

# The Boundaries and Legal Regulation of “Long-arm Jurisdiction” in Cross-border Cryptocurrency Crimes: A Case Study of the Chen Zhi Case

Haoyu Fan

*Koguan School of Law, Shanghai Jiao Tong University, Shanghai, China*

**Abstract:** With the development of blockchain technology, cryptocurrency has gradually become one of the financial hotspots. However, its virtuality, cross-border nature, and pseudo-anonymity have given rise to a new type of cross-border crime. Cryptocurrency essentially belongs to cyberspace, and the traditional international jurisdiction system based on the "territorial principle," constructed around physical space, struggles to cope. Countries like the United States misuse "long-arm jurisdiction," leading to a series of judicial sovereignty disputes and jurisdictional conflicts. This article, using the Chen Zhi case as an entry point, focuses on the difficulties of applying traditional jurisdictional theories in cross-border cryptocurrency crimes. Meanwhile, by adopting case study and comparative law methods, this paper deconstructs the judicial documents of the Chen Zhi case. It proposes a "reasonable connection" standard, incorporating proportionality, to assess the legitimacy of a nation's jurisdictional actions, define the boundaries of "long-arm jurisdiction," and create conflict resolution and relief mechanisms through international cooperation, aiming to balance crime fighting and the healthy development of digital finance.

**Keywords:** Cross-Border Cryptocurrency Crime; Long-Arm Jurisdiction; Judicial Jurisdiction; International Legal Coordination; Chen Zhi Case

## 1. Introduction

Technological innovation has not only brought about financial model innovation but has also given rise to new types of cross-border crimes. The characteristics of cryptocurrencies make them ideal tools for crimes such as money laundering, fraud, and terrorist financing. These

criminal activities are highly virtual, cross-border, complex, and hidden, posing a significant challenge to the traditional international jurisdiction system based on the "territorial principle" built around physical space. In recent years, "long-arm jurisdiction" has gradually become an important means for the United States to expand its judicial jurisdiction in the field of crypto assets and seek financial dominance.

Currently, Chinese academia largely rejects the "long-arm jurisdiction" practices of the U.S., with the representative view considering the "effects" principle at the core of "long-arm jurisdiction" is not widely accepted as an international legal norm. The U.S., when exercising "long-arm jurisdiction," often violates international obligations, infringes upon the sovereignty of other countries, and disregards the international norms of "reasonableness" in international law<sup>[1]</sup>. At the same time, to address the issue of various countries expanding their jurisdiction in cyberspace, the mainstream academic attitude toward this issue is that it is necessary to break through the traditional jurisdiction system based on territoriality and consider more "substantive connections," for example, some scholars suggest embedding the "real harm principle" into the "territorial principle"<sup>[2]</sup>.

United States v. Chen Zhi, a/k/a “Vincent” case (the “Chen Zhi Case”), involving wire fraud conspiracy and money laundering conspiracy, is a representative case. It showcases core issues such as determining jurisdictional connection points, jurisdictional conflicts, and the procedural justice of asset confiscation in criminal cryptocurrency cases, providing an important empirical sample for studying the application boundaries and regulatory pathways of "long-arm jurisdiction" in this field. Clarifying the boundaries of "long-arm jurisdiction" in cross-border cryptocurrency crimes and constructing a scientifically

reasonable legal regulatory system is of great theoretical and practical significance for balancing judicial sovereignty and combating cross-border cryptocurrency crimes.

## 2. The Manifestation of Jurisdictional Conflicts in the Chen Zhi Case

The core criminal entity in the Chen Zhi case is the "Prince Holding Group," which has long been active in Cambodia. It mainly engages in fraud and money laundering crimes through crypto assets. In 2020, FBI received multiple reports alleging that the Prince Holding Group was engaged in fraudulent activities. Due to a technical flaw in the cold wallet that stored the large amount of Bitcoin held by the Prince Holding Group, the U.S. Department of Justice was able to seize control of the wallet. By 2025, the case's first trial concluded, with U.S. law enforcement seizing 127,000 Bitcoins controlled by the Prince Holding Group, valued at over \$15 billion, setting a record for the largest cryptocurrency seizure in global history.

