation), 2

<sup>96</sup>*Ibid.*, 12

<sup>97</sup> The measures taken by the U.S. were mainly including the Plaza Accord of 1985, the Structural Impediments Initiative of 1989 and the GATT Tokyo and Uruguay Rounds. See as Ciuriak (n 93).

<sup>98</sup>, ‘Winning the Race to 5G and the Next Era of Technology Innovation in the United States’ (hearing by U.S. Senate Committee on Commerce, Science, and Transportation, Washington .D.C., Feb 6, 2019).

<sup>99</sup>‘Remarks by President Trump on United States 5G Deployment’, *The White House* April 12, 2019 <<https://www.whitehouse.gov/briefings-statements/remarks-president-trump-united-states-5g-deployment/>>.

<sup>100</sup>Raj Bhala, ‘National Security and International Trade Law: What the GATT Says, and What the United States Does’ (1998) 19 *University of Pennsylvania Journal of International Economic Law* 263., 265

<sup>101</sup>Peter Lindsay, ‘The Ambiguity of GATT Article XXI: Subtle Success or Rampant Failure’ (2003) 52 *Duke Law Journal* 1277., 1277

<sup>102</sup>Michael J Hahn, ‘Vital Interests and the Law of GATT: An Analysis of GATT’s Security Exception’ (1991) 12 *Michigan Journal of International Law* 558., 558

<sup>103</sup>Rene E Browne, ‘Revisiting National Security in an Interdependent World: The GATT Article XXI Defense after Helms-Burton’ (1997) 86 *The*

mentioned above, which related to the U.S export control regulations has not sought to a solution by WTO dispute settlement mechanism, but it still worth checking whether the activities (i.e. the sanction to Huawei) by U.S has fit its WTO obligations. There is no doubt that the “export control” behavior is not in consistency with WTO obligations, unless there is a permitted exception<sup>104</sup>. Therefore, it will be necessary to check whether the U.S. behaviors could be covered by the exception provisions in WTO rules. Generally, apart from the “General Exceptions” in Article XX of GATT, Article XXI of GATT specially authorized WTO members a special exemption in their WTO obligations based on “essential security” reasons:

Nothing in this Agreement shall be construed (a) to require any contracting party to furnish any information the disclosure of which it considers contrary to its essential security interests; or (b) to prevent any contracting party from taking any action which it considers necessary for the protection of its essential security interests (i) relating to fissionable materials or the materials from which they are derived; (ii) relating to the traffic in arms, ammunition and implements of war and to such traffic in other goods and materials as is carried on directly or indirectly for the purpose of supplying a military establishment; (iii) taken in time of war or other emergency in international relations; or (c) to prevent any contracting party from taking any action in pursuance of its obligations under the United Nations Charter for the maintenance of international peace and security.<sup>105</sup>

It is noting that, the key concept in this article is “essential security interests”, which is a different expression with “national security”. However, it would not be ambiguous to understand the “essential security interests” has the same meaning with GATT members’ “national security”. So that these two expressions will be not specifically distinguished below.

---

*Georgetown Law Journal* 405., 417

<sup>104</sup> Such as GATT Article XIII has extended the principle of “Non-discriminatory Administration of Quantitative Restrictions” to export restrictions.

<sup>105</sup> *General Agreement on Tariffs and Trade* art XXI

## *B. How to understand GATT XXI*

### *I. A cautious attitude when drafting Article XXI*

From the opinion by the drafters of Article XXI of GATT, this provision was initialed to balance the increasing national security concerns by WTO member states and the need to promote an effective agreement.<sup>106</sup> For instance, one of the drafters commented that: “We cannot make it (*i.e.* the national security exception) 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.”<sup>107</sup> What’s more, it was further concerned that “there was a great danger of having too wide an exception and we could not put it into the Charter, ... that would permit anything under the sun.”<sup>108</sup> Indeed, this cautious attitude has also been mentioned by WTO officials in the *Decision concerning Article XXI of the General Agreement* in 1982. It has noted that the “resources to Article XXI could constitute, in certain circumstances, an element of disruption and uncertainty of international trade...” and recognized contracting parties “should take account into consideration the interest of third parties which may affected.”<sup>109</sup> Further, it particularly highlighted that the contracting parties “should be informed to the fullest extent possible of trade measures taken under Article XXI” and “all contracting parties affected by such action retain their full rights under the General Agreement.”<sup>110</sup> Therefore, researchers held that the “necessary consideration of Article XXI” should be restricted by other elements in the context, such as “fissionable materials” or “war and emergency in international relations”, in order to prevent the unlimited freedom usage of this provision to hinder international trade.<sup>111</sup>

