ISSN: 2710-0170

The U.S. Trade Control Legal System and Chinese Enterprises' Responses

Yujun Cong

Beijing Normal University Law School, China

Abstract

Against the backdrop of warming China-U.S. relations, understanding the U.S. export control legal system remains crucial for China's legislation and enterprises engaged in cross-border trade. Complying with U.S. export administration regulations is the most basic bottom line for enterprises. This paper focuses on enterprises, taking the ZTE and Huawei cases as typical examples to explore the law enforcement strategies and judicial logic of the U.S. government. Concealment and deception are not the best strategies to respond to investigations. Enterprise executives should be cautious about traveling to sensitive regions and carrying documents, which can reduce the risk of sanctions against enterprises and their executives. Developing special compliance programs based on their own business characteristics has become an inevitable trend in enterprise management and a key to enhancing their competitiveness on the international stage.

Keywords

Victimization prevention; law enforcement strategies; judicial logic; corporate compliance.

1. Introduction

The ZTE and Huawei incidents, along with the Trump administration's launch of the "China Initiative," mark the full-scale start of the era of expanded law enforcement by the United States against Chinese enterprises. At that time, mainstream domestic media generally believed that the United States used the principle of "long-arm jurisdiction" to impose unwarranted sanctions on Chinese enterprises and individuals, which also became an academic consensus[1]. In the face of U.S. hegemony, Chinese enterprises have continuously improved their independent innovation capabilities, proving to the world with strength that Chinese enterprises can break through technological blockades and get rid of U.S. sanctions. Huawei Technologies Co., Ltd., once sanctioned by the United States, has regained unprecedented market popularity in the past year with its newly released digital devices and automobiles. However, the continuous occurrence of Chinese entrepreneurs being accused by the U.S. government constantly reminds us of the importance of responding to U.S. sanctions. As China-U.S. relations warm up, for Chinese enterprises (entrepreneurs), on the one hand, they need to be familiar with the U.S. legal tools in their fields; on the other hand, they should pay attention to the U.S. government's law enforcement strategies and judicial logic beyond legal texts, so as to enhance their ability to respond to U.S. investigations and reduce the risk of victimization.

2. Literature Review

Existing studies on U.S. import and export control sanctions against Chinese enterprises can be divided into the following categories:

The first category is the criticism of U.S. legal hegemony. Since the Trump administration, the United States has formulated a series of sci-tech competition strategies against China based on the dual logic of "weakening others" and "strengthening itself," aiming to block technology

ISSN: 2710-0170

exports to Chinese enterprises and crack down on advanced Chinese tech enterprises. This one-sided containment strategy has limitations and will eventually promote China's technological development[2]. Affected by political factors and foreign policies, "long-arm jurisdiction" has gradually expanded from interstate to extraterritorial, becoming a legal tool to infringe on the sovereignty of other countries[3]. Such "long-arm jurisdiction" often goes hand in hand with the extraterritorial application of U.S. domestic laws, causing irreparable losses to affected individuals and enterprises. Improving the extraterritorial application system of domestic laws is regarded as the key to breaking the deadlock[4]. These studies reveal the nature of the United States using its domestic legal system to restrict and suppress the development of other countries, and at the same time promote China to establish and improve the corresponding export control legal system. Providing relief measures for enterprises within the existing legal framework, both in the United States and domestically, helps Chinese enterprises carefully handle U.S.-related foreign trade business. However, in practice, the rights protection cycle for involved enterprises is long and costly, and legislative suggestions and reciprocal countermeasures are of limited help to individual enterprises.

The second category is the introduction and comparison of export control laws and regulations between China and the United States. The United States has many laws and regulations on export control. The U.S. Congress formulated and revised the *Export Administration Act* in 1949 and 1979 respectively. Based on this, the U.S. Department of Commerce formulated the *Export Administration Regulations* (hereinafter referred to as "EAR"). EAR regulates activities including exports, re-exports, and in-country transfers. Among them, re-exports include: the actual export of EAR-controlled items to another country/region after being exported outside the United States; the disclosure of EAR-controlled software or technology to entities in a third country/region abroad, i.e., "deemed re-export"; and the transfer of registration, control, or ownership of specific spacecraft by entities outside the United State. The U.S. export control laws and regulations form a strict network with EAR as the core, supplemented by the economic sanction system represented by the *International Emergency Economic Powers Act* (IEEPA) and other legal tools represented by the *Foreign Corrupt Practices Act* (FCPA). China adopted the *Export Control Law of the People's Republic of China* and the Ministry of Commerce issued the *Measures on the Unreliable Entity List* in 2020; in 2021, it adopted the *Anti-Foreign Sanctions Law of the People's Republic of China* and the *Measures for Blocking the Inappropriate Extraterritorial Application of Foreign Laws and Measures*[5] .The "Entity List" rule in EAR empowers the U.S. Department of Commerce, Department of Defense, Department of Energy, and Department of the Treasury to add entities, and substantially upgraded restrictions on Huawei around 2020. In response, China's *Measures on the Unreliable Entity List* have countermeasure and defensive functions[6]. These studies help us understand the legal tools of U.S. export control policies and compare and analyze China's countermeasures. However, these studies adopt a national perspective, and how to make China's export countermeasures effectively protect individual enterprises remains to be analyzed.

