A Qualitative Examination of Cybercriminal Governance in China

Abstract

Profit-driven cybercrime has evolved into a sophisticated industry, inflicting millions of dollars in losses on the world economy. However, limited research has been conducted on the extra-legal governance of this industry, particularly in China, one of the world's most prominent cybercrime hotspots. This study, based on comprehensive fieldwork in China from 2020 to 2022 and an analysis of both primary and secondary data, seeks to address this gap. It endeavours to answer the question: *How is the cybercrime industry governed in China*? In line with previous research on extra-legal governance, this study finds that Chinese cybercriminals have developed a series of private governance systems, encompassing both self-governance and third-party governance, to facilitate their business interactions. In addition, this study offered three main new findings that can be added to our understanding of extra-legal governance. Firstly, self-governance is notably effective in online marketplaces due to the swift transmission of information, thus diminishing the necessity for third-party governance in the cybercrime market and the use of violence. Secondly, cybercriminal firms tend to be less predatory than traditional criminal firms, likely attributed to the reduced need for territorial resources. Lastly, cybercriminals can relocate to countries where protectors are present and continue their illicit activities remotely, with protection being more likely offered when the inflicted harm does not impact the protector's own country's residents, and the political and economic gains outweigh the costs. This availability of protection could potentially elucidate the ongoing global dispersion of cybercriminals.

Total Word Counts: 60617

Qiaoyu Luo
D.Phil. Sociology
St Anne's College
Michaelmas Term 2023

Table of Contents

Chapter 1. Introduction

Cybercrime has evolved into a sophisticated industry around the globe, causing millions of dollars in economic losses to the world economy (Levchenko, 2011; Leukfeldt, 2014; Lusthaus, 2018). But how is the cybercrime industry governed? A well-established governance system can "define and enforce property rights, adjudicate disputes, and mitigate the harms of externalities" (Skarbek, 2011, p.702). On the other hand, when such a system is lacking, cooperation becomes challenging, and it is difficult for criminal industries to scale up and thrive. While social science studies on criminal governance have looked at various conventional criminal industries (Gambetta, 1996; Varese, 2001; Skarbek, 2014; Shortland, 2019), there have been few attempts at cybercrime. Among the limited literature, Lusthaus (2018) first attempted to address the topic. However, since his study targeted profit-driven cybercriminal cooperation on a global scale, less detail was provided for specific countries, especially one of the world's cybercrime hubs – China. Adding to the body of literature on cybercrime, governance, and cooperation, this thesis aims to examine the cybercrime settings in China and explore how governance is achieved among Chinese cybercriminals to promote social order and cooperation. This topic has yet to be addressed in the literature, but it is vitally important to do so. Not only has China become a major cybercrime hub in recent years, but the country also presents additional challenges for cybercriminal cooperation in addition to those found in other jurisdictions.

This research is based on an intensive two-year period of fieldwork in China between 2020 and 2022. The in-depth interviews with law enforcement officers, prosecutors, cybersecurity practitioners, and formal cybercriminals, supplemented with invaluable secondary data collected during the fieldwork, together represent a significant advancement in the scholarly understanding of cybercrime. Markedly, this study is the first of its kind to empirically investigate Chinese cybercrime on such a large scale. The findings

demonstrate the intricate dynamics of cybercrime in China, revealing mechanisms of communication, cooperation, and dispute resolution amongst cybercriminals – aspects that operate outside the state's institutional boundaries. In addition to the novel empirical findings, this research provides substantial contributions to broader sociological theories of governance. It enhances our knowledge of what role the Internet plays in the cooperation process and how the element of anonymity can have an impact on the creation of governance.

This introductory chapter outlines the motivation for this research. First, it provides an overview of governance theory, which serves as the theoretical framework to guide this research. Second, it provides a review of the literature regarding cybercriminals' cooperation and the importance of governance therein. Third, it discusses the unique context of China, in particular how its internet environment suggests cybercriminal cooperation should be difficult to pull off. Fourth, it outlines the core focus of this thesis, generates the specific research questions based on the preceding discussion, and discusses the scope of the research. Finally, it outlines and explains the structure of the monograph.

1. Governance Theory

Criminals utilise governance to achieve better cooperation and facilitate their economic activities. In criminal settings, cooperation is often much more difficult to achieve than in lawful environments because criminals are in a situation of uncertainty, where the time horizon is difficult to calculate, and they are deprived of the protection of the law. This section pulls together some of the essential elements of governance and summarises previous studies about how cooperation has been successfully achieved among criminals through their establishment of extra-legal governance.

1.1 The Rational Choice Approach and the Effect of Governance

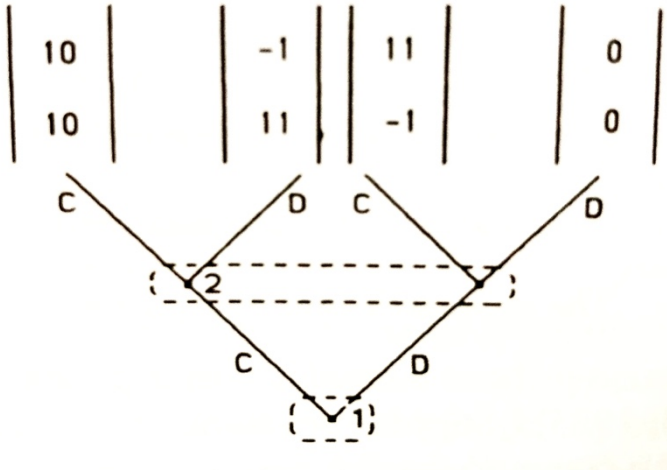
Criminal activities often seem puzzling at first sight: many criminals have a distinct appearance, way of talking, and way of living compared to ordinary people. Yet successful research experiences have shown that a good way to understand criminals and their activities is to study them as rational people, treating their actions and conduct as having underlying economic logic. Nevertheless, this approach does not assume decisions and actions made and conducted by individuals are perfect. As Skarbek (2014, p.3) notes: "People aren't robots. They sometimes make mistakes, get confused, satisfice, and struggle through a murky world of imperfect information and cognitive biases. However, when they recognise changes in costs and benefits, they respond to it". Thus, the rational choice approach recognises that the judgement of costs and benefits varies among individuals and the immediate situation.

Rational actors are self-interested. They act according to their own interests to pursue outcomes that value. However, being self-interested does not rule out the possibility of conducting altruistic actions as rational actors. When an overriding interest is presented, even the most selfish individual is incentivised to cooperate for their own personal interests (Schelling, 1990). Thus, as many studies show, cooperation can develop among self-interested actors, even between enemies, as a rational choice (Axelrod, 1990; Schelling, 1990; Hamill, 2010; Guzman, 2008; Gambetta, 2009; Varese, 2001; Shortland, 2019). One way to lure self-interested actors into cooperating is to create a system of governance that defines property rights and enforces agreements (Williamson, 1998; Skarbek, 2014; Ostrom, 1990; Leeson, 2014a; Barzel, 2002). According to Leeson (2014a, p.1), governance is "social rules that protect individuals' property and institutions of their

enforcement". The designated rules, coupled with punishments, can impose costs on uncooperative actors.

The effect of governance on affecting rational actors' choices can be best illustrated by

Figure 1: The Hardin Herder Game

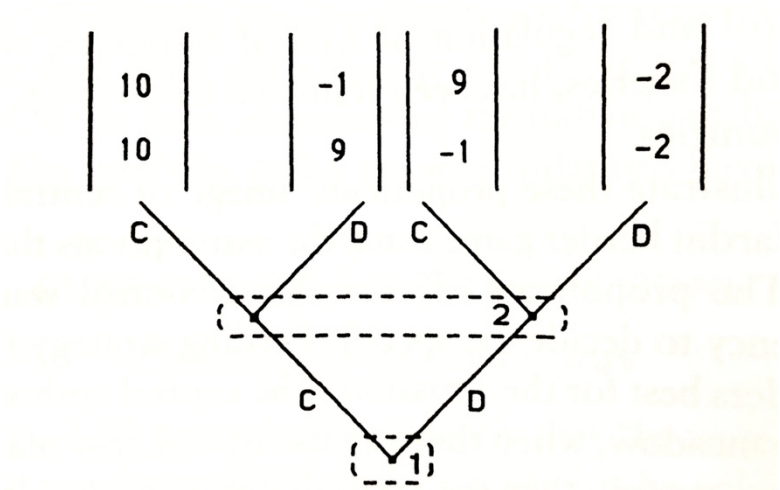


Note. From *Governing the Commons: The Evolution of Institutions for Collective Action* (p.4), by E. Ostrom, 1990, Cambridge University Press.

two games described in Ostrom's study (1990). The first game was introduced by Hardin (1968) and therefore called by Ostrom the 'Hardin herder game'. In the game, there are two herders who share a common grazing meadow to feed animals. The meadow can graze a maximum number of L animals in total. For the two herders, a 'cooperate' strategy is for each herder to graze L/2 animals, whereas the 'defect' strategy is for each of them to graze more than L/2 animals for a higher profit. Assuming each herder chooses to cooperate and only grazes L/2 animals, they will obtain 10 units of profit as a return. On the other hand, if both of them choose to defect and graze more than L/2 animals, they will obtain 0 profit. Finally, if one of them chooses to cooperate and the other chooses to defect, the defector will gain a larger profit by taking the other herder's benefit. In this case, the defector gets 11 unities of profit, and the "sucker" gets -1 units. The structure of the game is represented in Figure 1. In the Hardin herder game, to maximise one's profit and to always be better off, a rational herder will choose the defect strategy, regardless of the other's choice.

The second game has a slightly different setting. There is a central authority that governs the meadow and imposes punishments on the defectors. When the governor detects the defector, he will impose a penalty of 2 profit unities on the defector. The newly structured

Figure 2: The Central-authority Game with Complete Information



Note. From *Governing the Commons: The Evolution of Institutions for Collective Action* (p.4), by E. Ostrom, 1990, Cambridge University Press.

game is shown in Figure 2. In this case, the ideal solution for each herder to maximise their profit is to choose the cooperate strategy.

The different optimal equilibrium in the two games reflects the power of governance in affecting rational actors' choice to cooperate. Two points related to the second game need to be noted. First, the likelihood of the players choosing the cooperate strategy in game two is subject to the ability of the governor, including the design of a felicitous punishment scheme, to accurately spot the defection behaviour, and to make no errors in imposing punishments. These elements are not considered in the second game, and they affect the strength of governance. Second, as will be further discussed below, a central authority is not always required for governance. Social rules can be self-enforced. As long as rules are delineated, activities are monitored, and punishments are properly imposed, governance can be achieved without a central authority (Ostrom, 1990; Leeson, 2014a).

Cases of successful governance in boosting cooperation can be found around the globe. The economic achievement made by many states can be seen as one of the best examples. There are, however, many more examples in different social and economic settings. Governance provided by a state government represents only a fraction of the world's governance arrangements.

1.2 Private Governance

States and their government are the most commonly seen authorities that provide governance. Under the governance of the modern state, property rights are well defined by law, and the enforcement of the agreement is backed by the violently coercive power of the state. Institutions such as regulation, licences, insurance, courts and many others that address market problems and resolve disputes created by the modern state government have helped people capture the benefits from economic exchanges. They also encourage people to act collectively and refrain from taking actions against others and abusing common pool resources (Skarbek, 2014; Ostrom, 1990). In such a way, human predatory inclinations are constrained, and economic exchanges flourish (Hobbes, 2014; Barzel, 2002). For this reason, Hobbes famously claimed that without a solid government provided by the state, "there is always a war of everyone against everyone" (Hobbes, 2014, p.97).

However, research on governance has shown that the state and government are not the only capable authorities to provide governance. Alongside the state government, there is private governance, where individuals privately create social orders and institutions of their own enforcement (Leeson, 2014a). Examples of private governance can also be found in areas where religious organisations form and enforce agreements, especially those regarding family matters (Barzel, 2002), areas that are controlled by rebellions (Lessing, 2021; Chin, 2009; Shortland, 2019), and also criminals (Wang, 2017; Hamill, 2010;

Gambetta, 1996; Varese, 2001; Skarbek, 2014), who form the centre of this research topic and will be discussed further in the below sections. The governance services provided by a state government are limited within a territorial boundary. A state government does not govern criminal markets; it may decide to criminalise certain activities under a series of considerations, such as cost-benefits, cultural influence, and political and religious ideology. As a result, the governance services provided by the state government cannot reach these activities (Gambetta, 1996; Varese, 2001; Wang, 2017; Barzel, 2002; Leeson, 2014a; Lessing, 2021).

1.3 Self-Governance and Third-Party Governance

Private governance can be classified into two further broad categories: self-governance and third-party governance (Dixit, 2004). The boundary between the two categories lies in whether a designated third party is present to protect property rights and enforce social rules and agreements.

Under *self-governance,* social rules emerge as an automatic social process in the course of repeated interactions, taking the form of norms. Enforcement of agreements and norms in a self-governance system relies heavily on self-enforcement and communal punishment. One way for individuals to enforce an agreement and norms is to simply cut off future interactions with the wrongdoer. If the individuals value the stream of the benefit flowing from future interactions more than the short-term payoff of behaving in a proscribed manner, the threat of stopping future interactions can prompt them to adhere to behavioural proscriptions (Leeson, 2014b). Leeson (2014b, pp.366–367) calls it the "discipline of continuous dealing" and explains the underlying logic: “If you behave in a proscribed manner in your interaction with me today, I won’t interact with you tomorrow and may tell others not to interact with you either". This way of self-enforcement works particularly

well in long-term relationships when both parties are expecting profitable future exchanges (Barzel, 2002).