---

<sup>106</sup>Markus A Reiterer, ‘Article XXI GATT - Does the National Security Exception Permit Anything under the Sun’ (1997) 2 *Austrian Review of International and European Law* 191., 198

<sup>107</sup>Daniel K Blewett, *Analytical Index - Guide to GATT Law and Practice* (GATT Secretariat, Legal Affairs Division, 6th ed, 1994)., 554

<sup>108</sup>*Ibid.*

<sup>109</sup>*Decision Concerning Article XXI of the General Agreement* (No L/5462, World Trade Organization, 2 December 1982).

<sup>110</sup>*Ibid.*

<sup>111</sup>Reiterer (n 106).

## 2. Limited interpretation of GATT Article XXI

Article XXI (a) applied all-embracing statement, that when contracting parties believed the disclosure of information has violated essential security.<sup>112</sup> Because there were none of pre-conditions for the implementation of this provision, so that it could be seen as a “self-judging” provision. However, as the reflection of the cautious attitude of drafters, there should be some restrictions to utilize this provision.<sup>113</sup> Specifically, as the absence of an objective standard in this provision, the contracting party will have broad discretion to determine what is its “essential security interests”. Accordingly, a narrower interpretation of article XXI (a) will meet the long-term stability requirements of GATT.<sup>114</sup> It also worth noting that the disclosure of information—the duty to inform belongs to auxiliary duties in GATT, which was connected to certain primary obligations<sup>115</sup>. So that the duty to inform in article XXI (a) and the discretion of self-judgement of contracting parties to determine the violation of essential security interests, should only apply to secondary duties.<sup>116</sup>

Compared with the absence of standard of article XXI (a), it seems that article XXI (b) has more detail and objective explanations in its three factual settings (fissionable materials; arms; war and emergency in international relations). Nevertheless, article XXI (b) of GATT was regarded as the most controversial provision in this exception.<sup>117</sup> Two reasons make this provision hard to implement. Firstly, one of the pre-conditions of article XXI (b) is “consider necessary”, which is not an objective fact but also a subjective self-judgement by contracting parties. But in the light of the three factual settings listed from (i) to (iii)<sup>118</sup>, this provision has actually limited the scope for contracting parties to escape

from their obligation and kept its legal binding.<sup>119</sup> The second ambiguity appears in the three factual settings themselves in article XXI (b). The words “fissionable materials” and “arms” are quite clear description of certain items that will cause questions about “national security”, but “war” and “emergency in international relations” are not such precise.<sup>120</sup> This paper will not discuss the concept of “war”, because even with different theoretical definitions, it would not make people confused to distinguish “war” with other international conflicts that exclude the military and armed conflict.

So that the problem is what is the “emergency in international relations”? It is clearly that “emergency” is not a common term in international law, so that this term should inherit certain meaning from “war” in the former of the provision<sup>121</sup>. However, there is still the possibility that the “emergency” might not necessarily constitute the use of force. As the whole provision of article XXI (b) is “self-judging”, so that this subjective element might lead to the contracting parties to decide what is “emergency”, even which was distinguished from the other factual settings under (i) to (iii).<sup>122</sup> A typical case is the Sweden ever used “essential security exception” to defend its import quota system on footwear, claimed that:

[The] decrease in domestic production has become a critical threat to the emergency planning of Sweden’s economic defense as an integral part of the country’s security policy... Such [domestic production] capacity is indispensable in order to secure the provision of essential products necessary to meet basic needs in case of war or other emergency in international relations.<sup>123</sup>

This case ended with Sweden withdrew its import quota on footwear after the widespread doubt about the legitimacy of Swedish measures and its justification for national security.<sup>124</sup> One of the most important reasons was, the footwear, or the

<sup>112</sup>Hahn (n 102). 582

<sup>113</sup>Ibid. 583

<sup>114</sup>Ibid.

<sup>115</sup>CONTRACTING PARTIES TO THE GATT, BASIC INSTRUMENTS AND SELECTED DOCUMENTS (Supplement No. 26, Geneva, 1979).