The term "long-arm jurisdiction" originally referred to U.S. state courts exercising jurisdiction over defendants outside their state based on "minimal contacts principal" in civil litigation<sup>[3]</sup>. This concept has now been expanded to cover the U.S. and other countries extending judicial jurisdiction beyond their borders, along with foreign law enforcement actions and sanctions. It is necessary to distinguish it from the concept of "extraterritorial jurisdiction" here. Generally speaking, "extraterritorial jurisdiction" is a relatively broad concept of legal application, referring to a country extending its legislative, judicial and law enforcement powers beyond its territory and exercising these jurisdictions outside its territory. In contrast, "long-arm jurisdiction" mainly emphasizes the jurisdiction of courts, that is, courts exercising judicial jurisdiction over non-residents of the country (state). In the *World Volkswagen Corp. v. Woodson* case, the U.S. Supreme Court explained the standard for "long-arm jurisdiction," stating that it requires "minimum contacts" and emphasizing the defendant's purposeful actions and the foreseeability of being subject to the jurisdiction of the court where the case is filed<sup>[4]</sup>. These contacts must not violate basic principles of "fairness" and "substantive justice"<sup>[5]</sup>.

In the context of international criminal

jurisdiction, two principles are generally followed: one is the traditional "territorial principle," which asserts that a country has jurisdiction if the criminal behavior or its results occur within its borders; the other is the "substantial connection" principle, which requires that the country seeking jurisdiction has some degree of connection to the case. It is generally believed that territorial jurisdiction holds a higher rank. For example, in the *Bankovic v. Belgium* case at the European Court of Human Rights, the court held that "international law does not prohibit a country from exercising extraterritorial jurisdiction, but such jurisdiction is subject to the territorial sovereignty of other countries"<sup>[6]</sup>.

The main criminal acts of the Prince Holding Group took place in Cambodia, where the core management of the group operated. Under the territorial principle, Cambodia should have priority jurisdiction over the case. However, without Cambodia's consent, the U.S. directly exercised jurisdiction over the case and seized assets, disregarding Cambodia's territorial jurisdiction and, to some extent, violating Cambodia's judicial sovereignty. At the same time, the connection between the U.S. and the case is weak. According to the U.S. Department of Justice's indictment, the U.S. involvement in the case is based on three points: 1) the "Brooklyn Network" was part of the Prince Holding Group's criminal network located in the U.S.; 2) money laundering activities were conducted using accounts opened in U.S. financial institutions; 3) about 250 U.S. citizens were victims, with a total loss of approximately \$18 million<sup>[7]</sup>. Although the total amount involved is indeed large, it only accounts for 0.12% of the total amount of the crime. While these connections may justify some jurisdiction, the main issue is that the U.S. judicial authorities' seizure of 127,000 Bitcoins far exceeds the scope of criminal activity that actually affected the U.S. or its citizens.

As some scholars have pointed out, "The regulation of illegal acts outside the region is inseparable from the need of the power subjects within the region to maintain their internal order"<sup>[8]</sup>. That is, the United States hopes to adopt a dual approach of "long-arm jurisdiction" by courts and technological superiority in the crypto asset field to maintain its status as a central country in the international financial system, and take the lead in establishing

governance rules and operational mechanisms that are favorable to it<sup>[9]</sup>.

### **3. The Boundaries of “Reasonable Jurisdiction” and “Long-Arm Jurisdiction” in Cross-Border Cryptocurrency Crimes**

#### **3.1 Lack of Unified Stance and Standards on the Classification and Regulation of Cryptocurrency Crimes in Different Countries**

It is generally acknowledged that sovereign states possess jurisdiction by virtue of their sovereignty can be divided into legislative, judicial, and enforcement jurisdiction<sup>[10]</sup>. The "long-arm jurisdiction" discussed in this article specifically refers to the extraterritorial exercise of judicial jurisdiction.

Regarding the classification of cryptocurrency, different countries adopt different stances. For example, mainland China classifies all cryptocurrency-related financial activities as illegal financial activities. The European Union has passed the Market Regulation for Crypto Assets (MiCA), classifying crypto assets into three types, restrictions are only imposed when certain crypto asset trading activities may cause significant harm to investors' interests or threaten financial stability<sup>[11]</sup>. The U.S. generally classifies cryptocurrencies into three types: currency, commodities, and securities, gradually establishing regulatory frameworks for specific categories of cryptocurrency activities, for instance, the “GENIUS Act”.