The third category is case studies on U.S. export control sanctions against Chinese enterprises. The U.S. export control policy against Huawei not only impacts Huawei but also has a reverse impact on its domestic market, thereby affecting the world economy[7]. Focusing on the ZTE case, some scholars have discussed ZTE's overall risk prevention in export control[8], analyzed the reasons for sanctions and enlightenment[9], and presented ZTE's export control compliance program[10]. These studies conduct case analyses from a legal perspective, which can enhance our understanding of U.S. extraterritorial criminal law enforcement and introduce an important part of U.S. judiciary—compliance—in specific cases. Although these literatures mention the basic facts of the Huawei and ZTE cases, due to the lack of systematic sorting of relevant U.S. law enforcement activities, it is difficult to provide more targeted solutions for different types of "going global" enterprises to prevent related law enforcement risks, and it is

ISSN: 2710-0170

also difficult to put forward countermeasures for the country regarding the overall compliance risk control of China's export-oriented enterprises.

3. Research Design and Case Presentation

3.1. Research Objects and Methods

To accurately reveal the legal tools, law enforcement strategies, and judicial logic of U.S. criminal sanctions against Chinese enterprises, it is necessary to transform the paper-based, static, and abstract legal provisions into dynamic, serialized real "legal events" involving interactions and games among prosecutors, defenders, judges, and other participants.

The United States has sanctioned hundreds of Chinese enterprises (entities) in terms of export control. There are 308 entities from mainland China alone in the Entity List managed by the U.S. Department of Commerce's Bureau of Industry and Security (BIS), involving aerospace, communications, semiconductors, cross-border logistics, and other fields[11]. Among the many involved enterprises, the ZTE and Huawei cases in the communications field are the most well-known to the public. Moreover, these two cases have abundant public information such as legal documents, media reports, academic research, and online blogs, which can be obtained through online investigations, allowing a clearer presentation of the full picture of the cases and excavation of detailed case details, thus forming a complete comparative study. Therefore, this study selects the two typical cases of ZTE and Huawei.

The main research method of this paper is to use legal documents and relevant information publicly released on U.S. government websites such as the official website of the U.S. Department of Justice (www.justice.gov), the official website of the U.S. Department of Commerce (www.commerce.gov), and the official website of the Federal Register (www.federalregister.gov) to completely restore the relevant background, case facts, law enforcement, and judicial processes, and summarize the legal tools, law enforcement strategies, and judicial logic used by the U.S. side in export control cases.

It should be noted that unless otherwise specified, the case facts in this paper are all cited from public information on U.S. government websites.

3.2. ZTE Case

ZTE (full name: ZTE Corporation) is headquartered in Shenzhen. During the incident, it operated a subsidiary in the United States (ZTE USA) and a subsidiary in Tehran, Iran (hereinafter referred to as "Parsian"). Other involved enterprises include Beijing Baxing (hereinafter referred to as "8s"), Chinese Company A (hereinafter referred to as "CCA"), Iranian Company A (hereinafter referred to as "ICA"), and Iranian Company B (hereinafter referred to as "ICB").

3.2.1. Illegal Export

From approximately January 2010 to March 2016, ZTE shipped components purchased in the United States, which required a license from the U.S. Department of the Treasury's Office of Foreign Assets Control (hereinafter referred to as "OFAC"), from China to Iran. In early 2010, ZTE began bidding for two different Iranian projects: one with Iranian Company A and the other with Iranian Company B. Both project contracts were worth hundreds of millions of dollars and required the use of controlled U.S.-origin components.

On February 23, 2010, ICA and ZTE reached an initial agreement, under which ZTE would provide equipment to ICA to expand its existing telecommunications network in Iran within three years. On December 28, 2010, the two parties completed and signed the final supply contract. The contract was signed by four parties: ICA (signed by the vice president and general manager), ZTE (signed by the commercial manager), 8s (signed by the manager), and ZTE Parsian (signed by the general manager). According to the contract, 8s was to provide U.S.-

ISSN: 2710-0170

origin components to ICA, purchasing and transporting the original components from suppliers. 8s was supposed to enter into a procurement contract with ZTE Kangxun, ZTE's international procurement branch. ZTE Kangxun would act as 8s's procurement agent, purchase the prohibited items from the United States and resell them to 8s. Then 8s would be responsible for exporting these prohibited items from China to Iran. However, 8s had no history of procurement or transportation business and thus no real business reputation. In the end, although 8s was a party to the ICA contract, ZTE believed it had a certain market reputation and was less likely to be intercepted and searched, so it actually purchased and transported the prohibited items itself. In the shipping containers, ZTE concealed U.S.-origin components by packing them together with its own products. ZTE marked the U.S.-origin components on the packing list attached to the shipment but did not specifically indicate them on the customs declaration form. From January 2010 to December 2012, ZTE sent nearly 131 shipments to ICA, containing a large number of products listed on the Commerce Control List (CCL), and received a total of $68,155,078 from ICA during this period.