<sup>116</sup>Hahn (n 102). 584, see also Seyid Muhammad and Valiyaveettil Abdulazeez, *The Legal Framework of World Trade* (London: Stevens, 1958), 176

<sup>117</sup>Bhala (n 100). 267

<sup>118</sup>Briefly, article XXI (b) contains three standards: (i) “fissionable and related materials”, (ii) “arms items”, and (iii) “war and emergency in international relations”

<sup>119</sup>Hahn (n 102). 587

<sup>120</sup>Reiterer (n 106). 201

<sup>121</sup>GATT article XXI (b) (iii): “taken in time of war or other emergency in international relations”

<sup>122</sup>Hahn (n 102). 588

<sup>123</sup>Sweden - *Import Restrictions on Certain Footwear* (L/4250/Add.1, GATT, 15 March 1977), 1

<sup>124</sup>Spanogle John A. Jr, ‘Can Helms-Burton Be Challenged Under WTO?’ (1998) 27 *Stetson Law Review* 1313., 1331

military uniform could never be necessary “essential security interests” for a country and create “emergency in international relations”. In essence, the national security interests and commercial interests are intertwined and hard to be clearly divided.<sup>125</sup> If a contracting party intend to protect its economic interests and utilize “national security” as excuse, it will not be permitted. Therefore, researchers held that “emergency in international relations” should contain an armed conflict and this term should never be extendedly interpreted into non-military field.<sup>126</sup>

### *C. U.S. could not evade its WTO obligation according to GATT Article XXI*

Let us back to the U.S. ban on Huawei and its attitude on export control on high-technology products. As concluded above, apart from military issues, there are three actual standards for U.S. government to determine the threat to its national security: foreign government related transactions and entities related to critical infrastructure and strategic assets; communication sector-related transaction; and U.S. capacity in international technological leaderships. While the U.S. ban on Huawei has not been submitted to WTO panel to seek a solution, instead, seemed has been solved by negotiation between U.S and China,<sup>127</sup> it does not affect the judgment that the U.S. behavior has failed to meet its WTO obligations.

On the surface, when U.S. government decided to ban an entity in export control based on “national security” cause and which sanction was not persuasive in its national laws, such sanctions seemed to be explained by the “essential security exception” in GATT article XXI. Nevertheless, article XXI of GATT, as analyzed above, could only be interpreted and applied in limited scope, and which scope never cover protectionist measures.<sup>128</sup> In case of Huawei, BIS imposed severe sanction but did not provide enough evidence as case

of ZTE, to prove that Huawei has export sensitive products to embargoed countries, like Iran. Indeed, in author’s view, The US government is actually using “national security” as an excuse to crack down on other countries’ leading science and technology industries and maintain their own international leaderships, as the “Semiconductor War” with Japan in the 1980s, as the “5G Competition” with China now. In view of the tension between U.S and China and the unpredictable “trade war”, there is also a widely accepted suspicious that the ban on Huawei was a “weapon” for the U.S to put pressure on China.<sup>129</sup>

Obviously, such excuses of the U.S. export control in technologies cannot be persuasive and cannot trigger the application of GATT article XXI. As a special exception provision, the interpretation and application of article XXI are largely restricted, the extended interpretation are not permitted<sup>130</sup>. In case of Huawei, the possible provision that U.S. government could defend itself is article XXI (b).<sup>131</sup> Among them, (i) and (ii) is apparently irrelevant, that there is nothing in this case relate to fissionable materials and traffic in arms. In (iii), if the U.S. government could prove “war” or “emergency in international relations”, then it might be able evade its WTO obligations. However, even the “trade war” between U.S and China is fierce, every ordinary people with normal perception would never treat this situation as a “war” of armed conflict. Besides, a consensus is the “emergency in international relations” also need to be limited interpreted, that “armed conflict” and the resulting international tensions are necessary.<sup>132</sup> Thus, when U.S. government has failed to prove Huawei has directly violated its export control to export to embargoed countries, threatening its “national security”, but based on the aim of protecting its international leadership in technologies and

<sup>125</sup>Bhala (n 100)., 273

<sup>126</sup>Hahn (n 102). 588

<sup>127</sup> In G20 in Japan, Trump said that “US companies can sell their equipment to Huawei”, as long as the transactions won’t present a “great, national emergency problem”. However, in the light of Trump’s capricious style, things still need to be observed. See as Jackie Wattles, ‘Trump Reversed Course on Huawei. What Happens Now?’, *CNN Business* (30 June 2019) <<https://www.cnn.com/2019/06/29/business/huawei-trump-us-goods/index.html>>.