These varying classifications, stances, and regulatory approaches mean that the legal relationships involving cryptocurrency in different countries may differ. In the criminal field, this implies that whether certain cryptocurrency-related behaviors are criminalized in different national legal systems may vary. Given the decentralized and international nature of cryptocurrencies, jurisdictional disputes are almost inevitable. For example, in the Chen Zhi case, Cambodia later claimed that the Prince Holding Group's operations in Cambodia complied with local law after the case was exposed.

In summary, the international community currently lacks a unified understanding of the nature of cryptocurrencies. Differences in legal regulatory stances and systems may result in a "jurisdictional freedom" scenario, where multiple countries may claim jurisdiction over a

cryptocurrency crime due to the decentralized nature of cryptocurrencies and the widespread presence of digital traces. Some countries may be prompted to engage in "profit-driven law enforcement" while excluding other nations' territorial sovereignty and solidifying the technological advantages of certain countries, leading to the expansion of hegemony in the virtual world<sup>[12]</sup>.

#### **3.2 Technological Development Presents a Disruptive Challenge to Traditional National Jurisdictional Powers**

Blockchain technology is characterized by anonymity and decentralization, but its anonymity is not absolute. While law enforcement agencies can use blockchain tracing technology to track transaction paths, linking an anonymous wallet address to a real identity remains a significant technical challenge, especially since criminal organizations often use mixers to further obscure the original flow of funds. These technological tools place higher technical demands on law enforcement agencies. In the Chen Zhi case, the U.S. demonstrated its technological advantage in blockchain analysis and digital currency tracking, allowing it to trace the flow of funds and ultimately seize the assets even though the cryptocurrency was decentralized. However, not all countries have this technological capability. Cryptocurrency crime organizations are often located in regions with relatively lax regulation and unstable political environments, such as Southeast Asia and Latin America, these countries may not have specialized technical teams to prevent or investigate such crimes, or may even lack the necessary technical capability.

This implies that countries traditionally able to exercise jurisdiction based on the territorial principle may, due to technical limitations, subjective recognition, and political stances, fail to effectively investigate or prosecute cryptocurrency crimes. Meanwhile, countries with the technical ability and motivation to exercise jurisdiction over such cases may be relatively weakly connected to the crime—at least, criminal organizations often do not choose to operate in countries with more advanced regulatory and technological frameworks.

Additionally, traditional criminal jurisdiction theories rely on the location of the crime or the location of its results as the main basis for establishing jurisdiction. However,

cryptocurrency crimes are highly decentralized and uncertain in terms of their location. Transactions are not limited by geographic space and time, and theoretically, the number of transfers a cryptocurrency can undergo in one day is unlimited.

In conclusion, the decentralized, highly liquid, and anonymous nature of cryptocurrencies makes jurisdictional attribution extremely difficult. The decentralized nature of cryptocurrency transactions creates multiple potential jurisdictional connection points, further increasing the risk of jurisdictional disputes. The actual locations of VASP platforms, criminal organizations, and victims are often not aligned, and determining these locations is inherently challenging.

### **3.3 The Lack of Unified Standards in Determining the "Substantial Connection" in Cross-border Cryptocurrency Crimes**

As mentioned earlier, the decentralized characteristics of blockchain and cryptocurrencies make it difficult to determine jurisdiction based on the "territorial principle." Therefore, the "substantial connection principle" becomes critical. In current customary international law on jurisdiction, common substantial connections include territorial connections, personal connections, and connections based on national interests or victim status<sup>[13]</sup>.

However, if only a qualitative perspective is taken into account while neglecting quantitative considerations, the "substantial connection" is also meaningless in cross-border crypto asset crimes. In the Chen Zhi case, it is acknowledged that there is indeed a connection point between the U.S. and the criminal activities of the Prince Holding Group. Firstly, one of the Prince Holding Group's criminal networks was based in the U.S., using U.S. financial institutions to open fraudulent accounts for money laundering, thereby violating the U.S.'s financial management order. Secondly, there were U.S. citizens among the victims, and the group's fraudulent activities harmed their property rights. In this sense, the U.S. exercising protective jurisdiction is not unreasonable, and therefore, the U.S. Department of Justice's charges of wire fraud and money laundering are supported by factual evidence.