On November 22, 2010, ZTE signed a contract with Iranian Company B, which was signed by the CEO of ICB, ZTE's commercial manager, 8s's manager, and the general manager of ZTE Parsian. Similar to the ICA contract, 8s was responsible for supplying U.S.-origin components, but ZTE ultimately fulfilled 8s's contractual obligations. From January 2010 to December 2012, ZTE sent nearly 20 shipments to ICB. The expenses incurred by ZTE for transporting products to ICB were approximately $25.4 million, of which the cost of U.S.-origin components was approximately $11.8 million. The U.S.-origin components shipped by ZTE to Iran were obtained from its suppliers in bulk orders, and ZTE's orders were reflected in the suppliers' monthly supplies. Its monthly procurement volume reflected the global demand that the company had to meet, including its Iranian customers.

3.2.2. Evasion of Supervision

In the course of cooperating with Iranian enterprises, ZTE believed that 8s was insufficient to isolate ZTE's risks. Senior managers of ZTE ordered a company-level export control team to study, handle, and respond to the company's export control risks. On September 2, 2011, four senior managers jointly proposed to solve these problems. In the *Report on Comprehensively Rectifying and Standardizing the Company's Export Control-Related Business*, it was mentioned that the primary goal was to identify and establish new isolated companies to provide necessary U.S. components for projects in embargoed countries. This document was signed by ZTE's general counsel, executive vice president of sales, executive vice president of logistics, and CEO of ZTE. This reflects that ZTE sent U.S.-origin components to many sanctioned countries, such as Iran, Sudan, North Korea, Syria, and Cuba, without obtaining permits.

Around March 2012, Reuters published an article describing details of ZTE's sales of equipment to ICA, with the ZXMT system containing U.S.-origin components. The U.S. Department of Commerce's BIS requested ZTE USA to provide the ICA contract and packing list mentioned in the article in the form of an administrative subpoena. The U.S. Attorney's Office for the Northern District of Texas then initiated a grand jury investigation, and the FBI also issued a criminal subpoena to ZTE USA. In response to the article and the investigation, ZTE shipped some of the U.S.-origin components that had been transported to ICA back to China from Iran. In the summer of 2012, ZTE decided to temporarily stop sending U.S. equipment to Iran.

In 2013, ZTE Parsian began urging ZTE to continue business with its Iranian customers. The sales team of ZTE Parsian invited a group of ZTE executives to Tehran to help ZTE better understand the pressure exerted by its Iranian customers on the Iranian office. After the visit, senior managers of ZTE, including the CEO and vice president, decided to continue business with Iranian customers. ZTE was worried about breaching contracts with Iranian customers and also considered retaining its bank guarantees. In the same year, ZTE identified CCA as the

ISSN: 2710-0170

new transportation company based on factors such as the cooperative company's sales volume, willingness to cooperate, scale, and costs. In November 2013, ZTE continued to fulfill the contract with Iran, and in early July 2014, ZTE once again began shipping U.S.-origin components to Iran without the necessary permits.

On November 2, 2013, ZTE authorized the commercial manager of Parsian and the president of CCA to sign a contract. According to the contract terms, CCA was required to comply with all export laws, including those of the United States. On the other hand, CCA signed contracts with ICA and ICB. CCA purchased all components ordered by ICA from ZTE (including U.S.-origin components and ZTE's own components). Then ZTE purchased or produced the necessary components selected by CCA from ZTE's warehouse, and CCA shipped all products to ICA. ZTE erased its own trademarks on the products shipped to ICA. Between January 2010 and January 2016, ZTE, directly or indirectly through 8s and CCA, shipped nearly $32.2 million worth of U.S.-origin components to Iran without obtaining export licenses from the U.S. government.

3.2.3. Obstruction of Investigation

In 2012, ZTE required each employee involved in sales to Iran to sign a confidentiality contract, under which employees were required to keep confidential all information related to the company's exports to Iran. In meetings on August 26, 2014; December 2, 2014; November 20, 2015; November 21, 2015; January 8, 2016; and March 18, 2016, ZTE's defense lawyers, unaware that the statement documents provided by ZTE to consultants for communication with the government were false, reported to the Department of Justice and federal law enforcement agencies that the company had stopped business with Iran and thus no longer violated U.S. export control and sanction laws. In further meetings between defense consultants and the U.S. government, senior managers of ZTE reviewed and approved the defense consultants' statements, knowing at the time that the statements were false. To avoid detection of its resumed sales to Iran from 2013 to 2016, ZTE took measures to conceal data about those transfers in the computer system from accounting firms. ZTE's then CEO proposed to three senior managers of the IT department that all data related to Iranian business since March 2012 should be hidden from accounting firms. So they start CDIT team. The team had nearly 13 people, whose job was to remove all data related to Iranian business from 2013 to 2016. ZTE implemented an automatic deletion function for the personal email accounts of the 13 members of the CDIT team, so their emails were deleted every night to ensure no communication about hidden data existed. Members of the CDIT team also signed confidentiality contracts, agreeing not to share information related to CDIT, otherwise they would be fined 1 million RMB.

As a result, around January 8, 2016, and March 18, 2016, when defense lawyers presented the final information about ZTE's sales to Iran to the U.S. government, the information was false.

