

# TEMPORARILY APPLICABLE MODEL FOR INTERNATIONAL CRIME DEFENSE

LinFeng Murong

*Yuan Yang Volunteer Team of Xinghua Public Welfare Foundation, Hangzhou 310020, Zhejiang, China.*

*Corresponding Email: [muronglinfeng2024@qq.com](mailto:muronglinfeng2024@qq.com)*

**Abstract:** With the increasing severity of international crime, traditional model backgrounds and assumptions can no longer meet the analysis requirements. This article appropriately adopts a new type of analysis model to analyze defense measures for police or government department, create a new concept of "Long Loong block information module".

**Keywords:** International Crime; Defense; Model; Long Loong block information module

## 1 INTRODUCTION

At the present stage, in the face of changing international conditions, international crime is becoming more and more prevalent. As a matter of fact, "lone wolf" terrorist crimes are getting more and more intense, and terrorist activities are adept at conveying ideological and emotional messages in cyber contexts, stimulating the anger of youth groups against society through narratives that are both true and false. They are stealthy, sudden and random, and most of them are guided and organized in some way.

## 2 PAPER AND TEXT FORMAT

### 2.1 Model Background and Assumptions

How to make the defense? The difficulty of investigating international crimes is still very high, and with the border nature of the Internet not being obvious, this state of affairs is particularly serious, such as the recent terrorist attacks in many countries, where the attacks have all appeared to be dominated by foreigners in the territory of the "lone wolf" type of pattern, and the other party usually has a secondary transfer or movement outside the country, which is extremely rare for this kind of blatant approach. Such a approach is extremely rare.

At present, the international community mainly through the United Nations Conventions, such as the United Nations Convention Against Corruption and the United Nations Convention against Transnational Organized Crime [1], through joint law enforcement, repatriation, cross-border pursuit and other ways to achieve counter-terrorism cooperation, but all of the above ways are based on the basis of the other country has a good police structure, and the country has signed a bilateral agreement in goodwill and strictly abide by the convention, but in reality, most of the time, this assumption is not the case, and the other country has a good police structure, and the country signed a bilateral agreement and strictly comply with the convention. However, in most cases, this assumption is difficult to realize. The United Nations Convention against Corruption and the United Nations Convention against transnational organized crime can be seen in Figure 1.



**Figure 1** The United Nations Convention Against Corruption and the United Nations Convention against Transnational Organized Crime

Therefore, the author's main point is how to use a temporarily applicable international crime defense model under the existing worldview structure, due to the existence of geographical attributes of the country, but the imbalance in the transmission of information, such a model also leads to the poor control capacity of the state will become the main base of the crime, while the control capacity of the state will become the main target of the attack, the result is that the poor control capacity of the region may become the main target of the attack. As a result, regions with poor control capacity may become stooges and be used exclusively for attacking regions with strong state control capacity, because the harvest is also quite rich once it is achieved.

Correspondingly, there is the problem of different standards in international multilateral cooperation, for example, there are often different standards in evidence collection or research outside the country, some countries are legal, some countries are not legal, which also leads to the source of jurisdiction is difficult. Thus, the international crime defense temporarily applicable model are mainly used for the domination of the national crime defense, the author believes that the international social reality of the country is not controllable.

## 2.2 4-Step Temporarily Applicable Model

Based on the above model premise parameter assumptions, and thus put forward a 4-step defense model of the international crime defense, according to the source of the crime defense, the border in the middle, the back section, the end of the four stages of the defense stage, to analyze, in which the source and the ordinary middle is currently unable to Effective defense, which is based on the above model assumption premise, the offender, through the underground money laundering and transfer between countries, resulting in crime investigation and forensic difficulties in the assumption premise, and thus not in the model to consider the scope:

### 2.2.1 Source segment

the source jurisdiction ability to enhance lies in whether the standard is consistent, even if the relevant agreements and cooperation with the other country signed, based on the above assumptions, crime evidence collection and efficiency is difficult to be able to achieve results. For example, in the legal regulation of the Internet, certain countries emphasize the Internet enterprises themselves and industry self-regulation; while some countries such as Germany in the fight against malicious speech on the Internet to take harsh legal means, such as the Network Enforcement Act to regulate social networks [2]. The non-uniformity of the concept of terrorist crimes has become the key to hinder the international community's cooperation in combating terrorist crimes [3], and the different regulatory means directly affect the prevention and combating effects of cybercrime in various countries [4]. So the source segment defense mode features good or bad is very obvious, depends entirely on the source country jurisdiction ability and way, the evaluation standard is the local crime situation, if the source segment of the country continues to frequent such events, it proves that the source defense is actually a failure, even if the signing of the agreement, in fact, can not be effectively implemented.

### 2.2.2 Border field defense

this part as an autonomous and controllable defense, belongs to an important defense strategy. In the case of source defense is out of control, this defense becomes particularly important, for all the acts of entering the border, theoretically should be included in the supervision or jurisdiction, such as repeated illegal access to foreign ip should be effectively monitored and prevented, at least there should be effective measures to prevent it, completely free without any control measures is not appropriate, including visa, even if it is a visa-free entry, should also be registered. Necessary information identification, if the other country retained information identification is unreliable, it is necessary to carry out compensatory collection work, used to record the track of activities related to follow the relevant laws of their own countries.

This kind of defense is usually a blockchain-like level, the main reason for choosing a similar title, rather than the name of blockchain directly, mainly because of the special fragmentation of the information, resulting in the integration of information has been very difficult, but because most cases do not need to be decentralized, and information interaction needs to be tampered with the history of the data, resulting in the actual behavior of the flow of information, only cloaked in the name of the blockchain, but in fact, is not a blockchain mode, this gave birth to a new concept, and I has newly named this concept as "Long Loong block information module". In practice, there has been a prosecutor's office by refining the case elements: identity information (such as nicknames, etc.), social account information (such as WeChat, etc.), financial account information (such as Alipay, etc.), up and down the family relationship information, to build a "digital portrait" database, and through the modeling of intelligent algorithms, query the real identity or money laundering clues [5], with the traditional decentralized blockchain. The traditional decentralized blockchain is different, this practice commonly used in the process of information extraction and analysis paradigm, can be fully integrated into a kind of blockchain model, that is, for the "Long Loong block information module", as the main component of the domain defense architecture model, this module for the automation of the border domain defense interactions is very effective, and the efficiency of the case is very high. And the case handling efficiency is very high. By writing the algorithm of intelligent interaction of the module, the above information identifiers will be passed through the storage mode of the block for storage and interaction, on the one hand, it is used for the collection and exchange of data in various fields, and on the other hand, it is encrypted for storage, written through interaction and data tampering with proper authorization, and used for storing records. To cite a case of defense, a person has three WeChat groups with

hundreds of people, will create a module store in the "Long Loong block information module" as a block of "social account2", and when the payment interactions with all the people in the group reaches more than 200, an interaction algorithm in the "Long Loong block information module" is triggered. An interaction algorithm is triggered in the "Long Loong block information module", so that means the attribute module of the person will writes a block record of financial and interactions named "Internet e-commerce" module, encrypt and store it.

With large number of interactions at the same time by tampering with the historical block, these characteristic values are stored directly in the block information storage mode for easy extraction, sorting, and analyzing risks. Example of Long Loong block information module can be seen in Figure 2.