The unreasonable aspect of the U.S. jurisdiction in this case lies in its exercise of jurisdiction in

an "all or nothing" manner-seizing 127,271 Bitcoins, which far exceeds the scope of losses suffered by U.S. citizens. The international nature of cryptocurrency crime means that it often has multiple connection points. When evaluating these points under the "substantial connection principle," an overly broad interpretation of "substantial" would still lead to a situation similar to the "territorial principle," where multiple countries claim jurisdiction. If these countries can intervene "all or nothing," it would inevitably infringe upon the judicial sovereignty of other nations and increase the legal costs for victims located in other countries. This also creates a situation where certain countries, through this "jurisdictional arbitrage," would undermine fairness and justice.

There is currently a lack of a unified international consensus on the criteria for determining the "principle of substantive connection" in the jurisdiction of crypto asset crimes and whether there is a certain hierarchy among the various connection points enjoyed by "substantive connection". This legal vacuum makes certain countries' jurisdictional actions appear reasonable because they do have connections to the case. However, a horizontal comparison of these connections reveals their weakness (for example, the proportion of funds lost by U.S. victims).

## **4. Legal Regulatory Path for "Long-Arm Jurisdiction" in Cross-Border Cryptocurrency Crimes**

### **4.1 Establishing the Boundary Recognition Standard for "Long-Arm Jurisdiction"**

As mentioned earlier, applying the traditional "territorial principle" to address cryptocurrency crimes has become inadequate. On one hand, cryptocurrency crimes have virtual characteristics, meaning they do not depend on physical contact to commit crimes, nor can geographical concepts be used to assess criminal behavior and outcomes. On the other hand, cryptocurrency crimes tend to exhibit highly decentralized characteristics. Criminal behaviors, settlement platforms, and victims are usually spread across multiple judicial jurisdictions, and this "pervasive territoriality" creates intense conflicts over jurisdiction.

Therefore, the substantial connection principle is crucial and has become an important standard for assessing whether certain countries are

abusing their technological advantages to expand their jurisdiction. This should also take into account the principle of proportionality. That is, the judicial actions taken by the jurisdictional country-particularly with respect to the scope of the case (whether it is the full case or just part of the criminal behavior) and the execution of assets (whether it concerns all of the involved assets or just a part)-should align with the connection between the country and the case in a proportional manner.

This proportionality requirement is not a totally new concept. In fact, the U.S. courts once established the "reasonable jurisdiction principle" to ease jurisdictional conflicts arising from the U.S. taking judicial actions against foreign criminals. Under the "reasonable jurisdiction principle," U.S. courts considered the proportion between the domestic and foreign parts of a crime and the conflict with foreign laws, the effectiveness of enforcement measures, and other factors in determining whether they could exercise jurisdiction over the case<sup>[14]</sup>. However, this principle was later overturned in judicial practice, replaced by the "effects theory." According to the "effects theory," as long as a foreign company has a branch in the host country and engages in business activities, the host country can exercise personal jurisdiction<sup>[15]</sup>. This "effects theory" was adopted by the U.S. in the Chen Zhi case, where the criminal network of the Prince Holding Group in New York was a key point for U.S. jurisdiction.

From the perspective of strict interpretation, when elaborating on the "principle of reasonable jurisdiction", in the case of cross-border crypto asset crimes, first of all, the relevance should be considered, that is, first, the core links of the criminal act, such as the main channels for criminal planning, organization and implementation, and fund transfer, should be located within the territory of the host country; second, the defendant has an intentional connection with the host country. That is, the defendant must proactively carry out activities related to the crime in the host country, such as false promotion, attracting investors, setting up branches, etc. in the country where the court is located, and be able to foresee that their actions may be subject to the jurisdiction of the host country. Third, the direct and specific impact of the case on the interests of the host country, rather than abstract or potential ones.

Secondly, proportionality needs to be taken into

account, that is, the contribution or proportion of the aforementioned three types of related elements in the entire case. That is, on the one hand, the contribution degree of the criminal act located in the host country to the criminal act of the entire criminal group; on the other hand, The number of victims located in the host country, the amount of losses, and the degree of infringement upon the order of the host country account for the proportion of the harmfulness of the overall criminal acts of the criminal group. This determines the scope of jurisdiction that the host country can have and whether the overall jurisdiction of the case is reasonable. Only when all three elements are dominant can the overall jurisdiction of the host country be completely reasonable. Finally, it is necessary to determine whether the jurisdiction of the host country is conducive to the sanctions against criminals and the protection of the rights and interests of victims. This requires a comprehensive consideration of the transparency of the host country's legal system as well as the capacity and efficiency of law enforcement agencies.