3.3. Huawei Case

Huawei Technologies Co., Ltd. (hereinafter referred to as "Huawei") is headquartered in Shenzhen, and its U.S. subsidiary in Texas is Huawei Devices USA Inc. (hereinafter referred to as "Huawei USA"). SKYCOM Tech Co., Ltd. (Hong Kong Skycom Tech Co., Ltd., hereinafter referred to as "Skycom") is a company registered in Hong Kong, with its main business in Iran. The U.S. grand jury believes that Skycom is Huawei's subsidiary in Iran. As of 2007, Huawei's parent company owned Skycom through a subsidiary ("Huawei Subsidiary 1"). Around November 2007, Huawei Subsidiary 1 transferred its shares in Skycom to another entity ("Huawei Subsidiary 2"). Meng Wanzhou, Huawei's CFO, served on Skycom's board of directors from February 2008 to April 2009. In addition, the case involves four financial institutions, referred to as Financial Institution 1, Financial Institution 2, Financial Institution 3, and Financial Institution 4.

ISSN: 2710-0170

3.3.1. Fraud

Since around July 2007, Huawei has repeatedly claimed to the U.S. government and various victimized financial institutions, including Financial Institutions 1, 2, 3, and 4, as well as their subsidiaries and branches in the United States and the eurozone (collectively referred to as "victimized institutions"), that although Huawei conducts business in Iran, its actions do not violate applicable U.S. laws, including ITSR. In fact, the way Huawei conducts business in Iran violates applicable U.S. laws, including ITSR.

Around July 2007, agents of the U.S. Federal Bureau of Investigation ("FBI") interviewed the founder of Huawei ("Individual 1") in New York, who claimed that Huawei had no direct dealings with any Iranian company. Individual 1 further stated that he believed Huawei sold equipment to third parties, possibly in Egypt, and Egypt sold the equipment to Iran.

In late 2012 and early 2013, several news agencies, including Reuters, reported that Skycom violated U.S. laws by selling and attempting to sell embargoed U.S.-origin goods to Iran, and that Huawei actually owned and operated Skycom. In December 2012, Reuters published an article claiming to include an official statement from Huawei in response to and denial of these allegations. In January 2013, Reuters published a second article, also claiming to include an official statement from Huawei, once again responding to and denying the allegations. Based on Huawei's claims in these statements, the victimized institutions decided to continue their banking relationships with Huawei and its subsidiaries and affiliates.

In addition, Huawei repeatedly told Financial Institution 1 that it would not use Financial Institution 1 and its subsidiaries to handle transactions related to Huawei's Iranian business. In fact, Huawei used U.S. Subsidiary 1 and other financial institutions operating in the United States to handle U.S. dollar clearing transactions involving millions of dollars to advance its business in Iran. On August 22, 2013, Meng Wanzhou met with executives of Financial Institution 1, speaking in Chinese and relying in part on a Chinese-written presentation. At the request of executives of Financial Institution 1, Meng Wanzhou submitted an English version of the presentation around September 3, 2013, which included: first, Huawei's "operations in Iran strictly comply with applicable laws, regulations, and sanctions of the United Nations, the United States, and the European Union"; second, "Huawei's cooperation with SKYCOM is a normal business cooperation"; third, Meng Wanzhou's participation in Skycom's board of directors was to "help Huawei better understand Skycom's financial and operational performance, and strengthen and supervise Skycom's compliance"; fourth, "Huawei's subsidiaries in sensitive countries will not open accounts with Financial Institution 1 nor conduct business transactions with Financial Institution 1." Of course, the U.S. government believes these statements are false. In early 2014, Meng Wanzhou traveled to the United States and stopped at John F. Kennedy International Airport in the Eastern District of New York. When she entered the United States, the electronic device she carried contained a file in unallocated space, indicating that the file might have been deleted, which contained key points of her conversation with executives of Financial Institution 1.

Around 2017, due to concerns about the risks of Huawei's business practices, Financial Institution 1 decided to terminate its global relationship with Huawei. After learning of Financial Institution 1's decision, Huawei took measures to ensure and expand banking relationships with other financial institutions, including a subsidiary of Financial Institution 4. A Huawei employee, in meetings and communications with representatives of U.S. Subsidiary 4, falsely stated that Huawei was considering terminating its relationship with Financial Institution 1 because it was dissatisfied with the service level provided by Financial Institution 1. Based in part on these false statements and omissions by Huawei and other Huawei employees, the subsidiary of Financial Institution 4 agreed to expand its banking relationships

ISSN: 2710-0170

with Huawei and its subsidiaries and affiliates, and continue to maintain its existing global (including U.S.) banking relationships with Huawei.

3.3.2. Obstruction of Justice

Around 2017, in view of the U.S. government's criminal investigation into Huawei and its affiliates, Huawei and Huawei USA transferred witnesses with knowledge of Huawei's Iranian business to China and destroyed and concealed evidence of Huawei's business in Iran in the United States.