Individuals may also devise strategies to enhance the effect of self-enforcement or augment the discipline of continuous dealing. First, the parties may create an interdependent relationship. “Tearing the treasure map in half or letting one partner carry the gun and the other the ammunition” is a typical example of such situations (Schelling, 1990, p.135). By tiding up the interests of both parties, cooperation is achieved naturally while the parties pursue their own interests. Second, the parties may sacrifice freedom of choice irreversibly. By deliberately cutting his options, a party is able to prove his interest in cooperating. As Schelling (1990, p.22) claims: “Weakness is often strength, freedom may be freedom to capitulate, and to burn bridges behind one may suffice to undo an opponent". A similar concept is raised by Gambetta (2009, p.40), who notices that in pursuing cooperation, it is the constraints that are often stressed rather than the benefits: “If there are no ready-made constraints to display, there is still the option of designing some, of binding oneself in some way, of burning one’s bridge or tying one’s hand so that one’s partner knows that one could not defect even if one wanted to”. Third, a hostage is also frequently used to create a self-enforcing situation. An ancient example is marrying the daughter of the king to a ruler of an enemy country to ensure no defection can happen. The parties who wish to cooperate may also take hostages of themselves to create jeopardy in defection. Classic examples can be found in “drinking wine from the same glass” so that the safety of action is guaranteed (Schelling, 1990, p.135).

In a setting involving a group of people, communal punishment can take place to enforce agreements and norms. Collective actions in the form of boycotts, social isolation, and ostracism can take place to enforce rules and agreements. On some occasions, direct violence may also be applied to the wrongdoers as a consequence of violation (Barzel, 2002;

Elster, 2015; Skarbek, 2014). Since the burden is shared within a group, enforcement becomes more effective (Leeson, 2014a; Elster, 2015; Ostrom, 1990). Communal punishment also allows the reputation mechanism to function, which enhances the effect of the discipline of continuous dealing. The wrongdoer who develops a bad reputation from his wrongdoing will now be cut off from future interactions by not only his victim but the whole community (Leeson, 2014a). However, the effectiveness of communal punishment can be impeded by the size of the community. When the size of the community grows, communal punishment becomes less effective (Leeson, 2014a; Stringham, 2015; Landa, 1981; Skarbek, 2012; Ostrom, 1990). Information transmission is perceived to be a major problem in large communities. Information about dishonest behaviours must be easily disseminated to enough people for communal punishment to be applied. In large communities where there are more interactions between people, obtaining information about other people's wrongdoing is costly. The risk of detecting defections and violations therefore becomes low (Skarbek, 2012; Leeson, 2014a). Additionally, cultural differences can potentially influence perceptions of dishonesty, which further undermines the strength of the reputation mechanism (Leeson, 2014a). Finally, people who interact in large communities may face the collective action problem as everyone has an interest in not acting, and enjoys the benefits of free-riding (Olson, 1989; Ostrom, 1990; Skarbek, 2012; Stringham, 2015).

For *third-party governance*, social rules are commonly established in a more formal way, such as in the form of written code. In contrast to norms, the creation of formal rules requires a plentitude of resources. It involves a centralised decision-making process and requires a designated third party to interpret the rules and monitor the violations (Skarbek, 2014; Leeson, 2014a). The third party is also responsible for reinforcing the created rules, enforcing the agreements between the governed, and solving disputes in their territories.

According to Barzel (2002), third-party governance is more likely to be employed in four cases. The first is when the parties do not foresee a continuous net-benefit flow. For instance, a borrower is likely to defect as soon as he receives money from the lender because the relationship between the two parties is not synchronic, and the value of the agreement is not continually positive for both parties. In this case, the presence of a third party can guarantee the transaction. The second circumstance is when the information related to the interaction can be observed by an outsider, and it is costly for the participants to monitor the interaction. For instance, when there is a large number of parties in an agreement, each party will find it costly to identify violators. Hence a professional third-party governor is demanded. The third circumstance is when the expected time horizon of the relationship is short. Because repeated interaction is an essential element in self-governance, a third party is more likely to be employed to enforce agreements when the parties do not expect a long-term relationship. The final circumstance is when the cost of self-enforcement is high. In this case, employing a third party who can provide governance services may become a cost-efficient option.

Within the complexities of the real world, it is unusual to observe individuals or communities relying solely on one mode of governance, be it self-governance or third-party governance. Sometimes, the dichotomy of these two systems does not accurately reflect the multidimensional nature of the governance practices in human society. Instead, the two systems commonly coexist and interact, each compensating for the potential shortcomings of the other and together contributing to a comprehensive private governance system.

1.4 Governance within Markets and Firms

Governance systems are established to enhance cooperation within economic contexts. According to economics theory, particularly that which relates to industrial organisation, an economic context consists of markets and firms (Coase, 1937; Williamson, 1996)[1].

In essence, markets are "institutions that exist to facilitate exchange" (Coase, 2012, p.7). In markets, social actors interact and conduct social exchanges freely. A supplier delivers goods and services, receiving a predetermined payment from the buyer. However, exchanges in markets entail transaction costs, encompassing the costs of seeking information, negotiating, signing contracts, and resolving disputes (Williamson, 1996). To lessen these transaction costs arising from markets, firms are established. In contrast to markets, firms are economic organisations that internalise market exchanges. Within a firm, market transactions are eliminated and replaced by a coordinated production process directed by an entrepreneur. By signing a contract with the entrepreneur, and for a certain remuneration, the employee agrees to adhere to the directives of the entrepreneur within defined limits (Coase, 1937). Since the primary purpose of establishing firms is to minimise transaction costs, the boundary of firms lies at the point where the marginal cost of internalising transactions exceeds the marginal revenue. In other words, when economic transactions are infrequent and less complicated, operating within markets is preferable. Conversely, when transactions are regular, and the products or services are tailored to a specific transaction, the preference shifts towards firms (Coase, 1937; Williamson, 1996).

The distinct features of markets and firms significantly influence the forms of governance within them. Markets possess a horizontal structure. Parties within markets maintain their independence and flexibility to renegotiate terms. In the event of disputes,

[1] The concept of a network has been introduced and has attracted considerable discussion in recent years. While some scholars perceive the network as a third component, coexisting alongside markets and firms (Powell, 1990; Von Lampe, 2015), others view it as a broad concept that encompasses both markets and firms (Granovetter, 1985; Lusthaus, 2018). However, since the discussion of economic concepts extends beyond the scope of this thesis, the concept of the network is not employed here to avoid theoretical confusion.

they can freely utilise established governance mechanisms as is convenient. In the absence of state governance, self-enforcement emerges as a common cost-effective solution. Nevertheless, the institutional environment, characterised by factors such as market size, the degree of trust, and the availability of third-party enforcers, strongly influences the availability and effectiveness of governance mechanisms (Williamson, 1996). When self-governance becomes less effective, third-party governance comes into play (Barzel, 2002; Leeson, 2014a). In contrast, firms are structured hierarchically. Their organisational structure is typically characterised by a division of labour and a centralised chain of command that guides and coordinates member interactions. Moreover, firms are typically more capable of investing resources into the development of formal rules and designating coordinators to provide further coordination, adaptation, and dispute resolution according to the established rules. Consequently, governance systems within firms typically gravitate towards third-party governance. The hierarchical structure and pre-existing formal rules frequently limit the feasibility of self-governance.

1.5 Criminals and Extra-legal Governance

In criminal settings, actors cannot rely on the state to provide governance to protect their property rights and resolve disputes due to the illicit nature of their activities. Private governance is their only choice. Given that the governance systems created by criminals are not tolerated by the state, scholars commonly denote them as ‘extra-legal governance’ (Wang, 2017; Hamill, 2010; Gambetta, 1996; Catino, 2019; Varese, 2001). Extra-legal governance, as a type of private governance, shares similar features with legally developed governance systems. Both self-governance and third-party governance have been discovered in criminal settings.

Self-governance, on the one hand, has been found in several illicit markets. For instance, Symkovych's study on Ukrainian prisons (2018), Lesson's study on pirates (2014b), and Shortland's study on the kidnap market (2017) have found the existence of self-governance. In the case of Ukrainian prisons, Symkovych (2018) found that prisoners' interaction is regulated by a self-governed normative system. Criminal behaviours are regulated by a series of norms – the convict code. The convict code includes a set of behavioural principles that ensures social order within the prison, such as no informing, no stealing, and adhering to the prison hierarchy. The norms are peer-monitored and enforced by the prison community. Violators of the norms are isolated, downgraded in social status, and punished by beating. Strategies to enhance the power of self-enforcement are also found among criminals. For example, mafia members and gang members often are tattooed on visible parts of their bodies to demonstrate their high level of commitment (Catino, 2019; Skarbek, 2014; Gambetta, 2009). Moreover, Gambetta (2009) finds that the hostage is commonly used by criminals as a tool to ensure cooperation and prevent defection. On many occasions, information is used as a hostage instead of a human, as having evidence of a crime is often enough to prevent the other criminal from committing betrayal. A typical example of an information hostage is the mafia tradition of asking a new member to commit murder (Gambetta, 2009).

On the other hand, third-party governance in the criminal world is also not uncommon. Some markets, such as prostitution, gambling, and drugs, are often protected and governed by organised crime groups such as the Mafia (Gambetta, 1996; Wang, 2017; Varese, 2001; Kaplan & Dubro, 1986; Catino, 2019). Mafia groups are perhaps the most famous organised crime group, and specialise in supplying governance services (Gambetta, 1996; Varese, 2001). Mafia groups protect both legal markets that are not well-governed by the state government and illegal markets, such as drugs, gambling, and prostitution markets.

By acting as a state-like organisation, mafia groups collect ‘tax’ (protection money) in exchange for their governance services in their territories, such as enforcing agreements and settling disputes between the governed (Gambetta, 1996; Varese, 2001; Shortland, 2019). ‘Territory’ under mafia governance can also be a specific type of market, where multiple groups operate within the same geographical area. One example is the carting market, which was monopolised by only one of the mafia families in New York City (Varese, 2001). Moreover, the Mafia also protects criminal businesses from external threats, such as their rivals, their competitors, and sometimes even their customers. For instance, the gambling and prostitution industries often face trouble from customers unwilling to pay, while the business of drug distribution is prone to harassment from competitors (Chu, 2002; Catino, 2019).

Nevertheless, hybrid situations exist, and the governance of markets can shift from self-governance to third-party governance (Hamill, 2010; Skarbek, 2012; Lessing, 2021). In Californian prisons, for example, Skarbek (2012) discovered that inmates who at first relied on a self-governance system turned to a third-party governance system due to a dramatic increase in the prison population and ethnic diversity. As in legal settings, large-size communities face the information transmission challenge. When information about violations cannot be easily communicated to the community, communal punishment is difficult to enforce, and the self-governance system becomes less effective (Leeson, 2014a; Stringham, 2015; Landa, 1981; Ostrom, 1990). In this circumstance, as Barzel (2012) predicted, a third-party governance system becomes more attractive.

The economic concept of firms is also applied by scholars to understand criminal enterprises and their governance structure (Schelling, 1967; Reuter, 1983; von Lampe, 2015; Morselli et al., 2007; Lusthaus et al., 2022). Criminal firms have been defined as "delineable organisational entities that are roughly similar in function to organisations in

the legal economy, commonly referred to as businesses, business enterprises, enterprises, corporations, or firms" (von Lampe, 2015, p.127). Nevertheless, since they operate outside of the law and constantly face the threat of state repression, their organisational structure can be less formal compared to that of legal firms (Moreselli et al., 2007; Reuter, 1983). For the same reason, criminal firms also tend to have a smaller size and a shorter lifespan (Reuter, 1983). Building on existing literature, Lusthaus et al. (2022) proposed that the distinction between criminal firms and markets should hinge on the presence of a division of labour. For instance, when a criminal group consists of entrepreneurs, managers, employees, and temporary workers, it can be classified as a criminal firm. Overall, academic discussion on criminal firms appears to suggest that such a concept should be more inclusive, encompassing those criminal organisations that are structurally unstable, have less defined internal divisions of labour, and are situated on the defining boundary.

Criminal firms may take various measures to consolidate their internal governance. Studies show that criminal organisations often invest heavily in their recruitment process to screen out disloyal members (Pizzini-Gambetta & Hamill, 2011; Skarbek, 2014; Kostelnik & Skarbek, 2013). Recruiting members via ethnic ties is the most common strategy. The Sicilian mafia, for instance, requires their made members to be Sicilian (Gambetta, 1996). Similarly, some criminal firms choose to recruit members locally (Pizzini-Gambetta & Hamill, 2011; Varese, 2011). By leveraging ethnic and local ties during the recruitment process, criminal organisations can gather more information and knowledge about their members. This, in turn, facilitates easier punishment of both the members and their families in the event of defection. Accordingly, Campana and Varese (2013) liken local recruitment to a form of hostage-taking.