Overall, when it comes to the jurisdiction of crypto asset crimes, both the traditional territorial principle and the principle of substantive connection have become inadequate in response. It is necessary to reconstruct a judgment standard for "substantive connection" with the principle of proportionality as an important reference. However, we should also recognize that the requirement to fully meet the above three elements is rather strict. Therefore, it is necessary to further clarify the hierarchy of effectiveness of various elements. First of all, the principle of proportionality should be the first to be considered. If, on the whole, a certain criminal act of a criminal group within the territory of the host country accounts for a large proportion of the overall criminal acts, then of course there will be a certain correlation. At this point, What we need to consider is how to implement and effectively safeguard the interests of the victims. Such issues are result-oriented considerations and do not necessarily affect the rationality of jurisdiction. However, when there is a situation where the national court is "unwilling, unable, inconvenient or unable to effectively exercise jurisdiction or with the express and prior consent of the state"<sup>[16]</sup>, the consideration of the remaining two factors will result in different evaluations due to different positions. If the position of giving priority to

national sovereignty is adhered to, then the relevance has priority effect. If the position of protecting the interests of the victims is adhered to, then the jurisdictional motivation, jurisdictional capacity of the host country and the rationality of the establishment of the mechanism for returning the confiscated involved property are at a higher level. This may need to be balanced in individual cases.

#### **4.2 Establish a "Global Co-Management" Jurisdiction Mechanism for Crypto Asset Crimes**

The traditional model where sovereign states exercise jurisdiction individually may lead to some cross-border cryptocurrency crimes being inadequately addressed. Due to the virtual nature of cryptocurrency crimes, proving the intentional connection between the defendant and the country of the court is often difficult. Criminal organizations can avoid forming significant connections with any country by using anonymous networks, offshore servers, and other methods, resulting in a jurisdictional vacuum where no country can exercise jurisdiction based on the substantial connection principle. Additionally, in enforcement, the "dual criminality" principle is an important requirement for cross-border judicial assistance and extradition. However, in cross-border cryptocurrency crimes, the differences in how countries classify and recognize crimes involving cryptocurrencies create significant barriers to applying the dual criminality principle.

Therefore, rather than solely evaluating the effectiveness of a country's jurisdiction from a legal perspective, an outcome-oriented approach should be adopted. Traditional territorial law enforcement is unable to resolve the jurisdictional conflicts in cryptocurrency crimes effectively, nor can it address the growing nature of these crimes. A global "shared jurisdiction" model should be developed to address this issue, focusing on international cooperation in combating cross-border cryptocurrency crime<sup>[17]</sup>. This mechanism can be established through the conclusion of multilateral treaties. For instance, through treaties, the scope and nature of crimes involving crypto assets can be clearly defined, and the standards for defining crimes can be unified, providing a clear basis for the application of the principle of dual crimes. International cooperation rules for the

jurisdiction of cross-border crypto asset crimes can also be established through treaties, clearly defining the criteria for determining jurisdictional connection points, methods for resolving jurisdictional conflicts, and procedures for cross-border law enforcement cooperation, etc. Even in the treaty, a dedicated judicial institution can be established to have jurisdiction over cross-border crypto asset crimes.

Furthermore, in cross-border cryptocurrency cases, the crucial issue might not necessarily be which country exercises jurisdiction, but how the jurisdictional country manages the seized cryptocurrency assets. Therefore, the focus of the remedy mechanism for "long-arm jurisdiction" should be on the rationality of how the jurisdictional country handles the seized assets. It is necessary to assess whether the amount of cryptocurrency seized by the jurisdictional country aligns with its connection to the case. If it is disproportionate, the jurisdictional country should not hold assets beyond what is justifiable. The question of whether these assets should be held by a third-party neutral institution and how to establish a fair mechanism for victim compensation should be further studied.