4. Analysis

4.1. The Existing U.S. Legal Framework Easily Entangles Enterprises in Criminal Troubles

U.S. legal tools have very detailed provisions on import and export control. Special chapters are set in the *United States Code*, and government departments will revise and add relevant regulations according to needs when handling specific cases, so its completeness is self-evident. In the cases discussed in this paper, the U.S. government accused ZTE of three charges: conspiracy to illegally export, obstruction of justice, and making false statements to federal investigators. Huawei (including Meng Wanzhou) was mainly accused of (conspiracy to commit) fraud, (conspiracy to violate) the *International Emergency Economic Powers Act* (Title 31, Code of Federal Regulations, Sections 560.203, 560.204 and 560.206.), and obstruction of justice. Referring to U.S. accusations against other enterprises, conspiracy is the most frequent charge. Conspiracy generally refers to an agreement between two or more people to commit an unlawful act, or to achieve a lawful purpose by unlawful means[12]. In China, conspiracy does not constitute an independent crime, but U.S. criminal law holds that conspiracy itself is punishable and constitutes an independent crime. The establishment of conspiracy not only reflects the pre-emption of legal interest protection but also plays a role in the litigation process. Criminal offenses by multinational enterprises are often difficult to investigate, with difficulties in evidence collection, and prosecuting a substantive crime will face objective obstacles. It is obviously more difficult to prove that an enterprise has met the conditions for the completion of a crime than to prove the existence of an agreement. In order to make full use of the advantageous procedural rules related to conspiracy, save judicial efficiency, prosecutors are likely to abandon the prosecution of substantive crimes and instead prosecute conspiracy[13]. As long as enterprises can be brought into U.S. judicial procedures, judicial organs will have the opportunity to carry out further criminal investigations, investigate more criminal facts, and increase the judicial burden on involved enterprises.

Conspiracy to illegally export requires that the actor knowingly and intentionally conspires and agrees with others to export, re-export, and transfer, and causes U.S. goods, especially servers, switches, routers, and other components of cellular network infrastructure, to be exported, re-exported, or transferred without first obtaining the required export license from the U.S. Department of the Treasury's Office of Foreign Assets Control (See 50 USC §1705； 31 CFR part 560； 15 CFR §764.2(a)-(e)). Conspiracy to commit bank fraud requires that the actor, together with others, intentionally conspires to defraud financial institutions through one or more material false statements and promises, and obtain money, funds, credit, and other property owned, held, and controlled by financial institutions (See Title 18, United States Code, Sections- 1349 and 3551 et seq.). The charge of conspiracy does not require the actor to complete the offense, i.e., successfully export contraband to another country or successfully defraud funds from financial institutions. If the offense is completed, an additional charge corresponding to the act will be added on the basis of conspiracy, that is, at least two charges: conspiracy and the substantive act. In the Huawei case, prosecutors charged conspiracy to

ISSN: 2710-0170

commit bank fraud and bank fraud, while in the ZTE case, prosecutors only charged conspiracy to illegally export. This should be due to the difficulty of proof. The financial institutions cooperating with Huawei have subsidiaries in the United States, and the U.S. government has obtained the business records between them, so the fact that Huawei has obtained funds from financial institutions can be proved. Although the U.S. government has obtained the shipping documents for ZTE's exported products to Iran, physical evidence is difficult to fix, so it chose to charge ZTE with conspiracy. However, as long as criminal proceedings are initiated against an enterprise, the non-criminal sanctions it suffers are unbearable.

4.2. The Selection of Prosecution Objects Is Targeted

The legal documents of the ZTE and Huawei cases all mention that the parent companies of ZTE and Huawei have established subsidiaries in the United States, but their subsidiaries did not directly engage in criminal activities and were not listed as defendants. The U.S. government directly listed the parent companies as defendants. Is this personal jurisdiction or protective jurisdiction? The U.S. "Long-Arm Statute" has expanded personal jurisdiction. As long as a non-resident defendant has minimum contacts with the forum, U.S. courts can exercise personal jurisdiction over them[14]. As long as a defendant enterprise establishes a company in the United States, it has established contact with the United States; even more, as long as there is email communication with the United States, it constitutes contact and can apply personal jurisdiction. According to the content of U.S. export control laws, violations of export control are regarded as threats to U.S. national security, so the U.S. government also has jurisdiction based on the principle of protective jurisdiction.

Regardless of the type of jurisdiction, criminal charges against enterprises have become a fact, but not all actors who meet the prosecution conditions have been prosecuted. In the ZTE case, ZTE, together with Chinese enterprises 8s and CCA, and Iranian enterprises ICA and ICB, illegally exported goods. According to U.S. criminal law, the four parties jointly constituted a crime, but the DOJ did not prosecute 8s and CCA, let alone the two Iranian enterprises, nor did it prosecute any individuals. In the Huawei case, the DOJ prosecuted not only the enterprise but also Meng Wanzhou. Obviously, apart from political reasons, from the perspective of convenience, the reason for prosecuting Meng Wanzhou is that she was actually under U.S. control. The executives who approved ZTE's Report on Comprehensively Rectifying and Standardizing the Company's Export Control-Related Business had already constituted obstruction of justice, but the DOJ did not prosecute any ZTE executives, only requiring in the plea agreement that within six months after signing, ZTE would dismiss the four employees who proposed to find an isolated company (CCA) and settle all payment obligations to them（See Plea Agreement USA v. ZTE Corporation, No 3-17CR-0120K.）.