Criminal organisations may also invest in binding processes to reinforce the members' loyalty and foster alignment between the individual motivation and the collective interests

of the criminal organisations (Jankowski, 1991; Catino, 2019; Wang, 2017). A binding process forms bonds among the members of the criminal firms, which subsequently discourages opportunistic behaviour and strengthens the social order inside the firms (Catino, 2019; Jankowski, 1991). Catino (2019) pointed out that the more successful a binding process is conducted within a criminal organisation, the less necessary it is for the organisation to control its members. Similar to American street gangs, many cybercriminal firms establish a set of collective values and beliefs as a part of their binding process to solidify the group (Jankowski, 1991).

Moreover, criminal organisations may employ the strategy of compartmentation to control the information flow (Kostelnik & Skarbek, 2013; Catino, 2019). In essence, compartmentation is "based on the breaking down of information by allocating knowledge, and the activities related to it, to various units, individuals and/or organisations, making it difficult for one subject, whether internal or external, to form an idea of the picture as a whole" (Catino, 2019, p.268). This strategy is commonly used by drug-trafficking and terrorist groups (Kenney, 2007; Hofmann & Gallupe, 2015; Catino, 2019).

Furthermore, certain criminal organisations require demonstrable signs such as tattoos. For example, many members of the Yakuza bear large-scale tattoos applied via a traditional Japanese method that involves hand-pricking the skin with a cluster of ink-dipped needles (Hill, 2003). These markings generate a strong signal of the individual's dedication to the group. As Gambetta (2009, p.41) noted: "An effect of having highly visible tattoos is to make it more difficult for anyone to renounce a life of crime or, if the tattoo is gang-specific or business-specific, to switch from gang to gang or change one's business".

Finally, criminal organisations also create rules and establish a range of punishments to regulate members' behaviours. Punishments can span a wide spectrum, ranging from financial penalties and expulsion to physical harm. In extreme cases, these punishments

may escalate to the point of taking a member's life (Skarbek, 2014; Hamill, 2010; Leeson, 2014a; Catino, 2019; Gambetta, 1996; Varese, 2001; Lusthaus, 2018).

1.6 Extra-legal Governance and the State

Ultimately, criminals are defined by the state. The state illegalises certain activities and refuses to protect the property rights emerging from them. Extra-legal governance established by criminals, therefore, covers the domain where legal rights are denied by the state. In this sense, extra-legal governance cannot exist without the state's existence (Barzel, 2002; Lessing, 2021).

Unlike the rebels and insurgent groups that bare political ideologies to overrule state governance, criminals often do not intend to establish exclusive control over any territory. Instead, their governance usually overlaps with state governance. Criminals also often rely on state governance to provide services like health and education (Lessing, 2021). Thus, as the state has an interest in tackling criminals, criminals must seek protection from the outside to consolidate their governance.

Many criminals seek protection by corrupting state agents. State agents may turn a blind eye or actively provide protection to criminals in exchange for direct monetary gains or their services, such as fundraising, voting, or policing (Chin, 2009; Catino, 2019; Shortland, 2019; Jankowski, 1991). For instance, Ames (1981, p.107) pointed out that "police and politicians have used gangsters through Japan's modern history to help maintain social order, especially to counterbalance the burgeoning strength of lefties". Similarly, Wang (2017) found that it is essential for mafia bosses in China to build a good relationship with government officials in order to ensure their governance over the criminal world, as "it is impossible for local gangs to have a long-term existence if they fail to create links with government officials, especially those from the criminal justice system" (Wang, 2017,

p.168). In countries where state power is eroding due to economic transitions or political conflicts, alternative sources of protection might be provided by entities such as rebels, insurgent groups, or organised crime groups, such as the Mafia (Wang, 2017; Magaloni et al., 2020; Shortland, 2019; Varese, 2001; Chin, 2009). For example, in researching the drug industry in Myanmar, Chin (2009) found that at the core of this thriving industry is the protection and support given by the local authorities. He claimed:

> [I]t is true that many poor farmers must rely on poppy or coca plants to survive, but the deeply embedded political conflicts provide a social and political context for drug production because the people in power, be they the ruling authorities or the insurgent groups, often rely on drug money to achieve their political goals (Chin, 2009, p.237).

Overall, as Lessing (2021, p.868) argues, state governance and criminal governance are in a symbiotic relationship which "imply[ies] entanglement, a growing together, and mutual dependence that may deepen over". As a result, the analysis of extra-legal governance created by criminals must not overlook its relationship with the state.

2. Cybercriminal Governance

Cybercriminals often cooperate with their partners online. Cooperating online means the parties may reside in different physical locations and are less likely to receive physical retaliation from their partners even if they betray them. Cooperating online also entails anonymity. While ordinary criminals inevitably have to reveal certain information about themselves (e.g. their face, voice and perhaps ethnicity) during cooperation, cybercriminals do not. Instead, cybercriminals often use nicknames and IDs to represent their online identities, and these identities can be abandoned and easily replaced (Lusthaus, 2018; Dupont et al., 2016). Consequently, the deterring effect of potential punishment is

substantially weakened, and the likelihood of experiencing betrayal from a partner significantly increases for cybercriminals. For example, in Lusthaus's study (2018, p.141), a former cybercriminal explicitly expressed that he would scam others when the risks of being caught were low. Moreover, because defection happens so often online, some cybercriminals even perceive it as a necessary cost of doing business (Lusthaus, 2018, p.165).

While engaging with partners who might potentially defect is already challenging enough, the presence of law enforcement actions adds an extra layer of difficulty for cybercriminals. A number of studies suggest that undercover agents exist in many online underground markets (Kuzmin, 2012; Lusthaus, 2018; Yip et al., 2013). There are also stories of undercover operations that lead to the apprehension of cybercriminals (Kuzmin, 2012). Distinguishing potential undercover agents from bona fide criminal partners, therefore, forms another challenge for this criminal group. Furthermore, Dupont (2013) found that there is a short supply of diplomatic skills among cybercriminals, which imposes another threat to cooperation. Dupont found that random acts of aggression, such as quarrels and DDoS attacks against other community members fuelled by touchiness and boredom frequently happen in a cybercriminal community, making trust relationships among community members extremely fragile.

Yet the flourishing of illicit online marketplaces and the wide presence of cybercriminal groups all over the world suggest that cybercriminals have found ways to overcome these difficulties (Haslebacher et al., 2017; Chu et al., 2010; Bancroft & Reid, 2016; Rhumorbarbe et al., 2016; Hutchings, 2014). As in conventional criminal cooperation, extra-legal governance plays a crucial role (Lusthaus, 2018; Leukfeldt & Kleemans, 2017; Holt et al., 2016; Wehinger, 2011).

Recent research on cybercrime has revealed that self-governance largely exists online (Blundell et al., 2004; Dupont & Lusthaus, 2022; Lusthaus, 2018). A simple way to self-enforced agreement is by the 'discipline of continuous dealing'. Cybercriminals can simply refuse to collaborate with wrongdoers. In online marketplaces, cybercriminals may also make use of the reputation mechanism (Krylova, 2019; Lusthaus, 2018; Leukfeldt & Kleemans, 2017; Holt et al., 2016; Wehinger, 2011). As Dupnot and Lusthaus (2022) pointed out, online marketplaces amplify the scope of the reputation mechanism, enabling the broader dissemination of information. The accessibility of information on these online platforms therefore allows the reputation mechanism to function on a larger scale as opposed to just within limited networks. Cybercriminals can disseminate information about wrongdoing in forums, leading to communal punishment executed by the entire community, such as social isolation and ostracism. Some marketplaces also have a review system, where members who have purchased products from vendors can leave a written review or a score on a rating scale to assess the vendor (Van Wegberg et al., 2018; Yip et al., 2013). In online marketplaces, reputation is the foundation for entering an online market and doing business with other criminals. Cybercriminals have to accumulate their reputation and reach certain ranks in order to access certain resources. Dealing with a person who has a good reputation in the marketplace is always preferable for cybercriminals. Reputation is linked to nicknames, as the "only thing that should be known to cybercriminals about a person with whom they are doing business is his or her nickname" (Lusthaus, 2018, p.96). Therefore, cybercriminals need to carefully operate their nicknames as brands. Although there is often a lack of physical enforcement in online cooperation, the economic consequence of losing reputation is severe.

In addition to the 'soft punishments', cybercriminals may also take further aggressive actions such as 'doxing' and 'swatting' to punish wrongdoers as a substitution for physical

retaliation. The former involves revealing personal information about the targeted cybercriminal, and the latter involves making a call to emergency services, thereby triggering the dispatch of a tactical police squad to the suspect's location under the pretence of an ongoing violent crime (Lusthaus, 2018, pp.130–131). Distributed denial-of-service (DDoS) attacks may also be used by cybercriminals against defectors as an even more direct punitive measure (Dupont, 2013). However, to execute these actions, the attacker often needs to have good social engineering and/or technical skills. To compensate for any lack of technical skill, cybercriminals may ask their collaborators to provide personal information beforehand. When one's real identity is revealed, the protection of anonymity ceases. Gambetta (2009) raised the concept of the 'information hostage' and claimed that "just showing one's face is itself like giving a hostage" in cyberspace (Gambetta, 2009, p.63). Two paedophile cyberspace rings studied by Gambetta (2009) provide an example of this concept. In order to join the groups, criminals have to upload at least ten thousand photographs as evidence of their crimes. Sometimes members are also required to meet with the administrators in person or upload their own pictures and videos.

Alongside self-governance, third-party governance also holds a crucial position. Administrators are appointed in many online marketplaces to create rules, maintain business order, and resolve disputes. In fact, most marketplaces have their own enforcement boards that establish market regulations and administer penalties, such as expulsion (Bhaskar et al., 2019; Collier et al., 2021; Dupont & Lusthaus, 2022; Lusthaus, 2018; Yip et al., 2013). Some marketplaces are also divided into multiple layers by the administrators. To access the middle and bottom layers, members often need to be vetted or approved by the administrators by providing proof of their honesty (Lusthaus, 2019). Additionally, administrators may offer escrow services to facilitate the process of business

transactions. In this case, the administrators act as a guarantor and hold the money until the buyer receives the products (Broadhead, 2018; Leukfeldt et al., 2020; Lusthaus, 2018).

Nevertheless, despite the presence of self-governance and third-party governance online, defection still happens often due to the structural limitations of the online governance system. For instance, the effectiveness of the online reputation mechanism can be impeded by fake reports and ratings. Moreover, despite the associated expenses, online identities that are considered untrustworthy can still be discarded and replaced with fresh, untarnished profiles (Dupont et al., 2016). Furthermore, online marketplace operators and administrators are also anonymous. They may decide to abruptly close the marketplaces and flee with the funds held in escrow for orders that remain unfulfilled. This is known as an 'exit scam', and it is not uncommon in the cybercrime world (Bhaskar et al., 2019; Hou, 2021). After all, virtual enforcement is so weak that even the most stringent online enforcement strategies fall short when compared to offline physical punishment, as Lusthaus held (2018, p.137): "old nicknames can be shed and new identities built. But death is final".

As a result, it is unsurprising to see many cybercriminals choosing to cooperate with each other offline. By cooperating offline, the challenges posed by the Internet and anonymity are mitigated, and conventional strategies to achieve governance can be adopted (Lusthaus, 2018; Leukfeldt, 2014, 2015; Lusthaus & Varese, 2021). An example of offline cooperation among cybercriminals can be found in Leukfeldt's (2014) study. Leukfeldt found that cooperation among cybercriminals in Amsterdam has a strong offline component: the criminals become acquainted through previous social ties, and most meetings and recruitments take place on the street. A similar case was found in Râmnicu Vâlcea – the Hackerville in Romania (Lusthaus, 2018). In Râmnicu Vâlcea, a range of highly structured cybercriminal firms existed. Within these firms, many members

maintained personal connections. These individuals frequently convened in person, establishing a sense of community. Moreover, studies have highlighted that even among cybercriminals who ostensibly collaborate predominantly online, offline relationships are prevalent among the central members (Dupont & Lusthaus, 2022; Leukfeldt, Lavorgna & Kleemans, 2017; Lusthaus, 2019). In the aforementioned cases of offline cooperation, traditional governance strategies are heavily employed. Thus, the level of violence associated with cybercrime can exceed common perceptions.

3. The Case of China

Today, China has become one of the biggest cybercrime hotspots in the world. According to Xinhua (2022), the Chinese police apprehended a total of 103,000 individuals suspected of participating in cybercrime in 2021. Over 27,000 online businesses and institutions were involved. The police also successfully dismantled more than 6,000 cybercriminal groups that conducted a variety of cybercrime, including fraud, hacking and money laundering. In line with these newspaper articles and reports, existing academic works on Chinese cybercrime also reveal that large-scale underground cybercrime markets and cybercriminal groups exist in China (Kshetri, 2013; Nguyen & Luong, 2021; Yip, 2011).