#### **5. Conclusion**

This article uses the Chen Zhi case as an empirical example to deeply analyze the practical application and jurisdictional disputes of "long-arm jurisdiction" in cross-border cryptocurrency crimes. It also proposes corresponding legal regulatory paths. Some host countries use technological advantages and dominance in the cryptocurrency market to establish "long-arm jurisdiction," which can effectively combat cross-border cryptocurrency crimes to some extent, its application also faces multiple dilemmas, such as blurred jurisdictional connection points, intensified jurisdictional conflicts. To effectively address these issues, it is necessary to clarify the boundaries and determination criteria of "long-arm jurisdiction" and avoid the abuse of jurisdiction. A diversified mechanism for coordinating jurisdictional conflicts should also be established to promote legislative coordination among countries, avoiding the law becoming an extendable tool of political power<sup>[18]</sup>.

It should be noted that this study has some limitations, as it only analyzes the Chen Zhi case. the operational model of cryptocurrencies is

diverse, and the crimes involved are varied. Whether the jurisdictional standards discussed here can be applied to different types of crimes is an area that requires further study. Additionally, if a multilateral treaty approach is adopted to resolve jurisdictional crises related to cryptocurrency crimes, the specific contents and operational mechanisms of the treaty have not been detailed here. Finding a balance between effectively combating crime and avoiding the establishment of cryptocurrency hegemony through international collaboration is a critical issue worth pondering and striving for.

### References

- [1] Xiao Yongping.(2019)Legal Analysis and Countermeasure Research on 'Long-Arm Jurisdiction'. *China Legal Science.*, 6: 39-65.
- [2] Zhang Ting, Chen Li.(2023)The Application Dilemma and Solution of Criminal Jurisdiction in Transnational Cybercrimes. *Journal of South-Central Minzu University (Humanities and Social Sciences Edition).*, 10:108-115.
- [3] The "LONG ARM STATUTE" in the Legal Dictionary entry, <https://legaldictionary.net/long-arm-statute/>, visit date on December 27, 2025.
- [4] Yang Yuguan.(2022)The Origin, Expansion and Response of Long-Arm Jurisdiction in the United States. *Legal Journal.*, 4: 73-92.
- [5] *International Shoe Co. v. Washington*, 326 U.S.310(1945).
- [6] *Bankovic v. Belgium et al.* ,Application No 52207/99,123 ILR 94.
- [7] *United States v. Chen Zhi, a/k/a "Vincent"*, No 25-CR-312.
- [8] Qu Wensheng.(2021)From Extraterritorial Jurisdiction to Extraterritorial Regulation: From the Perspective of Jurisdiction Theory. *Social Sciences in China.*, 4: 44-66.
- [9] Song Shuang. (2025)Political and Economic Analysis of U.S. Digital Asset Policy during Trump 2.0. *Contemporary American Review.*, 2:65-84.
- [10] Harold G Maier,Extraterritorial Jurisdiction at a Crossroads:An Intersection Between Public and Private International Law, 76 *American Journal of International Law*, 280(1982); Anthony J.Colangelo, What is Extraterritorial Jurisdiction,99 *Cornell Law Review*, 1310(2013).
- [11] Yi Yan.(2025)Main Contents of the EU Crypto Asset Market Regulation Act. *China Money Market.*, 5:73-76.
- [12] Kan Daoyuan.(2021)Analysis of the United States' 'Cyber Freedom' Strategy. *Modern International Relations.*, 8:18-23.
- [13] Wu Peiqi.(2022)What is' Extraterritorial Jurisdiction ': Tracing Its Origin, Correcting Its Name and Theoretical Adjustment. *Nanjing University Law Journal.*, 1:18-36.
- [14] M. Matsushita, T. Schoenbaum and P. Mavroidis, *The World Trade Organization* ( 2nd edn. , Oxford: OUP, 2006), 866.
- [15] Jia Bingbing.(2022)International Public Law: Interpretation and Application in Peacetime. *Tsinghua University Press.*, 2nd Edition, August 2022:281.
- [16] Liu Jian.(2004)On the Jurisdiction of the International Criminal Court and State Sovereignty. *Legal Science. Journal of Northwest University of Political Science and Law.*, 5:85-89.
- [17] Shao Yi.(2021)Long-Arm Jurisdiction of Network Data: From the 'Minimum Connection' Standard to the 'Global Co-Management' Model.*Law and Business Research.*, 6:73-87.
- [18] Orde F. Kittrie, *Lawfare: Law As A Weapon of War*, Oxford University Press, 2016, p. 14.