4.3. Parallel Law Enforcement by the U.S. Government Deals a Double Blow to Involved Enterprises

According to the plea agreement with the DOJ, ZTE agreed to pay a maximum fine of approximately $1.19 billion (including a fine of $892,360,064 and liquidated damages of $300,000,000). The DOJ set a three-year probation period until March 22, 2020 (the U.S. Federal Court decided in October 2018 to extend the probation period to March 22, 2022). During the probation period, ZTE must accept supervision by an independent compliance monitor team appointed by the U.S. government, comply with U.S. export control laws and fulfill the obligations of the settlement agreement, and issue an annual report to synchronize its compliance status. At the same time, the U.S. Department of Commerce's BIS reached a settlement agreement with ZTE, requiring it to pay a civil penalty of $361 million. During the probation period, ZTE did not fully fulfill the plea agreement and the settlement agreement. On April 16, 2018, the U.S. government determined that ZTE had violated the March 2017 agreement and imposed an export ban on ZTE, forcing ZTE to sign a superseding settlement

ISSN: 2710-0170

agreement, which required an additional fine of $1.4 billion (including $1 billion in fines and $400 million in an escrow account) and imposed a 10-year period of supervision on ZTE. It can be seen that in addition to accepting compliance supervision, ZTE also paid criminal fines and civil fines to the DOJ and BIS respectively. The subsequent superseding settlement agreement added at least $1 billion, exceeding the criminal fine. The BIS settlement agreement stipulates that ZTE must comply not only with the agreement with BIS but also with a series of documents signed with the DOJ and OFAC. Violations of documents from other agencies are also regarded as violations of this settlement agreement, which will also lead to further penalties.

Similarly, the U.S. Department of Commerce has imposed administrative sanctions on Huawei. The U.S. Department of Commerce's BIS announced specific measures to implement the presidential order, adding Huawei to the "Entity List." On August 19, 2020, the U.S. Department of Commerce revised the Entity List, adding another 46 Huawei affiliates to the Entity List. On May 15, 2020, the Bureau of Industry and Security (BIS) of the U.S. Department of Commerce revised the Foreign-Produced Direct Product Rule (FDP), bringing semiconductor designs based on U.S. software and technology, and chips manufactured using semiconductor production equipment listed on the U.S. Department of Commerce's Control List (CCL) under export control. In fact, this extends jurisdiction to enterprises not registered in the United States, such as TSMC and Samsung, prohibiting them from selling goods to Huawei. In August of the same year, 38 new Huawei affiliates were added to the Entity List, and the Foreign-Produced Direct Product Rule (FDP) was revised to expand the product scope to any product (the May 2020 ban only involved semiconductors and integrated circuits), and clarified that Huawei and its affiliates on the Entity List are subject to export control as purchasers, intermediate consignees, ultimate consignees, and end-users. After being sanctioned by the United States, Huawei did not reach an agreement with the United States like ZTE, which resulted in Huawei not being removed from the list for a long time, affecting its main business.

For enterprises, although U.S. penalties (mainly fines) are severe, the "double-pronged" law enforcement strategy combining parallel law enforcement by other government departments and corresponding administrative sanctions requires special attention. Focusing only on criminal risk prevention may make it difficult to gain a foothold in U.S.-related business. As the content of export control compliance involves not only the part that constitutes a crime but also the prevention of export control violations.

5. Discussion

5.1. Enterprises and Their Executives Should Act Prudentl to Improve the Ability to Prevent Victimization

The FBI's criminal investigation into ZTE was triggered by a Reuters report, and the key evidence confirming the criminal facts were two internal ZTE documents: *Report on Comprehensively Rectifying and Standardizing the Company's Export Control-Related Business* and Export *Control Risk Evasion Plan*. These "confidential" documents were made public on U.S. government websites. In 2014, a senior manager of ZTE was detained for inspection at the airport when going to the United States. The U.S. side found two documents related to the "evasion plan" in the computer of the secretary accompanying the executive[15]. The documents, written by the legal department, detailed the export control risks faced by Iranian business, but this warning failed to stop ZTE's illegal activities, and the signatures of several executives also appeared on the documents. Another evasion plan clearly mentioned finding an isolated company to block ZTE's risks, which became ironclad evidence of illegal export and obstruction of justice.

In 2013, French Alstom executive Frédéric Pierucci was detained by the U.S. government at New York's Kennedy Airport, and all his accompanying materials were seized[16]. This

ISSN: 2710-0170

sensational news must have been known to executives of well-known enterprises. In this context, foreign executives should carefully consider traveling to the United States or at least avoid carrying electronic storage devices to avoid giving the U.S. government the opportunity to search. It should be noted that this is not "victim blaming" but a suggestion to reduce the risk of victimization from the perspective of victim prevention, which belongs to the category of crime prevention. Countries that have frequent judicial cooperation with the United States should also be paid attention to. According to the U.S. government, Meng Wanzhou visited the United States in early 2014 and stayed at John F. Kennedy International Airport in the Eastern District of New York. At that time, the U.S. government may have inspected Meng Wanzhou's electronic devices and found deleted key points of the conversation with financial institution executives. In view of this, as Huawei's CFO, Meng Wanzhou should have been more capable of dealing with U.S. government investigations than others, but unfortunately, she was detained by Canadian police and forced to sign a plea agreement with the United States.