However, China is by no means the best place for cybercrime operations. The internet environment in China is rather extreme compared to the rest of the world. First, the freedom to access information online is constrained. To regulate the use of the Internet, the ‘Great Firewall’ project was started in 1998, which shaped the Chinese internet infrastructure (Stevenson, 2007; Liang & Lu, 2010). According to the ‘Great Firewall’ project, only agencies and businesses that have been approved by the government are allowed to establish a ‘backbone network’ and license the operation of Internet service providers (ISPs)

at the next tier. Also, all ISPs are required to install filters to block unwanted content, such as foreign internet tools (e.g. Google, YouTube, Facebook etc.) and mobile apps (e.g. WhatsApp, LINE). Moreover, as a part of the 'Great Firewall' project, the 'Golden Shield' project has been set up to monitor internet information on both national and international levels. The Chinese government also puts pressure on businesses by publishing regulations about self-censorship. Companies are held liable for harbouring illegal content and may face severe financial penalties (Walton, 2001). However, the line between legal and illegal content is not well defined by Chinese law and varies from time to time. Therefore, to minimise the risk of receiving potential penalties, self-censorship conducted by businesses is often stricter than the actual requirement (Liang & Lu, 2010). The restrictions on accessing international websites, including online illicit marketplaces, pose obstacles for Chinese cybercriminals trying to learn new crime techniques from foreign collaborators. They also reduce the range of potential partners they can work with. The hindered access to online illicit marketplaces might complicate the trading of products or services between Chinese and foreign cybercriminals. In a similar vein, the restricted use of foreign mobile apps, such as Telegram and WhatsApp, could obstruct seamless communication between the Chinese and their foreign counterparts.

Second, there is intensive internet surveillance in China (Lee & Liu, 2012). Since 2012, comprehensive online real-name registration rules have been implemented, which eliminate cyberspace anonymity to a large extent (Lee & Liu, 2016). Under the rules, internet users are required to disclose their online identity by binding all online accounts with a national ID number and/or mobile phone number (which is also required to be bound with the national ID number). A special internet police force has also been established to assist with internet surveillance in China. Although the exact number of internet police has never been announced by the government, it was estimated to be over two million in 2013

(Li, 2015). While few studies suggest that online censorship and surveillance focus mainly on political discourses (Wang et al., 2016; Stockmann & Luo, 2019), police apprehension due to illicit online behaviours are not uncommon. For instance, a man was arrested and given public security penalties[2] by the police due to his unauthorised use of virtual private network (VPN) services in 2020 (Jingshi Police, 2020). In another case, a man was arrested and consequently sentenced to five years' imprisonment for providing illegal VPN services to others (Haas, 2017). The implementation of the real-name registration system and the intensive online surveillance create substantial difficulties for cybercriminals wanting to collaborate on local online platforms.

Using VPNs could potentially offer a solution to the above two problems, as they not only allow users to access foreign websites but also conceal their real IP addresses. Nevertheless, intensive online surveillance in China introduces notable hurdles. As provided above, since the unauthorised use of VPNs is illicit in China, the government has been cracking down on not only the VPN users but the VPN providers. On the other hand, VPN providers approved by the government are likely to be subject to monitoring. Therefore, it is challenging for Chinese cybercriminals to locate and sustain access to a reliable VPN service. Furthermore, the employment of VPNs does not ensure the security of cybercriminal activities. Through technical measures, VPN traffic can also be detected by the police, especially for VPNs that have weaker encryption or security protocols. Thus, activities may still be tracked even when VPNs are in use (Aravind et al., 2023; Miller et al., 2018).

Finally, Taneja and Wu's study (2014) shows that alongside the 'Great Firewall' project, cultural factors such as a lack of English skills and virtual habits also lead to a rather

[2] Public security penalties are a form of administrative punishment imposed by the police for violations of regulations that maintain public order that are not severe enough to warrant criminal charge. Public security penalties do not involve judicial proceedings and are typically handled by police at their discretion. They can range from warnings and fines to detentions, depending on the severity and nature of the violation.

isolated internet environment in China. Even if the technical hurdles are crossed, the cultural and language barriers constitute another complexity for international cybercriminal cooperation. As several studies suggest, cooperation among Chinese cybercriminals predominantly remains within the boundaries of their nationality (Kshetri, 2013; Yip, 2011).

On the whole, cybercrime operation in China is characterised by internet isolation, intensive online surveillance, and strong government repression. Operating in such an extreme internet environment, the extra-legal governance system built by Chinese cybercriminals must react accordingly to adapt. Three distinct features may be expected. Firstly, since Chinese cybercriminals tend to cooperate with individuals of the same nationality, the size of the cybercriminal community could be smaller. There are also fewer cultural variations. Therefore, reputation mechanisms and self-governance could potentially be more effective among Chinese cybercriminals compared to those operating internationally (Leeson, 2014a; Stringham, 2015; Landa, 1981; Skarbek, 2012; Ostrom, 1990). Secondly, because of the challenges in cooperating online, offline cooperation may be preferred by Chinese cybercriminals. Thus, traditional governance strategies employed by conventional criminals could be more often found. Thirdly, to deal with online surveillance and potential apprehension, cybercriminals in China may actively seek protection to safeguard their operation.

One source of protection could be corrupt state agents in China through the use of *guanxi* practice. For Wang (2017), the practice of *guanxi* in China has a strong connection to protection. *Guanxi* (literally meaning 'relation'), a Chinese version of social capital, is defined as "a unique type of relationship or a behavioural pattern deeply rooted in Chinese history and culture, where 'particularistic ties' have long been used for an instrumental purpose" (Chang, 2011, p.315). In China, regardless of the wills of individuals, everyone

lives within a *guanxi* network (Fei et al., 1992). *Guanxi* relationships can be established in two ways: via blood relationships and through social interconnection (Tsang, 1998). While the former indicates the family tie, the latter covers a wide range of social relationships such as friend, neighbour, classmate and alumnus. What makes the *guanxi* relationship special is the implied exchange of intelligence and favours among the members of the network (Luo, 1997). Under the influence of the long-term practice of relying on this informal institution in China, individuals within the *guanxi* network often find themselves obliged to show favouritism. Abstaining from favouritism often leads to a loss of reputation within the network and potential future benefits from the informal favour exchange (Wong & Chan, 1999; Luo, 1997). The consequences of this can be crucial. As Wang (2017) notices, the non-transparent nature of the legislation and enforcement process in China creates a dependency for individuals to rely on the *guanxi* network to obtain information and get things done. Also, because of the existing gap between the law on paper and the law in action, and unequal protection between public property rights and private property rights, this informal institution still retains its importance in modern Chinese society. Luo (1997, p.43) even argues that "no company can go far unless it has extensive *guanxi* in its setting".

Due to its practice of favouritism, *guanxi* practice is often associated with corruption and the flourishing of criminal activities. Through the *guanxi* practice, government officials can act as protectors who safeguard the underworld (Luo, 2008; Wang, 2017; Varese, 2011). For example, gang bosses often develop *guanxi* with local police to avoid criminal investigation and punishment. Wang's (2017) case studies on the success of some notorious gangs in Chongqing show the importance of building a politico-criminal *guanxi* network in criminal cooperation. In small towns, kinship ties are mostly used by criminals to build *guanxi* networks with police, whereas in big cities, *guanxi* is often established by

identifying common social identities and a common third party. Wang (2017) demonstrates a typical *guanxi* network-building process used by criminals:

> A gang boss would identify the police officer who took charge of a criminal case his gang members were involved in, and get familiar with that officer by finding mutual friends and common experience. (p.160)

Once the relationship is initiated, various forms of bribes are sent to the police officer on traditional gift-giving occasions and when money is most needed. Because of the special occasion, and sometimes due to the presence of middlemen (people in the police officer's *guanxi* network), the police officer often finds it difficult to reject the bribe as part of the *guanxi* practice. Starting with the building of *guanxi* with one person, gang bosses are then able to extend their *guanxi* network using the person as a middleman and infiltrate the police system (Wang, 2017).

Few studies have been conducted on Chinese cybercrime, despite China being one of the biggest cybercrime hotspots in the world. Some existing studies appear to be outdated. For example, Lusthaus's work (2018) found that there were only low-level cybercrime cases in China and that most of them were related to IP infringement. This finding does not seem to accurately represent the cybercrime landscape in China today, taking into account the size and economic consequences of these crimes. Other studies contain limited detail and capture only a fraction of Chinese cybercriminal activity. In particular, most of them focus purely on the online marketplace (Cai et al., 2018; Kshetri, 2013; Yip, 2011). The most recent study conducted by Nguyen and Luong (2021) constitutes the first in-depth exploration of Chinese cybercriminal networks associated with transnational cyber fraud. Still, their research does not primarily concentrate on the subject of extra-legal governance.

Overall, there has been a lack of comprehensive research within China concerning the dynamics of cooperation and extra-legal governance among Chinese cybercriminals. This

thesis represents a pioneering, large-scale empirical study to bridge this knowledge gap. By probing into how Chinese cybercrime cooperation functions within such an extreme internet environment, this investigation seeks to expand our understanding of governance and cooperation.

4. Research Questions and Research Scope

Drawing from the theoretical frameworks on governance, the empirical body of work on cybercrime and its governance, and the particularly unique and extreme case of Chinese cybercrime – a topic that has not yet been thoroughly investigated – the principal research question for this study is thus formulated: *How is the cybercrime industry governed in China?*

In order to empirically address this central research question, it is vital to first sketch an accurate portrayal of the modern cybercrime landscape in China. This involves discerning the types of cybercrime prevalent in China, determining potential interconnections amongst various cybercrimes, and elucidating the forms of cooperation among cybercriminals. As such, to pave the way towards our core research question, I pose an initial specific research question: *How is the landscape of cybercrime in China characterised?*

Upon addressing the initial question, I will delve further to understand how the cybercrime industry is governed. The second specific research query is subsequently formulated: *How are the collaborative interactions among Chinese cybercriminals governed?* To respond comprehensively to this query, cooperation amongst Chinese cybercriminals in both online and offline dimensions will be examined.

In a challenging environment, criminal activities face constant external threats from the predatory behaviours of rivals and threats of state repression. It seems critical for these

operations to reach out for protection to ensure their survival. The question of who these potential protectors might be, along with their respective roles, merits further investigation to understand the whole picture. Thus, the final specific research question is as follows: *Who are the protectors of Chinese cybercriminals, and how do they accomplish this protection?*

By answering the research question, this empirical study offers valuable insights into Chinese cybercrime. It provides a comprehensive picture of Chinese cybercrime and examines how cooperation is archived by Chinese cybercriminals who operate largely outside of the state's control and legal infrastructure. It also uncovers how cybercriminal economics can function in an extreme environment, which has, until now, been largely unexplored. In addition to providing these innovative empirical findings, this study also contributes substantively to broader sociological and criminological discourses on cooperation. It sheds light on the significant impact of anonymity – a key characteristic of online interactions – on the traditional models of cooperation. By probing these elements, this study helps to bridge the gap between conventional sociological theories of cooperation and the new realities introduced by digital technologies. It lays the groundwork for future research in this area, promising a more comprehensive understanding of cybercrime and its implications for both law enforcement and policymaking.

It should be noted that the research aims to study only cybercrimes that are economically driven. Therefore, cybercrimes with political motivations, such as cyberattacks that are performed by state actors or groups that are sponsored by a certain state are outside of the scope of current research. Moreover, as it will be made clear in the following chapters, cyber fraud lies at the core of the country's profit-driven cybercriminal activities and the cybercrime industry in China is essentially built around cyber fraud. There are, of course, other types of cybercrimes that are unrelated to the business of cyber fraud, but they do not

seem to reach the same industrial scale as cyber fraud. Thus, the subject of this study is concentrated on the industry of cyber fraud in China, and I use the term ‘cybercriminal’ to refer to the actors within this industry.

5. Thesis Outline

After outlining the methodology and data collection processes utilised in this dissertation, Chapters 3 and 4 endeavour to address the first specific research question. Chapter 3 offers an overview of the cybercrime landscape in China, highlighting that the nation's cybercrime sector is predominantly centred around cyber fraud. This chapter elucidates a range of criminal activities, including scam promotion, communication transmission support, and money laundering, all of which underpin the seamless operation of cyber fraud. In essence, the chapter posits that the realm of cybercrime is fundamentally an industry of cyber fraud. It then delves into the most common scams found in China and debates both the emergence of such a robust cyber fraud industry in the country and the reasons why its internet infrastructure doesn't deter cybercriminal activity. Chapter 4 shifts its focus to the subjects being governed – the participants within the cyber fraud industry. By amalgamating statistical data sourced from court judgments with insights from interviews, this chapter paints a comprehensive picture of the individuals operating within the realm of cyber fraud. In summary, while many of these actors lack advanced IT skills, they are nonetheless professional criminals, each honing a distinct area of specialisation.

Using the economic concepts of markets and firms, Chapters 5 and 6 answer the second specific research question by examining the two forms of criminal cooperation respectively. Chapter 5 reviews the market structure in both online and offline domains and discusses

how governance is achieved in these two realms. It analyses how cybercriminals utilise the reputation mechanism, hostage-taking, norms, and communal punishment to self-regulate the market. Additionally, the chapter discusses the role of third parties in creating and maintaining rules and enforcing agreements in the criminal market. Chapter 6 probes the structure of cybercriminal firms in China and examines the various strategies these firms adopt to ensure internal governance. It also discusses the relationship between cybercriminal firms and other external actors, suggesting that cybercriminal firms tend to be less predatory than traditional criminal organisations.

Before drawing a conclusion, Chapter 7 addresses the third specific research question. It centres on traditional protectors, as identified by existing research – namely organised crime groups, corrupt government agents, and local armed groups within criminal industries. The chapter examines their potential role in governing the Chinese cyber fraud industry. It reveals that organised crime groups have limited involvement as protectors within the cybercrime industry. However, cybercriminals actively seek protection from state agents to reduce the risk of apprehension. Furthermore, should local protectors withdraw their protection, cybercriminals may even relocate overseas to seek protection from foreign entities.