<sup>128</sup>Hahn (n 102). 582

<sup>129</sup> The treatment to Huawei has been a frequent topic of negotiation between U.S and China recently. See as Teddy Ng et al, ‘Chinese Team Arrives in US for Trade War Talks under Shadow of Latest Huawei Charges’, *South China Morning Post* (29 January 2019).

<sup>130</sup> This cautious attitude run through the drafters’ opinion and the interpretation of each subclause. See as Blewett (n 107). 554; see also Muhammad and Abdulazeez (n 116). 176; Hahn (n 102). 582-588

<sup>131</sup> Article XXI (a) could only refer to secondary obligations, and Huawei did nothing inappropriate in disclosure of information; article XXI (c) is about UN Charter and UN activities, which is irrelevant in this case.

<sup>132</sup>Hahn (n 102). 588

other political considerations to implement export control and sanction to Huawei. This protectionist measure violated U.S. WTO obligations of fair international trade and could not be exempted on the basis of Article XXI of the GATT.

## VII. CONCLUSION

The U.S. ban of Huawei has indicated that the U.S. export control on technologies is not transparent, and the standards of “national security” look like a “black box”. However, for a long time, “national security” in foreign investment regulations is a frequent topic to discuss, but seldom scholars have pay attention to the “national security” in export controls. Through the analysis of U.S. export control regulations on technologies itself and the “national security” in U.S. foreign investment laws, combined with cases, this paper raised three standards for BIS to determine the threats to “national security”: (1) foreign government related transactions and entities related to critical infrastructure and strategic assets; (2) communication sector-related transaction; and (3) U.S. capacity in international technological leaderships. Amongst the three reasons, (2) and (3) are closed connected. This paper also examined whether U.S. ban on Huawei and its attitude and measures in export control on technologies fit its WTO obligations, and concludes that the U.S. protectionist measures could not use GATT article XXI as an excuse to evade its WTO obligations. In other words, the U.S. violated its WTO obligations in Huawei case.

## BIBLIOGRAPHY

### Articles/Books/Reports/Documents

- [1]. Alavi, Hamed and Tatsiana KHAMichonak, ‘EU and US Export Control Regimes for Dual Use Goods: An Overview of Existing Frameworks’ (2017) 17 *Romanian Journal of European Affairs* 59
- [2]. Aoi, Tamotsu, *Historical Background of Export Control Development in Selected Countries and Regions* (Center for Information on Security Trade Controls)
- [3]. Bhala, Raj, ‘National Security and International Trade Law: What the GATT Says, and What the United States Does’ (1998) 19 *University of Pennsylvania Journal of International Economic Law* 263
- [4]. Blewett, Daniel K, *Analytical Index - Guide to GATT Law and Practice* (GATT Secretariat, Legal Affairs Division, 6th ed, 1994)
- [5]. Browne, Rene E, ‘Revisiting National Security in an Interdependent World: The GATT Article XXI Defense after Helms-Burton’ (1997) 86 *The Georgetown Law Journal* 405
- [6]. Casselman, Joshua W, ‘China’s Latest Threat to the United States: The Failed CNOOC-Unocal Merger and Its Implications for Exon-Florio and CFIU’ (2007) 17 *Indiana International & Comparative Law Review* 155
- [7]. Ciuriak, Dan, ‘The US-China Trade War: Technological Roots and WTO Responses’ [2019] *SSRN Electronic Journal*
- [8]. *CONTRACTING PARTIES TO THE GATT, BASIC INSTRUMENTS AND SELECTED DOCUMENTS* (No Supplement No. 26, GATT, 1979)
- [9]. D’Amato, C Richard, ‘National Security Dimensions of the Possible Acquisition of UNOCAL by CNOOC and the Role of CFIUS’ (at the U.S.-China Economic and Security Review Commission, 13 July 2015)
- [10]. *Decision Concerning Article XXI of the General Agreement* (No L/5462, World Trade Organization, 2 December 1982)
- [11]. DR, Fitzgerald, ‘Leaving the Back Door Open: How Export Control Reform’s Deregulation May Harm America’s Security’ (2014) 15 *North Carolina Journal of Law and Technology* 65
- [12]. F.Corr, Christopher F, ‘An Umbrella in a Hurricane: Cyber Technology and the December 2013 Amendment to the Wassenaar Arrangement’ (2015) 13 *Northwestern Journal of Technology and Intellectual Property* 153
- [13]. Feldman, Mark, ‘China’s Outbound Foreign Direct Investment: The US Experience’ (2017) 13 *International Journal of Public Policy* 304
- [14]. Fergusson, Ian F and Paul K Kerr, *The U.S. Export Control System and the President’s Reform Initiative* (No R41916, Congressional Research Service, 2014) 37
- [15]. ‘Guidance Concerning the National Security Review Conducted by the Committee on Foreign Investment in the United States’ (2008) 73 (No. 236) *Federal Register* 74567
- [16]. Hahn, Michael J, ‘Vital Interests and the Law of GATT: An Analysis of GATT’s Security Exception’ (1991) 12 *Michigan Journal of International Law* 558
- [17]. James, Mendenhall and Baker Stewart, ‘Economic Politics and National Security: A CFIUS Case Study’ in *American Society of International Law. Proceedings of the Annual Meeting*