5.2. Enterprises' Concepts and Decisions in Responding to Government Investigations Urgently Need to Be Updated

Both ZTE and Huawei started as small local companies. After China's accession to the WTO, the domestic market economy developed rapidly, and the two enterprises gradually grew stronger and began to enter the overseas market. Integrating into the world market means more opportunities on the one hand and requires enterprises to abide by corresponding rules on the other hand. Zhao Xianming, Chairman and CEO of ZTE, said, "ZTE acknowledges that it has violated U.S. export control-related laws and regulations and is willing to bear corresponding responsibilities. The company will continue to actively promote reforms, has formulated new compliance processes, and carried out major personnel adjustments. We have learned many lessons from this experience and will strive to become a model of export control compliance governance, committed to building a compliant, healthy, and trustworthy new ZTE" [17]. ZTE knew all along that transactions with Iran violated U.S. law, and still decided to continue the illegal activities after the legal department issued risk warnings. More severe penalties could have been avoided, and this is not a hindsight perspective. Because during the investigation, defense lawyers and law firms repeatedly told the DOJ that ZTE had stopped transactions with Iran (though misled by ZTE), otherwise, the charge of making false statements would not have been added.

In contrast, Huawei has portrayed itself as a victim in the media, and its official has not admitted to violating U.S. export control laws. Even if Meng Wanzhou signed a deferred prosecution agreement and admitted to the illegal acts in the agreement, if she fulfills the obligations stipulated in the deferred prosecution agreement during the deferred prosecution period, the prosecutor will drop the charges after the probation period, and the act committed by the suspect should be regarded as innocent in law[18]. Therefore, it is reasonable for Meng Wanzhou's lawyer to claim that Meng is innocent after she signed the DPA. Due to the only description of the criminal facts from the U.S. side, it is difficult to evaluate Huawei's and Meng Wanzhou's fraudulent acts. However, combining the two cases, it can be seen that the business cooperation strategy and response strategy to U.S. law enforcement centered on deception are no longer suitable for the current market environment. Under the premise of a reasonable legal system, only integrity-based operation can enable enterprises to operate continuously and steadily.

5.3. Enterprises Should Grasp the Key Links in Building a Compliance Management System

The ZTE incident indeed exposed major problems in ZTE's compliance management. From the perspective of compliance elements, the top-level tone was completely absent. Many executives were planning how to isolate risks rather than stop illegal activities. Although the legal

ISSN: 2710-0170

department in the organizational system issued risk warnings, it did not further perform compliance duties, and all suggestions were about evasion. Compliance training was a mere formality and could not prevent illegal acts. When the DOJ and lawyers entered for investigation, they failed to prompt relevant personnel to actively cooperate and make correct statements. It can be said that ZTE's compliance management system was almost paralyzed at that time. After being involved in the case, ZTE carried out large-scale reforms in organizational settings, established a compliance department, and formulated special compliance programs for anti-bribery, export control, and data protection. It can be seen that the soul of corporate compliance is not a comprehensive compliance management system, but the establishment of special compliance programs targeting the enterprise's "compliance risk points" [19]. But as mentioned earlier, compliance is not all of the ZTE case; it is only an obligation in the agreement, which can be said to be a clause set by the U.S. government to prevent enterprises from committing similar illegal acts again.

6. Conclusion and Prospect

A in-depth analysis of the ZTE and Huawei cases from the perspective of criminal integration is not only valuable for restoring the context of the cases themselves but also opens a window for us to observe the practice of U.S. trade control laws. In these two typical cases, substantive laws such as U.S. criminal law and federal regulations are not isolated provisions but are closely intertwined with the dynamic law enforcement processes of administrative departments such as the Department of Justice and the Department of Commerce, as well as the trial logic of judicial organs, jointly forming a complete and highly enforceable legal operation system. The game between prosecutors and defenders in the cases is not only a dispute over the application of legal provisions but also a repeated contest over practical details such as law enforcement standards, evidence rules, and compliance requirements. This vivid case presentation provides Chinese enterprises with intuitive materials far beyond theoretical interpretations to understand the U.S. judicial system. Compared with existing studies, this dynamic analysis based on individual cases can effectively make up for the limitations of macro legal framework studies—it shows us that U.S. trade control is not a rigid set of rules but continuously extends its jurisdiction and strengthens its control through the adjustment of law enforcement strategies and the application of judicial logic. For example, the frequent application of conspiracy in cases shows how U.S. judicial organs expand the scope of accountability by lowering the burden of proof; the parallel law enforcement mechanism reflects the synergistic effect of administrative sanctions and criminal penalties, forming multiple pressures on enterprises. The revelation of these details can help Chinese enterprises more accurately grasp the practical logic of U.S. trade control, rather than merely staying at the literal understanding of legal provisions.

Of course, due to the limitations of research scope and information availability, there are still many issues worthy of in-depth discussion in this paper. For example, the question of whether the U.S. lawyer who "betrayed" ZTE violated the attorney-client privilege not only involves the specific application of U.S. lawyer ethics but also relates to enterprises' understanding of lawyers' roles and risk prevention in cross-border legal matters—where is the boundary of lawyers' confidentiality obligations? Under what circumstances does the so-called "whistleblower system" in the United States take precedence over confidentiality obligations? The answers to these questions directly affect Chinese enterprises' selection and use of legal services in U.S.-related legal disputes.