Chapter 2. Research Methodology

This chapter outlines the research design of this project and the key methods and data used. It first explains the general research approach. This is followed by an overview of the data included in this study. Next, it explains the detailed data collection process. This includes issues such as sampling, access, and obstacles that I had to overcome while carrying out this research project. The final section examines the ethical issues and limitations of this research.

1. General Research Approach

The purpose of this research is to investigate how the Chinese cyber fraud industry is governed. This is a topic that has not been widely covered by academics, and therefore little is known about it. Also, due to the sensitivity of the research topic in China, there is a lack of comprehensive and reliable public datasets. Because of the above two reasons, a strongly quantitative approach is not possible. Moreover, a qualitative research design is believed to be appropriate for studying hidden populations, causal relationships and micro-level and meso-level processes. The qualitative method has also been the dominant approach used by scholars studying extra-legal governance (Hamill, 2010; Wang, 2017; Chu, 2002; Gambetta, 1996; Varese, 2001; Hill, 2003) There are several successful examples of qualitative research on cybercriminal cooperation (Collier et al., 2021; E. R. Leukfeldt, 2014; Lusthaus, 2018; Yip et al., 2013).

This study takes the exploratory approach adopted in Lusthaus's (2018) study on global cybercrime. This approach sits well between the deductive approach that conducts qualitative hypothesis testing and the inductive approach that conventionally employs ethnography to build theoretical suppositions. The study starts with a clear set of research

questions that links to a sociological puzzle and has theoretical roots in governance. It then draws on novel and extensive data collection on Chinese cybercrime to explore this puzzle. While hypothesis testing is not engaged in this research, clear research questions are provided. Specific hypotheses cannot be generated as too little is known about Chinese cybercrime at this point. But, following the exploratory work in this study, one goal of this research is to develop testable hypotheses for future deductive studies.

To capture as many cybercriminal activities as possible, this study uses both primary and secondary data, collected online and offline. It relies on interview data and secondary data such as newspaper articles, articles published by law enforcement agencies, private cybersecurity firm reports, official documents from law enforcement agencies and prosecutors, and judgments from the courts. For sensitive topics such as the questions embedded in this research, qualitative research that comprises individual interviews can be used to build rapport with participants, which may reveal sensitive and hidden information (Hennink, et al., 2020). This information is then compared and supplemented by secondary data to demonstrate a comprehensive picture of the phenomenon. Some degrees of triangulation are also achieved during this process, which improve the reliability of the evidence (Hennink, et al., 2020). The next section will provide detail about the data composition of this study.

2. Data Composition

The data used in this research consists of both primary data and secondary data. This section provides a general description of the data being collected. The detailed collection process will be demonstrated in the following subsection.

2.1 Primary data

The majority component of the study is the interview data. These were collected during three years of fieldwork in different regions of China between 2020 and 2022 (with two exceptions: two of the interviewees resided in the US). In total, 66 semi-structured interviews were conducted. Most of them were conducted in person (N=51), and some of them were conducted via phone calls or online chatting software (N=15). Overall, participants were generally reluctant to participate remotely (via phone and online interviews). This could be due to the sensitivity of the topic and the possible monitoring of their communications. They might also feel less in control of the interview (e.g. if the conversation was recorded) this way. Thus, the face-to-face interview was the primary interview method. The average interview time was 59 minutes. The shortest interview lasted about 15 minutes, and the longest one lasted about 150 minutes. Most of the calculation of interview time is an estimation, with a few minutes of deviation. This is because the majority of these interviews were not recorded (N=49). This is mainly due to the sensitivity of the topic. More details on this issue will be addressed in the later sections.

The interview participants involve five main groups of people: law enforcement officers, practitioners in the cybersecurity sector, prosecutors, former cybercriminals, and people who are related to cybercrime but difficult to define. The last group of participants includes two businessmen who have been to some of the cyber fraud hubs and "almost got involved in cybercrime" (GD-R-1, SC-R-1) and a graduate who was accidentally recruited into a cyber fraud group (SX-R-1). The category boundaries are not strictly defined, as some interviewees cross them, and have multiple identities: for example, some practitioners work closely with law enforcement agencies and participate in cybercrime crackdown activities. The general approach is to interview participants from different backgrounds that are

related to cybercrime rather than focus on one single group of participants. This approach helps to achieve triangulation and reduce potential bias.

Below, Table 1 provides a list of interview subjects. Key information about the interviewees is provided. In the case when multiple identities were presented, I labelled the participants according to their main connection to the topic. Moreover, to better protect the anonymity of the interviewees, only the province of the participants is provided. The participants are the main information source about Chinese cybercrime. They understand the phenomenon from different perspectives. Comparing and piecing together their views provide the research with a comprehensive picture of the area of study.

Table 1 : List of Interview Subjects

No	Alias	Code	Category	Province	Time (mins)	Type	Year
1	Haodong	BJ-CSP-1	Cyber Security Practitioner	Beijing	30	Phone/Online	2020
2	Xinyu	GD-CSP-1	Cyber Security Practitioner	Guangdong	40	In Person	2020
3	Ningxin	GD-CSP-2	Cyber Security Practitioner	Guangdong	30	In Person	2020
4	Xiangwei	GD-CSP-3	Cyber Security Practitioner	Guangdong	30	In Person	2020
5	Zui	GD-P-1	Law Enforcement Agent	Guangdong	30	In Person	2020
6	Zhimei	GD-P-10	Law Enforcement Agent	Guangdong	150	In Person	2020
7	Zhaojun	GD-P-11	Law Enforcement Agent	Guangdong	60	In Person	2020
8	Peilan	GD-P-12	Law Enforcement Agent	Guangdong	60	In Person	2020

9	Shengjing	GD-P-13	Law Enforcement Agent	Guangdong	120	In Person	2020
10	Haochu	GD-P-14	Law Enforcement Agent	Guangdong	60	In Person	2020
11	Xiude	GD-CSP-4	Cyber Security Practitioner	Guangdong	30	In Person	2020
12	Xingan	GD-P-17	Law Enforcement Agent	Guangdong	150	In Person	2020
13	Qingjie	GD-P-18	Law Enforcement Agent	Guangdong	150	In Person	2020
14	Zen	GD-P-16	Law Enforcement Agent	Guangdong	20	Phone/Online	2020
15	Yanfang	GD-P-2	Law Enforcement Agent	Guangdong	40	In Person	2020
16	Yueyi	GD-P-3	Law Enforcement Agent	Guangdong	40	In Person	2020
17	Ruimin	GD-P-4	Law Enforcement Agent	Guangdong	60	In Person	2020
18	Daihui	GD-P-5	Law Enforcement Agent	Guangdong	80	In Person	2020
19	Yinghua	GD-P-6	Law Enforcement Agent	Guangdong	30	In Person	2020
20	Anni	GD-P-7	Law Enforcement Agent	Guangdong	30	In Person	2020
21	Yi	GD-P-8	Law Enforcement Agent	Guangdong	25	Phone/Online	2020
22	Jinghuai	GD-P-9	Law Enforcement Agent	Guangdong	150	In Person	2020
23	PengPeng	GZ-P-1	Law Enforcement Agent	Guizhou	30	Phone/Online	2020
24	Rouxun	GZ-P-10	Law Enforcement Agent	Guizhou	75	In Person	2020

25	Jingzhong	GZ-P-11	Law Enforcement Agent	Guizhou	30	In Person	2020
26	Chushao	GZ-P-12	Law Enforcement Agent	Guizhou	60	In Person	2020
27	Ruicong	GZ-P-2	Law Enforcement Agent	Guizhou	60	In Person	2020
28	Cheng	GZ-P-3	Law Enforcement Agent	Guizhou	60	In Person	2020
29	Hanling	GZ-P-4	Law Enforcement Agent	Guizhou	100	In Person	2020
30	Haoshuo	GZ-P-5	Law Enforcement Agent	Guizhou	40	In Person	2020
31	Xinxue	GZ-P-6	Law Enforcement Agent	Guizhou	120	In Person	2020
32	Muhui	GZ-P-7	Law Enforcement Agent	Guizhou	40	In Person	2020
33	Xinrou	GZ-P-8	Law Enforcement Agent	Guizhou	60	In Person	2020
34	Mandong	GZ-P-9	Law Enforcement Agent	Guizhou	100	Phone/Online	2020
35	Kangjian	HEB-P-1	Law Enforcement Agent	Hebei	40	Phone/Online	2020
36	Yun	HUB-P-1	Law Enforcement Agent	Hebei	30	Phone/Online	2020
37	Haojing	HUB-P-2	Law Enforcement Agent	Hebei	10	Phone/Online	2020
38	Xiumei	HUB-P-3	Law Enforcement Agent	Hebei	30	Phone/Online	2020
39	Kaile	SX-P-1	Law Enforcement Agent	Shanxi	90	Phone/Online	2020
40	Yuqing	SX-R-1	Relevant Actor	Shaanxi	40	In Person	2020

41	Haoming	SX-H-1	Former Cybercriminal	Shaanxi	120	In Person	2020
42	Feiyue	SX-H-2	Former Cybercriminal	Shaanxi	30	In Person	2020
43	Qinglan	SX-H-3	Former Cybercriminal	Shaanxi	10	In Person	2020
44	Shentu	SX-H-4	Former Cybercriminal	Shaanxi	40	In Person	2020
45	Youlv	SX-H-5	Former Cybercriminal	Shaanxi	40	In Person	2020
46	Rubo	US-CSP-1	Cyber Security Practitioner	USA	40	Phone/Online	2020
47	Ming	US-CSP-2	Cyber Security Practitioner	USA	20	Phone/Online	2020
48	Hongzhe	GD-H-1	Former Cybercriminal	Guangdong	120	In Person	2021
49	Qiubai	GD-P-15	Law Enforcement Agent	Guangdong	40	In Person	2021
50	Youpu	GD-P-19	Law Enforcement Agent	Guangdong	120	In Person	2021
51	Yanse	GD-P-20	Law Enforcement Agent	Guangdong	70	In Person	2021
52	Ling	GD-P-21	Law Enforcement Agent	Guangdong	65	In Person	2021
53	Qiang	GD-P-22	Law Enforcement Agent	Guangdong	70	In Person	2021
54	Guogong	GD-PST-1	Prosecutor	Guangdong	15	In Person	2021
55	Yunmeng	GD-PST-2	Prosecutor	Guangdong	30	In Person	2021
56	Mengzhi	GD-PST-3	Prosecutor	Guangdong	40	In Person	2021

57	Xueman	GD-PST-4	Prosecutor	Guangdong	40	In Person	2021
58	Xiuping	GD-PST-5	Prosecutor	Guangdong	40	In Person	2021
59	Bo	GD-R-1	Relevant Actor	Guangdong	60	In Person	2021
60	Fengshu	GX-P-1	Law Enforcement Agent	Guangxi	90	Phone/Online	2021
61	Zhenqiang	GX-P-2	Law Enforcement Agent	Guangxi	90	In Person	2021
62	Siwen	GX-P-3	Law Enforcement Agent	Guangxi	70	In Person	2021
63	Sugar	SC-H-1	Former Cybercriminal	Sichuan	60	In Person	2021
64	Yian	SC-R-1	Relevant Actor	Sichuan	50	In Person	2021
65	Wangming	SX-CSP-1	Cyber Security Practitioner	Shaanxi	70	Phone/Online	2022
66	Chengzi	SX-CSP-2	Cyber Security Practitioner	Shaanxi	40	Phone/Online	2022

There are reasons for ruling out active cybercriminals in this research. Interviewing active offenders in China was overall deemed to be too risky. Ethical consideration is one of the biggest concerns when the interview subjects are active criminals. Given the potential surveillance risks in China, handling the aspects of sensitivity, security, and consent posed substantial challenges. Practical reasons are also an important consideration. Active criminals are difficult to approach. They also have fewer reasons to disclose their activities. When they do, their credibility is hard to assess. In addition, since I engaged a lot of law enforcement participants, staying away from active offenders helped prevent any potential issues, especially if law enforcement officials wanted to know about the offenders I interviewed. Compared with active cybercriminals, former cybercriminals are better

subjects. As will be discussed in more detail, former cybercriminals are easier to approach. Some of them now work as cybersecurity practitioners. Once they agree to participate in the interview, they have little motivation to lie. However, despite the fact that prison inmates can be a fruitful information source, because of ethical concerns, particularly regarding the issue of consent, they are not included in the sample. In any case, during the fieldwork, the COVID-19 restrictions in China made accessing prisons impossible.

2.2 Secondary data

These data are all recorded in Chinese, and many of them have never been used by scholars to study cybercrime. My secondary data include 1) newspaper articles, 2) blog posts from law enforcement agencies, 3) private cybersecurity firm reports and materials, 4) documents given by law enforcement agencies and prosecutors in the course interviews, and 5) judgments from the courts.

Among the secondary data, newspaper articles and blog posts were mainly used to acquire background knowledge for the research. They were not coded and not directly cited in the study. Private cybersecurity firm reports and materials and documents given by law enforcement agencies and prosecutors in the course interviews were coded for qualitative analysis.