- (Cambridge University Press, 2008)
- [18]. Jiang, Jingli and Gen Li, 'CFIUS: For National Security Investigation or for Political Scrutiny' (2013) 9 *Texas Journal of Oil, Gas, and Energy Law* 67
- [19]. John A. Jr, Spanogle, 'Can Helms-Burton Be Challenged Under WTO?' (1997) 27 *Stetson Law Review* 1313
- [20]. Johnson, Bryan, *The U.S.-Japan Semiconductor Agreement: Keeping Up the Managed Trade Agenda* (No.805, The Heritage Foundation, January 1991) <<https://www.heritage.org/asia/report/the-us-japan-semiconductor-agreement-keeping-the-managedtrade-agenda>>
- [21]. Liebler, Susan W and William H Lash III, 'Exon-Florio: Harbinger of Economic Nationalism' (1993) 16 *Cato Review of Business and Government*
- [22]. Lindsay, Peter, 'The Ambiguity of GATT Article XXI: Subtle Success or Rampant Failure' (2003) 52 *Duke Law Journal* 1277
- [23]. Meijer, Hugo, *Trading with the Enemy: The Making of US Export Control Policy toward the People's Republic of China* (Oxford University Press, 2016)
- [24]. Mostaghel, Deborah M, 'Dubai Ports World Under Exon-Florio: A Threat to National Security or a Tempest in a Seaport?' (2007) 70 *Albany Law Review* 583
- [25]. Muhammad, Seyid and Valiyaveetil Abdulazeez, *The Legal Framework of World Trade* (Stevens, 1958)
- [26]. Reiterer, Markus A, 'Article XXI GATT - Does the National Security Exception Permit Anything under the Sun' (1997) 2 *Austrian Review of International and European Law* 191
- [27]. Rogers, Mike, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE* (No 112th Congress, U.S. House of Representatives, 8 October 2012)
- [28]. Ros-Lehtinen, Ienan, 'An Imperfect Balance: ITAR Exemptions, National Security, and U.S. Competitiveness' (2013) 1(2) *National Security Law Journal* 43
- [29]. Seitzinger, Michael V, *Foreign Investment in the United States: Major Federal Statutory Restrictions* (No RL331003, Congressional Research Service, 2013) 18
- [30]. Seyoum, Belay, 'National Security Export Control Regimes: Determinants and Effects on International Business' (2017) 59(6) *Thunderbird International Business Review* 693
- [31]. SM, Dvorin, 'The Export Administration Act of 1979: An Examination of Foreign Availability of Controlled Goods and Technologies' (1980) *Northwestern Journal of International Law & Business* 179
- [32]. Sweden - Import Restrictions on Certain Footwear (No L/4250/Add.1, GATT, 15 March 1977)
- [33]. Tipler, Christopher M, 'Defining "National Security": Resolving Ambiguity in the CFIUS Regulations' (2014) 35 *University of Pennsylvania Journal of International Law* 62
- [34]. Vabulas, Felicity and Duncan Snidal, 'Organization without Delegation: Informal Intergovernmental Organizations (IIGOs) and the Spectrum of Intergovernmental Arrangements' (2013) 8(2) *The Review of International Organizations* 193
- [35]. Zive, Joshua C, 'Unreasonable Delays: CFIUS Reviews of Energy Transactions' (2013) 3 *Harvard Business Law Review* 169
- Web pages/News*
- [36]. D., Palmer, 'U.S. Lawmakers Cheer as China Steel Firm Backs out - Reuters', Reuters (19 August 2010) <<https://www.reuters.com/article/us-usa-china-trade/u-s-lawmaker-s-cheer-as-china-steel-firm-backs-out-idUSTRE67140C20100819>>
- [37]. Deng, Iris and Yingzhi Yang, 'US Ban on Huawei's 5G Technology Could Be a Blessing in Disguise for the Chinese Brand, Say PR Experts', South China Moring Post (25 February 2019) <<https://www.scmp.com/tech/big-tech/article/2187622/us-ban-huawei-5g-technology-could-be-blessing-disguise-chinese-brand>>
- [38]. Federal Communications Commission., 'Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs' (2 May 2018) <<https://www.federalregister.gov/documents/2018/05/02/2018-090/protecting-against-national-security-threats-to-the-communications-supply-chain-through-fcc-programs>>
- [39]. 'Federal Register: Addition of Entities to the Entity List' <<https://www.federalregister.gov/documents/2019/05/21/2019-10616/addition-of-entities-to-the-entity-list>>
- [40]. 'Federal Register: Additions to the Entity List' <<https://www.federalregister.gov/documents/2016/03/08/2016-05104/additions-to-the-entity-list>>
- [41]. 'Huawei Now World's Largest Telecom Equipment-Maker - Caixin Global' <<https://www.caixinglobal.com/2018-03-19/huawei-now-worlds-largest-telecom-equipment-maker-101223256.html>>