Another issue worthy of attention is the difference between the "Special Compliance Coordinator (SCC)" in the settlement agreement signed by ZTE and BIS and the compliance monitor in the plea agreement. Behind this difference lies the division of responsibilities,

ISSN: 2710-0170

regulatory priorities, and operational models between U.S. administrative and judicial organs in corporate compliance supervision: does the SCC focus more on the implementation of administrative compliance requirements or also take into account judicial behavior correction? What are the differences in their supervision periods, authority scopes, and reporting paths? Clarifying these issues can provide Chinese enterprises with a more detailed reference for understanding the U.S. government's compliance supervision system, helping enterprises formulate more targeted response strategies in similar situations.

In addition, due to the fact that some case materials involve judicial confidentiality clauses and objective obstacles such as network restrictions in cross-border information acquisition, issues such as the specific identification standards of "long-arm jurisdiction" in U.S. trade control law enforcement, the cooperation mechanism between different departments in case investigations, and the effectiveness evaluation indicators of enterprise compliance programs remain to be further explored in future studies. However, the ZTE and Huawei cases have clearly shown that in the context of globalization, Chinese enterprises are facing an increasingly complex international legal environment. In particular, the law enforcement efforts and judicial logic of the U.S. trade control system pose continuous challenges to enterprises' cross-border operations. In-depth research on these cases and the legal operation rules behind them is not only a need for academic research but also a practical requirement for Chinese enterprises to improve risk prevention capabilities, build compliance management systems, and enhance international competitiveness. In the future, as China-U.S. economic and trade relations evolve dynamically and the international legal environment continues to adjust, relevant research needs to be continuously updated to provide more comprehensive and operable theoretical support and practical guidance for Chinese enterprises to "go global."

References

[1]Zhang Lei, Chen Nan: "U.S. 'Long-Arm Sanctions' and China's Responses", Journal of Guizhou Provincial Party School, No. 6, 2020.

[2]Huang Zhaolong, Han Zhaoying: "An Analysis of U.S. Sci-Tech Competition Strategy Against China in the Context of Sino-U.S. Strategic Game", Qiushi Journal, No. 2, 2022.

[3]Xiao Yongping: "A Jurisprudential Analysis and Countermeasure Study on 'Long-Arm Jurisdiction'", China Legal Science, No. 6, 2019.

[4]Liao Shiping: "The Extraterritorial Application of Domestic Laws and Its Responses—Taking U.S. Extraterritorial Application Measures as an Example", Chinese Review of International Law, No. 3, 2019.

[5]Cai Kaiming: "U.S. Legal Policy Tools Against China and China's Countermeasures", Administrative Reform, No. 4, 2022.

[6]Liao Fan: "The Unreliable Entity List System from a Comparative Perspective", Journal of Comparative Law, No. 1, 2021, p. 169.

[7]Chen Sichong, Wang Ziyu, Liang Yitian: "The Reverse Market Impact of U.S. Tech Sanctions Against China—A Case Study of Huawei", International Economic Review, No. 2, 2022.

[8] Liu Junxia: "U.S. Trade Export Control and Risk Prevention from the Perspective of 'ZTE Incident'", Practice in Foreign Economic Relations and Trade, No. 11, 2018.

[9]Zhang Yajun: "Reasons for ZTE's Two U.S. Trade Sanctions and Important Enlightenments", Practice in Foreign Economic Relations and Trade, No. 7, 2018.

[10]Chen Ruihua: "ZTE's Special Compliance Program", Chinese Lawyers, No. 2, 2020.

[11]"In 2023, Which Chinese Enterprises Were Sanctioned by the United States Again", https://www.163.com/dy/article/ILCL4E470552NHJB.html, last accessed on January 16, 2024.

[12]John Smith, Criminal Law: Cases and Materials, Butterworths, 2002: 375.

[13]Lin Junhui: "A Review of the Value of Conspiracy Rules in Anglo-American Criminal Law", Journal of National Prosecutors College, No. 4, 2012, p. 147.

ISSN: 2710-0170

[14]:Zhang Silu: "A Re-examination of the Effect of Long-Arm Jurisdiction and Its Enlightenment to China", Gansu Social Sciences, No. 5, 2017, p. 180.

[15]"The Whole Story of ZTE Incident: A More Profound Reflection Than the Fine", https://www.jfinfo.com/news/20180418/1304151, last accessed on January 29, 2024.

[16] Frédéric Pierucci, [France] Matthieu Aron: The American Trap, CITIC Press, 2019, p. 21.

[17]: "ZTE Reaches Settlement with U.S. Government, Agrees to Pay $890 Million Fine", https://www.thepaper.cn/newsDetail_forward_1634305, last accessed on January 29, 2024.

[18]Zhang Zetao: "Standardizing Deferred Prosecution—Drawing Lessons from the U.S. Deferred Prosecution System", Chinese Criminal Science, No. 3, 2005, p. 66.

[19]Chen Ruihua: "ZTE's Special Compliance Program", Chinese Lawyers, No. 2, 2020, p. 88.