During my fieldwork, I realised that a large extent of Chinese cybercrime is connected to cyber fraud. Consequently, I decided to gather judgments relating to cyber fraud cases to foster a better understanding of Chinese cybercrime. Judgments from the courts in China are a valuable dataset for this research. Each individual judgment contains a description of the background of the case and modus operandi. If the case involves more than one defendant, it includes a brief description of how the defendants met, how they communicated (what platform they used), and the nature of their cooperation. The

judgments also provide geographical information, including the location of the victim, the defendant when he/she was arrested, and the defendant's place of birth. The locations are reported by districts of cities. In addition, judgments illustrate the criminal records of the defendants, the sentences, and the evidence used in prosecution. Demographic information, including the date of birth, gender, and level of education of the defendant is also provided. In total, 6,686 judgments were collected and used to provide descriptive statistics. These judgments are trials between 2014 and 2019 that contained the keyword 'cyber fraud' (网络诈骗). By examining the descriptive statistics generated from the court judgment, the evolution of modus operandi and patterns of cooperation can be revealed. They can also be used qualitatively to achieve triangulation. Descriptive statistics can be generated from these data to demonstrate the profiles of Chinese cybercriminals. The data are biased as they represent only Chinese cybercriminals who are arrested and prosecuted. However, they at least represent a portion of Chinese cybercriminals. The interviews can also help to address this bias by providing information on those who have not been arrested. In addition, 312 judgments were extracted to conduct qualitative content analysis (300 were randomly selected and 12 judgments were purposively selected due to the suggestion of my participants). How they were selected will be discussed in the below section.

Most of the secondary data are publicly accessible. Nevertheless, some of them are not. These include two types of data. The first type is the law enforcement confidential investigation documents. They are in the forms of files, reports and hand-made diagrams. I labelled them as LECID (N=16). The second type of data are internal reports and materials made by cybersecurity companies. I collected nine reports in total, which I also labelled as CSCR. They were given to me in the course of interviews by the participants. Table 2 below summarises the secondary data that were coded and cited in this study.

Table 2: Secondary Data Provided by Interview Subjects

LECID -1	A Confidential Investigation Document
LECID -2	A Confidential Investigation Document
LECID -3	A Confidential Investigation Document
LECID -4	A Confidential Investigation Document
LECID -5	A Confidential Investigation Document
LECID -6	A Confidential Investigation Document
LECID -7	A Confidential Investigation Document
LECID -8	A Confidential Investigation Document
LECID -9	A Confidential Investigation Document
LECID -10	A Confidential Investigation Document
LECID -11	A Confidential Investigation Document
LECID -12	A Confidential Investigation Document
LECID -13	A Confidential Investigation Document
LECID -14	An Internal Police Report
LECID -15	A Diagram Drawn by a Police Officer
LECID -16	A Diagram Drawn by a Police Officer
CSCR-1	A Report Provided by a Cybersecurity Company
CSCR-2	A Report Provided by a Cybersecurity Company
CSCR-3	A Report Provided by a Cybersecurity Company
CSCR-4	A Report Provided by a Cybersecurity Company
CSCR-5	A Report Provided by a Cybersecurity Company
CSCR-6	A Screenshot Provided by a Cybersecurity Company that Records Communications between Cybercriminals
CSCR-7	A Screenshot Provided by a Cybersecurity Company that Records Communications between Cybercriminals
CSCR-8	A Screenshot Provided by a Cybersecurity Company that Records Communications between Cybercriminals

CSCR-9	A Screenshot Provided by a Cybersecurity Company that Records Communications between Cybercriminals

3. Data Collection

This section outlines how the primary and secondary data were collected during the fieldwork. The overall data collection strategy, the sampling strategies and the influence of challenges caused by the COVID-19 pandemic are also discussed.

3.1 Interview Data Collection

Overall, participants were primarily recruited through three sampling strategies: geographical sampling, purposive sampling, and snowball sampling. Most of the time I used these three sampling strategies in this order. I first selected the location where I wanted to go, and where I was able to go under the COVID-19 policy in China. I then recruited local participants before I arrived and arranged the meeting agenda. After the interview, I asked the participants if they were able to refer me to more potential interviewees. However, this order was not followed strictly. In some cases, I contacted the participants before deciding to travel to a specific location. This typically happened when an interviewed participant referred me to a person who resided in another city. As mentioned, most of the interviews took place in person. Online and phone interviews were used on occasions when the participants were in remote cities, when the meeting had to be cancelled due to lockdowns, and when the participants specifically wanted to be interviewed this way (usually due to their busy schedule). As noted, almost all participants preferred a face-to-face interview.

Geographical Sampling

Prior to the fieldwork, I had both practical and strategic considerations in mind. Practically, it is impossible to undertake interviews across the whole country, considering the size of China and time limitations. Location choice is also influenced by the presence of suitable participants. The majority of my fieldwork locations were in large cities in China. These include the capital cities of different provinces and some other economically developed cities, such as Shenzhen. There are three practical reasons for this decision. First, most of the cybersecurity companies are located in large cities in China. Therefore, it would be easier for me to recruit cybersecurity practitioners in these places. Second, law enforcement agents in big cities are more likely to have experience in combatting cybercrime. There are not only more experienced personnel in law enforcement agencies who can handle complicated cybercrime cases, but there are also likely to be more victims in these large cities. Law enforcement agencies in these cities also often lead crackdown operations against cybercrime. As a result, the chances of recruiting law enforcement agents who are familiar with cybercrime are higher. Third, most of my existing contacts and experience are from large cities in China.

Strategically, in order to understand Chinese cybercrime from a comparative angle and allow for variation, I decided to cover cities with different political and economic statuses. For example, I conducted interviews in some 'first-tier' (most developed) cities in China, such as Shenzhen, some 'second-tier' cities such as Chengdu, and some rural areas such as Lianjiang. I also ensured I went to cities that were suspected hubs of cybercrime. The tier system is widely adopted in China to classify the economic status of prefecture-level cities. The official classification is provided by the China Business Network (Xin, 2022), which is a government-owned organisation. I selected the cities in each tier mainly based on practical considerations, such as accessibility, the number of existing contacts there, and the proximity to other cities that I planned to visit.

Nevertheless, due to the impact of the COVID-19 pandemic, my travel plans were significantly affected. I had to abandon many locations on my list and went only to the cities where I was able to visit in accordance with ongoing and strictly enforced travel restrictions. The geographical sampling was therefore not strictly applied. More details on this will be discussed in a later section.

Purposive Sampling

Following Lusthaus's (2018) strategy, before my fieldwork commenced, I identified three groups of people: practitioners in the cybersecurity sector, law enforcement officers, and former cybercriminals now working in the field of cybersecurity. For the practical reasons stated above, I didn't pursue active cybercriminals or prison inmates. As was expected, I did not encounter any troubles with former cybercriminals, and most of them were talkative and open to the discussion of cybercrime. They provided me with a large amount of invaluable information that enabled me to complete this study.

I purposively recruited participants who came from the above career background. To do so, I initially asked my friends who worked in the cybersecurity sector to invite me to a number of cybersecurity-related WeChat groups. Later, I joined more groups of this type via links shared by group members in the course of their daily chats. These WeChat groups are essentially platforms for people who work in the cybersecurity field to chat and share information. Chat contents included regulated chatting, the latest cybersecurity-related scandals and news (such as a database breach), the newest technologies, and job opportunities. Most of the groups consist of over 100 members based in different cities in China, from a range of career backgrounds related to cybersecurity, including former cybercriminals. None of my friends were active participants in these groups, nor did they have extensive knowledge of the group members. Given the size of these groups and the

fact that members were dispersed across different regions of China, the potential for selection bias was reasonably mitigated. I sent out invitations to the groups to recruit participants. Most participants recruited in this way were cybersecurity practitioners, some of them were formal law enforcement agents, and some of them now work closely with the police. Surprisingly, a formal cybercriminal actively responded to my invitation and was very open to discussing the topic.

In addition, I met a few prosecutors and cybersecurity practitioners through sports and an internship. During the chats, I came to know that they were very knowledgeable about cybercrime; I then included them in my samples. I tried to recruit via email and LinkedIn some famous cybersecurity practitioners and former cybercriminals who now work in the private cybersecurity sector. But my attempts failed as I received no response from any of them. In the end, I was unable to recruit any participants this way.

Snowball Sampling

Snowballing was an essential sampling method in my recruitment process. I used snowball sampling in two ways. First, I recruited people from my existing contacts. For example, some of my school friends and family friends now work in the cybersecurity sector and as law enforcement agents. Second, I always asked my participants if they could refer any other potential candidates to me after their interview. These attempts acquired fruitful results. After the interviews, I asked my participants to introduce me to new participants who might be willing to be interviewed. Through this snowball process, I conducted several trips that were not planned before the start of my fieldwork. I went to several cities and towns that were introduced to me as cybercrime hubs and I was able to interview local law enforcement agents and cybersecurity practitioners. I was also able to conduct many

interviews in remote places with people whom I had not met before, and who would otherwise be unlikely to talk to me.

My fieldwork journey started in Shenzhen, a city in Guangdong Province located in the southern part of China. I also used Shenzhen as a base, as it is the city where I was born and raised. Because of the proliferation of the IT industry in China, many of my childhood and school friends graduated from computer-science-related subjects and worked in technology companies in different large cities. A few of them are in Shenzhen. Thus, I started recruiting cybersecurity practitioners who I knew. The objectivity of this research remains largely unaffected by my positionality: it's pertinent to note that despite leveraging my personal contacts in China, the links between myself and the participants were rather tenuous. Since we had not been in contact for several years post-graduation, I had limited familiarity with most of these individuals. Moreover, being a Chinese citizen, they had less reason to lie to me about the real situation. Interestingly, a lot of cybersecurity practitioners in China now work closely with law enforcement agencies to tackle cybercrime. An important reason is that there is, in general, a lack of cybersecurity personnel in law enforcement agencies, especially in police departments. Therefore, many cybersecurity practitioners have detailed knowledge of the cybercrime situation in China. They are also able to provide views from a different angle that complements the information given by law enforcement agents.

I also had contacts in law enforcement agencies in a few cities in China. Most of them were my family friends, and I had never met them before the interview. Also, none of my family members works in the field of cybersecurity. Therefore, the connection between myself and the participants was also weak. Having existing contacts helped me a lot in recruiting law enforcement agents; there seems to be a general political concern about unknown researchers from Western countries. On the one hand, since crime is a sensitive

topic in China, law enforcement agents were generally unwilling to talk to strangers about it. On the other hand, law enforcement agents in China also worry that what they say might be reported in a twisted way that conveys a negative image of China. Thus, instead of approaching unknown law enforcement agents through email or phone, I relied heavily on my existing contacts to recruit law enforcement agents. No formal process was required for the interviews as long as they were conducted privately and without mentioning any specific cases.

Similarly, I recruited most of the former cybercriminals through snowball sampling. I did not ask whether they had been convicted when approaching them, unless they mentioned their convictions voluntarily. Most of them were friends or colleagues of cybersecurity practitioners. Since it was not a secret within the company and perhaps also in the cybersecurity sector, they were relatively open to speaking about their past and provided me with information from both sides.

I also recruited an additional group of people through snowball sampling – people related to cybercrime but who were difficult to define. I came across them by accident when one interviewee told me that they knew someone who would be good person to talk to. One person is a businessman who used to run a business in Myanmar. He provided me with invaluable information about the socio-political context in Myanmar and how Chinese cybercriminals operate there. The other person worked in a cyber fraud firm for a few months without even knowing she was conducting cyber fraud. She was arrested but was found not guilty. It would therefore be inappropriate to classify her as a former cybercriminal. She provided me with detailed information about how cyber fraud firms were able to operate in a big city and recruit dozens of people like her. The information provided by this group of interviewees complemented the statements from other groups of participants and gave me a better picture of the cyber fraud industry in China.

Interview Locations and Recording

Before the interviews, I always asked my participants where they felt the most comfortable talking. In most cases, no preference was given by the participants. In this circumstance, I offered to talk in public locations such as a café. Most of my interviews took place this way. However, on some occasions, I was invited to a participant's professional office to conduct the interviews, as the participant wanted to talk in a more private environment about the sensitive topic.

I also asked my participants whether they minded if the conversation was recorded. I recorded our conversations only when a positive answer was quickly given. If the participant was reluctant or concerned, I simply chose not to record and told them I would only take notes. When the interview was not recorded, I wrote down as much as I could in the notes. After every interview, I transcribed the notes into a digital form and saved it to my encrypted hard drive as soon as I could. During this process, I organised the notes in a logical way and filled out the abbreviations and incomplete sentences made when writing by hand. I referred to the digital notes during the writing process. For information that I believed to be important, I tried to note down the exact sentences the participants used. I would ask the interviewees to repeat the sentences when necessary. This action sometimes generated unexpected positive effects on the interview: the participant would elaborate on the topic and provide rich detail. Overall, in terms of interview quality, I did not feel there was much difference between those interviews that were recorded and those that were not. This confirmed to me that only recording interviews when participants were absolutely open to it was the correct choice for my project.

Influence of the COVID-19 Pandemic

I began my fieldwork at the beginning of 2020. Soon after, a few interviews were conducted in Shenzhen, the pandemic started in China and lasted for over three years. My fieldwork was significantly affected by the pandemic, and my plans were forced to change several times.

The biggest challenges I faced were fear, lockdowns, and travel restrictions. At the beginning of the pandemic, I knew very little about the disease, and I had no supply of face masks. I was very afraid of going out to meet people. Later, the lockdown started in various cities in China. Because people were deeply affected by the pandemic in both physical and psychological ways, arranging interviews, even online, was difficult at the time. Thus, for the first half of 2020, almost no interviews were conducted.