- [42]. 'In the Matter of: Zhongxing Telecommunications Equipment Corporation ZTE Plaza, Keji Road South Hi-Tech Industrial Park Nanshan District, Shenzhen China; ZTE Kangxun Telecommunications Ltd. 2/3 Floor, Suite A, Zte Communication Mansion Keji (S) Road Hi-New Shenzhen, 518057 China Respondent'; Order Activating Suspended Denial Order Relating to Zhongxing Telecommunications Equipment Corporation and ZteKangxun Telecommunications Ltd.', Federal Register (23 April 2018) <<https://www.federalregister.gov/documents/2018/04/23/2018-08354/in-the-matter-of-zhongxing-telecommunications-equipment-corporation-zte-plaza-keji-road-south>>
- [43]. Ng, Teddy et al, 'Chinese Team Arrives in US for Trade War Talks under Shadow of Latest Huawei Charges', South China Morning Post (29 January 2019)
- [44]. 'Remarks by President Trump on United States 5G Deployment', The White House <<https://www.whitehouse.gov/briefings-statements/remarks-president-trump-united-states-5g-deployment/>>
- [45]. Soo, Zen, 'How US Went from Telecoms Leader to 5G Also-Ran without Challenger to China's Huawei', South China Morning Post (2 April 2019) <<https://www.scmp.com/tech/enterprises/article/3004325/how-us-went-telecoms-leader-5g-also-ran-without-challenger-chinas>>
- [46]. TANAKA, AKITO, 'China in Pole Position for 5G Era with a Third of Key Patents', Nikkei Asian Review (3 May 2019) <<https://asia.nikkei.com/Spotlight/5G-networks/China-in-pole-position-for-5G-era-with-a-third-of-key-patents>>
- [47]. 'Temporary General License', Federal Register (24 March 2016) <<https://www.federalregister.gov/documents/2016/03/24/2016-06689/temporary-general-license>>
- [48]. Wattles, Jackie, 'Trump Reversed Course on Huawei. What Happens Now?', CNN Business (30 June 2019) <<https://www.cnn.com/2019/06/29/business/huawei-trump-us-goods/index.html>>
- [49]. Weisman, Steven R, 'Sale of 3Com to Huawei Is Derailed by U.S. Security Concerns', The New York Times (online at 21 February 2008) <<https://www.nytimes.com/2008/02/21/business/worldbusiness/21iht3com.1.10258216.html>>
- [50]. 'Winning the Race to 5G and the Next Era of Technology Innovation in the United States' (hearing by U.S. Senate Committee on Commerce, Science, and Transportation, Washington, D.C., Feb 6, 2019).
- [51]. <https://www.commerce.senate.gov/public/index.cfm/2019/2/winning-the-race-to-5g-and-the-next-era-of-technology-innovation-in-the-united-states>