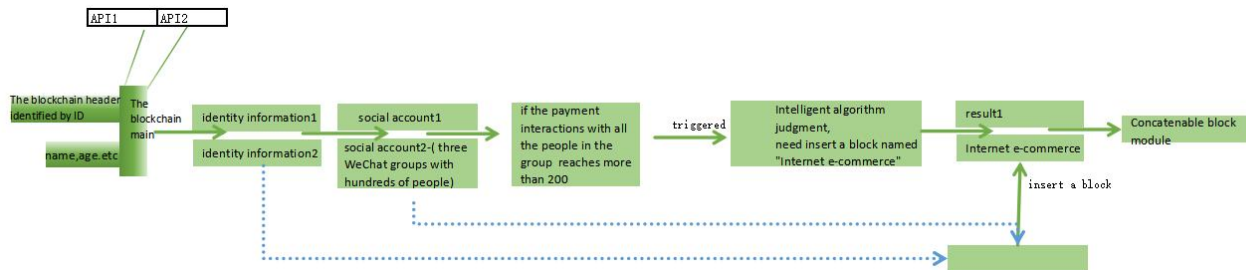


Figure 2 Example of Long Loong Block Information Module

### 2.2.3 Intruder defense mechanism

this part is similar to the normalized epidemic monitoring, due to the assumption of the source jurisdiction of the loss of control, this defense mechanism needs to be normalized, through regular supervision, patrolling and control, including but not limited to the normalized monitoring of the Internet, the major traffic areas, hot news areas or involving hot characters supervision and control, etc., used to prevent the occurrence of extreme violence, to prevent the adverse consequences and impacts. prevent the occurrence of extreme violence, and prevent adverse consequences and impacts. Due to the assumptions, the current practice of all countries in the world has already been established, and only the advantages and disadvantages can be compared to discuss how to enhance the defense. For example, in practice, developed countries tend to invest more resources in network security infrastructure, such as security protection systems and intrusion detection technology [6].

### 2.2.4 Citizen-level emergency defense mechanism

in the above three environments may be due to the loss of control of the source jurisdiction under the role of the problem, actually, this part will be the most important link, in the event of a major international crime to break through all of the above defenses, usually triggers the emergency defense mechanism immediately, especially the citizen-level defense, the minimum situation, in the confirmation of the international crime of people continue to commit crimes in the situation, the Citizens can mobilize emergency defenses to defend or prevent the attack, and these emergency defenses are reciprocal and parallel; citizens may request defense or warnings through regular reporting channels, while governments may also set up special emergency defenses for situations that threaten the safety of ordinary citizens, to investigate and interrupt major criminal acts before they occur. This part of the emergency defense record is mandatory to record, even if the false report, but also usually as a risk issue permanent record, to facilitate the relevant departments to make risk prevention.

In addition, for the crime reduction and compensation, follow-up analysis mechanism, is also very important, due to international crime, often presents the nature of the hidden investigation is limited, how to restore the crime chain and criminal motives is the key, usually although the difficulty of obtaining evidence is higher, but the adverse consequences are often obvious, even if it is the instruction of the attack, usually can be restored and follow-up analysis, which can usually be done through other ways of compensation or international negotiations.

## 3 CONCLUSION

In summary, the temporary application model of international crime defense leads to a very diverse and hierarchical deployment of resources for defense, but is equally costly. Through some new technologies and means, such as the "Long Loong Block Information Module", increased resource investment, emergency defense arrangement and effective record analysis, it is possible to compensate for the effective control of the three sections of the border defense: the middle section, the back section and the end section.

## COMPETING INTERESTS

The authors have no relevant financial or non-financial interests to disclose.

## REFERENCES

- [1] Zuo Zenan, Li Conger. Study on Police Cooperation in Overseas Fugitive Recovery in the Context of Economic Globalization. *Economist*, 2023(11): 53-56.

- [2] Sun Yu. Act to improve the enforcement of laws in social networks in Germany (referred to as "network enforcement law"). *Network Information Law Research*, 2020(2): 6.
- [3] Wang Jianbo. The concept of "terrorism" and its development under the perspective of the comprehensive convention against terrorism. *Chinese Journal of Criminal Law*, 2011(11): 108.
- [4] Huang Zhixiong. The "road controversy" of Internet regulation and the implications of its rules. *Law review*, 2019(5): 12.
- [5] Jia Yu. *Research on Legal Supervision of Big Data Investigation and Treatment*. China Procuratorial Press, 2022: 97-105.
- [6] Zhou Qi, Chen Kaixin. Exploration of international cooperation mechanism of network security. *Contemporary World and Socialism*, 2013(5): 4.