I resumed my fieldwork in June 2020 when the situation improved in China. There was about a one-year period when the pandemic seemed to calm down, and I did most of my interviews during this time. However, travelling around the country was still difficult mainly due to two reasons.

First, lockdowns took place from city to city for different periods of time. When the cases of infection went up in a city, it had the tendency to go into lockdown. Once a city was in lockdown, people were not allowed to travel into or out of the city. Shenzhen went into lockdown a number of times, which disrupted my travel plans to a large extent, as I was effectively trapped. There were also occasions when a trip had to be cancelled because the destination city went into or was likely to go into lockdown. For instance, I had to cancel my trip to Xinjiang because the city went into lockdown a few days before I planned to travel there. On one occasion, I was advised by a law enforcement officer to cut short my trip and leave, as he was firmly convinced that a city-wide lockdown was imminent.

Second, there were general travel restrictions in the country. Some cities only allowed me entrance if I had not been to certain cities with a high number of infectious cases, and some cities permitted entrance only if there had been no case of infection for a number of days in the city from which I had travelled. Self-isolation for a period of time was also required in many cities. For these reasons, I was unable to enter some cities. Beijing and Shanghai were two that I never had a chance to visit. Because of these challenges, I didn't visit every place I had intended to conduct interviews in.

From January 2022, the travel restrictions became even stricter in China because of the emergence of the Omicron variant. PCR tests were required to be taken on a daily basis in Shenzhen, and travelling became even more difficult. There were also more lockdowns across the country. I managed to make a few short trips to cities close to Shenzhen and conducted some phone/online interviews. But at this point, with both research and day-to-day life becoming very challenging, I decided to conclude my fieldwork and return to the UK in August 2022.

An additional challenge to the fieldwork was the recruitment of participants during the pandemic. To reduce the risk of infection, many law enforcement agents were required to follow a ‘two points, one line’ schedule during the weekdays, meaning that they should only travel between their home and their workplace. They were also required to avoid unnecessary contact with people during the weekend. As a result, my invitations were turned down by many law enforcement agents and cybersecurity practitioners who worked closely with them. What’s more, visiting prisons was strictly forbidden during the pandemic.

Overall, because of the pandemic, my fieldwork trips were forced to become fragmented. I couldn't visit all the places I had planned to go to, including the two big cities, Beijing and Shanghai. My recruitment of candidates was also subject to practical constraints. As a

result, my collection of interview data was less than I had hoped for but still sufficient to address my project aims.

Secondary Data Collection

As mentioned in the earlier section, I collected five different types of secondary data in China during the fieldwork, which were: 1) newspaper articles, 2) blog posts from law enforcement agencies, 3) private cybersecurity firm reports and materials, 4) documents given by law enforcement agencies and prosecutors in the course interviews, and 5) judgments from the courts. A content analysis on secondary data can provide an overview of the cybercrime environment in China and triangulate with the interview results.

Newspaper Articles and Articles Published by Law Enforcement Agencies

I collected 43 newspaper articles and articles published by law enforcement agencies on WeChat. WeChat is the most popular instant messaging and social media app in China. It allows organisations to create public accounts that can push feeds to subscribers and interact with them. In China, a lot of the articles are now published on WeChat Public Accounts (公众号). I subscribed to six public accounts run by law enforcement agencies, local governments and reliable newspaper publishers: The People's Daily (人民网), Safe Beijing (平安北京), Safe Guiyang (平安贵阳), The People's Public Security Newspaper (人民公安报), The Chinese police (中国警察网), and a public account ran by a cybersecurity company that works intensively with the law enforcement agency – Ending Fraud (终结诈骗). I regularly downloaded articles that reported on the Chinese cybercrime phenomenon published by these official accounts. These articles were mainly used to acquire background knowledge for the research. They were not coded and not directly cited in the study. Alongside these downloaded articles, I also searched articles on government

websites, law enforcement websites, and official websites of newspaper publishers on occasions when I wanted to make citations. The citations are in the form of websites, and the links to the articles are provided in the bibliography.

Private Cybersecurity Firms Reports

Most cybersecurity firm reports seem to be either internal or printed and only shared at conferences. I found only two publicly accessible reports made by private cybersecurity companies on the Internet. One of them was published by Tencent in 2017, and the other was made by Baidu in 2020. I didn't find any other available reports online when I was in China. However, when interviewing practitioners, I received a few more reports from the participants. Some of them were written as internal reports within the firms, and others were written for industry conferences but not published.

Documents from the Law Enforcement Agencies

I was also shown some investigation documents during the interviews with law enforcement and prosecutors. Some were diagrams they used in meetings, and others were reports or files. In some cases, I was not allowed to take away the original copy, but I was allowed to transcribe them in handwritten form with the omission of key information (e.g. names of the suspects). To avoid problems, I always asked my participants to check the transcriptions. I acquired permission to cite these data with the condition of keeping the source and the party mentioned in these reports anonymous.

Court Judgments

At the beginning of the project, I planned to download judgments through China Judgments Online (https://wenshu.court.gov.cn). This website is run by the government, and it

contains all criminal cases (except sensitive cases that are related to national security) since 2007. These cases are sorted by the articles in the Criminal Law of China, stored in MS Word files and available to download freely. I also planned to download judgments from the first trial that were associated with three cybercrime-related articles (articles 285, 286, 287) from 2014 to 2019. These articles address the offences of unauthorised access to computer systems, disrupting computer systems, and other offences committed by exploiting computer systems respectively. However, I soon identified two problems that forced me to adjust my plan. First, the China Judgments Online website was unstable at the time of the data collection process. It also has a very limited number of shown cases upon search. As a result, downloading all cases became difficult. Second, I realised that a significant number of the cyber fraud cases were not sentenced under these three articles but under articles related to fraud, selling of ID cards, assisting criminal behaviour, destruction of national wireless system etc. This is perhaps also the reason why the number of cases sentenced under these three articles is surprisingly small. Thus, using only cybercrime-related articles would omit a significant number of cyber fraud cases, which is the core of this research.

As a result, I made two adjustments to my original plan accordingly. I decided to use another website that contains criminal judgments run by a non-governmental organisation – Open Law (http://openlaw.cn). The website is very similar to China Judgments Online, but it allows users to download multiple cases at once. This made the collection of data much more convenient. I also searched for some criminal cases on both websites and found that the results were identical. I was therefore convinced that this website was a reliable source.

I used the advanced search function on the website and downloaded criminal cases from the first trial between 2014 and 2019 that contained the keyword ‘cyber fraud (网络诈骗)’.

The website was down most of the time from the end of 2020 until August 2022 for unknown reasons. Therefore, I was unable to download cases later than 2019.

Information extracted from the judgments was transferred and integrated into MS Excel through programming to capture the following information about the criminals involved in the judgment:

- Name of the criminal
- Gender
- Date of birth
- Education
- Career
- Criminal record
- Place of birth
- Place of residence
- Year of apprehension
- Trial charges
- Length of imprisonment
- Fine

I engaged the assistance of two friends with computer science backgrounds, who had no involvement in this research, to help at different stages of the process. This Excel sheet was subsequently imported into R to generate the descriptive statistics necessary for this research. Furthermore, I also conducted a qualitative content analysis of these judgments. Given the substantial quantity of judgments, it was not feasible to read all of them. Therefore, I wrote a program to randomly select 300 cases and purposefully selected an additional 12 cases mentioned by my participants. I manually coded these cases along with my interview data for further qualitative analysis.

4. Ethics and Risks

Given the research involves illegal behaviour, there are several potential ethical considerations, including maintaining confidentiality and anonymity and securing sensitive data (Dickson-Swift et al., 2008; Lusthaus, 2018).

To overcome these issues, all participants reported anonymously. They were also free to decide whether their interview was recorded. The interview data was carefully preserved on an encrypted laptop and a hard disk and kept confidential. Also, an information sheet that clearly stated my identity, the purposes of the research and the rights of participants was given together with a consent form. However, because of the sensitivity of the research topic, only oral consent was asked. Participants were also told before the interviews started that they were in control of what was and what was not to be disclosed. They were able to withdraw from the study at any time (Dickson-Swift et al., 2008). In order to further protect the anonymity of my participants, codes and randomly assigned pseudonyms were used to refer to them. I did not show the city in which the participants were based but used the province instead. Furthermore, I only indicated the year of the interview data.

Another ethical issue is coercion. Those who were recruited through social ties might feel obliged to participate in my research. Emphasis on voluntary consent and anonymity was given before the interviews started as mitigation.

Extra care was taken when I interviewed former criminals. As Lusthaus (2018) mentioned, the risks posed to researchers between interviewing traditional criminals and cybercriminals are different, with researchers possibly facing virtual threats due to the lack of conventional territoriality in cybercrime. Extra precaution was taken when contacting participants, including accepting only printed documents, paying attention to any links sent by participants, emphasising that they should not disclose information about ongoing crime, and being ready to stop the participant in time when such information was about to be disclosed (Hutchings, 2014). However, during the interviews, I did not encounter any risky situations, and each went smoothly.

Ethical issues and risks involved in using secondary data are minimal. Most of them are publicly accessible, and parties involved in specific cases were already reported

anonymously in many reports and articles. For those who were not, such as those who appeared in the investigation documents, I used a black ink pen to cross over the names when they were given to me. On occasions when I had to copy out the document, I did not copy the names of the individuals mentioned in the document.

5. Limitations

As with most research, this study is not without limitations. The first limitation comes from the sampling strategies used in the interview data collection process. Participants were not chosen randomly but purposively in this study. The selection of participants was also largely affected by practical constraints, with the pandemic being a major factor. I only travelled to a few provinces. For example, I did not conduct any interviews in Shanghai and did only one phone interview with a participant from Beijing. I also did not visit many north-western provinces in China, such as Xinjiang and Heilongjiang. Therefore, there is a potential for selection bias in the interview data, which may affect the accuracy and generalisation of the study. But, in the circumstances, it was not possible for me to correct such a bias.

However, the influence of data caused by imperfect geographical sampling could be limited. In China, local police have jurisdiction over a case as long as one victim is located in their city or is part of the criminal process that happened in their city. Thus, it is not uncommon for a policeman from Shenzhen, for example, to investigate a cybercrime case where criminals operate in Beijing. Moreover, when a cybercrime case involves victims from multiple cities, police from different cities may cooperate in the investigation. In fact, I often heard complaints from the police that they had to take too many trips to different cities in China. A similar experience was shared by many cybersecurity practitioners as

they often have customers from other cities. Therefore, most of my participants have experience in dealing with cybercrime cases outside of their cities, including Beijing and Shanghai, and other remote areas.

The issue of accuracy and generalisation was further mitigated by triangulation. Triangulation was achieved by interviewing different groups of people and using secondary data. By interviewing participants from different backgrounds, a more comprehensive view of the same issue can be better understood. The use of secondary data serves the same purpose. They also correct the geographical bias as cases and information reported in the secondary data come from different places in China. I actively compared statements between the participants and the secondary data to acquire an accurate account of the discussed matter.

The second limitation is the accuracy of the participant statements. This may be caused by inaccurate recollection, misunderstanding of the questions or dishonesty. This is a problem in many interview-based studies and is not specific to my project. Triangulation was also adopted to minimise this risk. Moreover, critical questions were sometimes asked more than once in different ways to avoid misinterpretation and dishonest responses from the participants. Contradictory statements were examined carefully together with the background of the participant. The offering of anonymity and the non-recording of interviews also helped to reduce the risk of dishonesty. Participants have less motivation to hide information if the confidentiality of the data is assured and their name cannot matched to the information.

Finally, the study does not include two essential sources of information: active cybercriminals and inmates. Information provided by these two groups of people would be invaluable in the study of crime-related topics. The limitation is mitigated by recruiting a relatively large number of participants and applying various types of secondary data. The

application of triangulation and the use of secondary data, especially the court judgments, may compensate for the missing interview data to an extent. But these groups are still not directly represented in the sample.

Chapter 3. The Industry

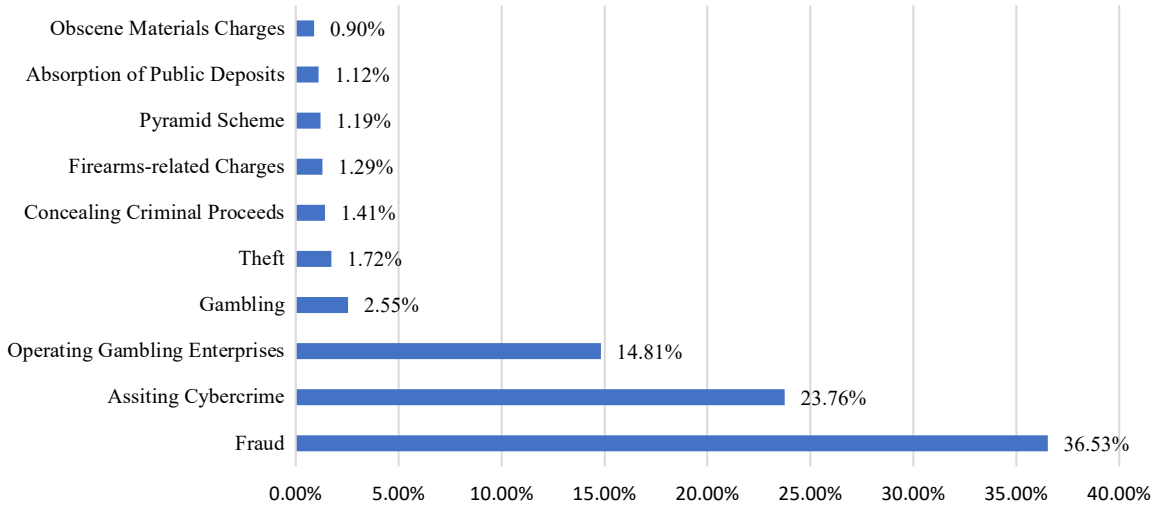
Over the last few decades, China has been in the midst of an internet revolution. After the infamous announcement in 1986 that “across the great wall, we can reach every corner of the world”, the number of internet users in China has grown rapidly (Liang & Lu, 2010). In 2018, there were 802 million people connected to the Internet, which covered 58% of the whole country’s population. By comparison, the United States had only 300 million internet users (McCarthy, 2018). Thanks to the proliferation of the Internet in China, the cybercrime rate has also dramatically increased. Nowadays, China has become home to many of the world's most prominent cybercriminals. A report provided by the Supreme People's Court of the People's Republic of China revealed that 282,000 cybercrime cases were brought to initial judgment in China between 2017 and 2021. Among these cases, one-third of them were cyber fraud (The Supreme People’s Court of the People’s Republic of China, 2022). That said, since most cybercrime incidents are not reported, this may be only the tip of the iceberg (Jewkes & Yar, 2013; Wall, 2008). In line with this report, the empirical data also suggest that a significant amount of cybercrime activities in China today are linked to cyber fraud. A wide range of professional cybercrime actors, specified in different areas, are running their businesses surrounding cyber fraud.

This background chapter presents a contextual overview of the cybercrime industry in China. The first section illustrates that cyber fraud lies at the core of the country's profit-driven cybercriminal activities and the cybercrime industry in China is essentially built around cyber fraud. The second section provides a detailed account of the widespread scams prevalent in China. The third section examines the socioeconomic factors that shape the current structure of cyber fraud. The fourth and final section inspects China's internet infrastructure and discusses its limitations in effectively controlling cybercrime.

1. Cyber Fraud: The Epicentre of Chinese Cybercrime

While a multitude of cybercriminal activities prevail in China, it is undeniable that cyber fraud constitutes the core of Chinese cybercrime. According to a report provided by the Supreme People's Court of the People's Republic of China , 282,000 cybercrime cases were

Figure 1: Top 10 Charges in Cybercrime Cases in China 2017-2021



adjudicated in the first instance by courts in China between 2017 and 2021. Of these cybercrime cases, 36.53% were sentenced under the charge of fraud, representing the highest proportion, while 23.76% were sentenced under the charge of 'assisting cybercrime', ranking second in prevalence. Notably, charges of 'damaging computer information systems' and 'unauthorised access to computer information systems' did not even rank in the top ten most prevalent charges (The Supreme People's Court of the People's Republic of China, 2022). The top ten most prevalent charges are listed in Figure 1. Furthermore, the same report noted that of the cases prosecuted under the charge of 'assisting cybercrime', 53.45% were related to cash-out activities, 18.25% were associated with providing communication transmission support, and 4.95% were tied to offering promotion services, which is to refer potential victims to cybercriminals. The data provided in this report indicate that there exists an extensive cybercrime industry within China,

where numerous cybercriminal activities revolve around cyber fraud, offering essential support and services.

The empirical evidence underlines this assertion, showing that an overwhelming majority of cybercriminal activities in the country have ties to cyber fraud. Most reports provided by cybersecurity firms indicate that cyber fraudsters form the largest customer base for illicit online services and products (CSCR-1, CSCR-2, CSCR-3). For instance, an internal report by a Chinese cybersecurity firm noted that in September 2021, out of the 110 million mobile malware-related activities detected in China, an astounding 98.73% were linked to scam-promotion (CSCR-4). The interview data also echo these cybersecurity reports. Almost all interviewees strongly emphasised the prevalence/dominance of cyber fraud and the illicit businesses around it while talking about cybercrime in China. For example, a cybersecurity practitioner, Ningxin, viewed cyber fraud as emblematic of Chinese cybercrime, as it represents the state of the art in cybercrime technology. He wrote:

> I believe that cyber fraud is acting as a driving force behind the evolution of cybercrime technology. It also reflects the current state of cybercrime technology in China...You see, cyber fraud brings in money quickly. It's even reputed to be more lucrative than selling drugs. Driven by substantial profits, there is a large investment in the technological development of cyber fraud. Initially, several years ago, the technology only involved altering call numbers to impersonate anyone. However, the technology has now evolved to the construction of fraudulent websites and the usage of Trojans. The professionalisation of cyber fraud now even extends to late-stage operations, including online money laundering and cross-border fund transfers. (GD-CSP-2)

The linkage between cyber fraud and other forms of cybercrime in China is further exemplified by two cases extracted from court judgments. The first case is *Tang Jiansheng, Zhang Liuxiu re Fraud* (Case No. [2017] Gan 1127 Xing Chu No.181)[3]. In this case, as Figure 2 shows, Tang and his scam group, consisting of four members, purchased SIM

[3] 汤建胜、张六秀诈骗一审刑事判决书, (2017) 赣 1127 刑初 181 号

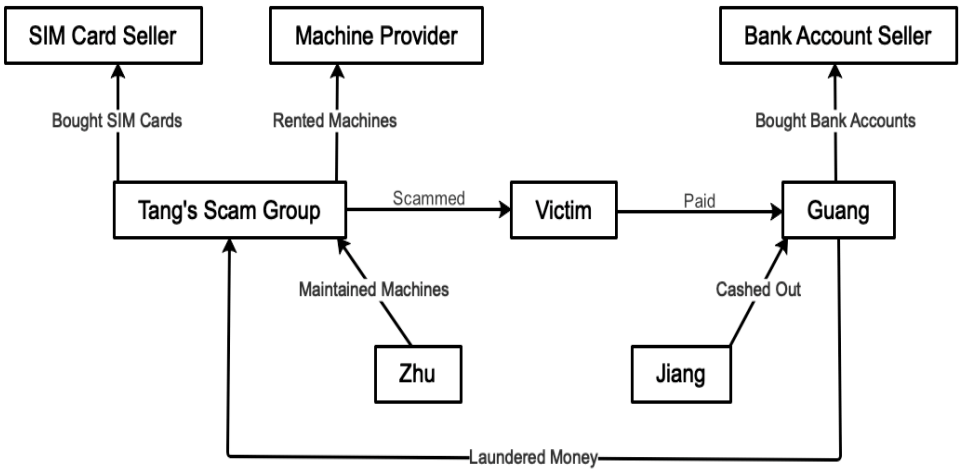


Figure 2: Criminal Operation in *Tang Jiansheng, Zhang Liuxiu re Fraud*

cards and rented machines with software that allowed them to disseminate vast scam messages and make multiple phone calls at a time from unknown third parties. They then sent the machines to another cybercriminal, Zhu, who provided machine set-up, testing and maintenance services to various scam groups. When executing the scam, Tang and his group asked the victims to transfer money to Guang, a money launderer who had purchased many bank accounts from unknown third parties. After the money was paid and laundered, Guang recruited Jiang, a money mule to cash out the money, took a 5% commission and returned the rest to Tang and his group. This case reflects that a successful cyber fraud operation in China often involves not only the cyber fraudsters, but also multiple cybercriminals who play equally important roles.

The second case is *Jin Huan, Li Rongkang, Sun Lei & Others re Concealing Crime-related Income* (Case No. [2020] Shan 0702 Xing Chu No.190)[4]. In this case, cybercriminals with advanced technical skills were involved. As demonstrated in Figure 3 below, Fighter, a criminal from a scam group located in the Philippines and whose real name was unknown, contacted Sun, a hacker who lived in China, online and paid him to

[4] 金欢、李榕康、孙磊等掩饰、隐瞒犯罪所得、犯罪所得收益罪一审刑事判决书，(2020）陕 0702 刑初 190 号

build and maintain three fraudulent gambling websites where the owner could manipulate the game results. After accepting the task, Sun paid Hema, another hacker, to improve the source codes of the websites. Sun also paid JingKuan, a more advanced hacker, to revise the web configurations and to solve technical problems that went beyond his capacity. At the same time, Fighter found Yin, a Chinese money launderer who lived in the Philippines but had never met Fighter, to help him to exchange the stolen money from Chinese yuan to the Philippine peso. Yin then recruited Jin, Jiang and Yi, who were located in China, as his money mules: they provided their bank accounts to Yin, which were later provided to Fighter by Yin to receive the money transferred from Fighter. When the money was transferred to the accounts, they cashed out the money and gave it to Yin, Yin then gave

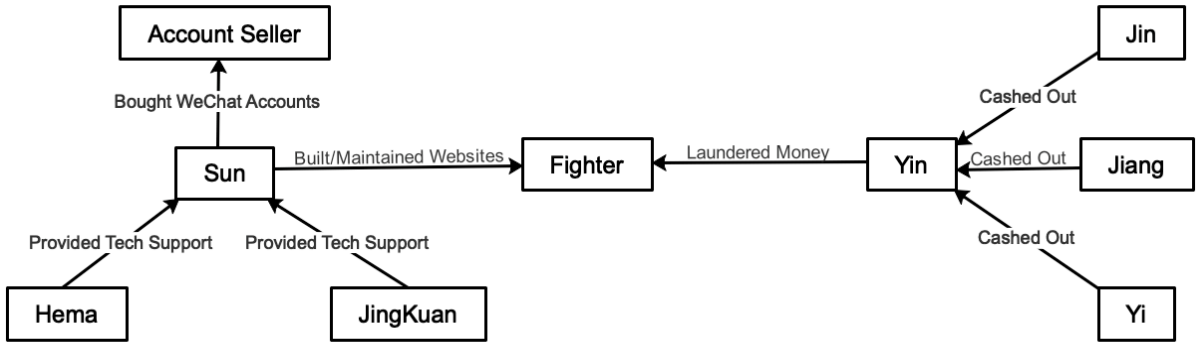


Figure 3: Criminal Operation in *Jin Huan, Li Rongkang, Sun Lei & Others re Concealing Crime-related Income*

Fighter the peso at a pre-agreed exchange rate.

Overall, stemming from the empirical data, it is clear that the cybercrime industry in China today is primarily constructed around cyber fraud. The following section moves on to examine the prevalent frauds in China to offer a further understanding of the country's cybercrime.

2. Prevalent Frauds in China

Cyber fraud has presented itself in various forms in China. People's Daily, a newspaper publisher managed by the Chinese government, published several reports that revealed numerous prevalent scams and their modus operandi in the country in recent years, in which many scams were assigned names to represent the modus operandi, such as the 'Who am I scam', 'money-for-child scam', and the 'government impersonation scam' (Wen & Tang, 2018). The lists provided in the reports are however not exhaustive; numerous scams not included in the reports were also introduced by my interviewees who reflected on pre-collected judgments in relation to cyber fraud, suggesting that the number of scams is still rapidly increasing in China following the development of wireless technologies and the change of people's social activity patterns (GD-CSP-2, GD-P-2, GZ-P-5, GZ-P-12, GD-P-4, GD-P-5, GZ-P-9). Moreover, while the majority of these scams target Chinese citizens, there is mounting evidence to suggest that cybercriminals are beginning to focus their attention on foreign victims as well. Policeman Ruoxun recounted a case where a cyber fraud group specifically targeted Russian victims and recruited two Russian speakers to facilitate the translation of online chats (GZ-P-10). Overall, the prevalent scams can be roughly grouped into six types:

Acquaintance Scams

Acquaintance scams take place when a criminal pretends to be someone whom the victim knows, such as a company leader, a friend, or a relative, and makes up an excuse such as being involved in a car accident to lure the victim into giving them money. One of the most well-known scams of this type is the 'Who am I scam'. For example, in the case of *Lin Moumou, Yuan Moujia & Yuan Mouy re Fraud* (Case No. [2016] Hei 0223 Xing

Chu No.149)[5], one of the victims received a phone call from a defendant who claimed to be her old friend and asked her to guess his name. While the victim asked if he was Liang, one of her husband's old friends, the defendant confirmed and said he had changed his phone number because he had lost his old phone. The conversation went on for a while and everything seemed normal, carrying into the next day. However, the defendant then reached out to the victim once more, alleging that their bank card had accidentally been demagnetised. He further claimed that he had an urgent business payment to make, and asked if the victim could lend him a certain amount of money. The victim agreed without a second thought and transferred 5000 yuan (approximately $800) to the account provided by the defendant. After the bank transfer was done, the defendant made up another excuse and asked the victim to lend him more money. The victim was suspicious, called her husband, and finally realised that she had been scammed.

Shopping/Service-related Scams

Shopping and service-related scams occur when a criminal pretends to be someone who is associated with government services or commercial activities, such as a seller, airline staff, bank staff, or civil servant. They then ask the victim to pay a fee to fulfil their duties, such as paying tax, or to receive services/secure benefits such as an airline ticket exchange, shopping discount or reimbursement. The 'airline ticket refund scam' is one of the most famous scams. For instance, in *Wen Yuanyu, Tang Jiansheng re Fraud* (Case No. [2007] Qiong 9003 Xing Chu No.200)[6], the defendants purchased airline-ticket order information online and sent telephone texts via software to victims who had made ticket orders recently, announcing that their flights had been cancelled and providing a contact number. When the

[5] 林某某、袁某甲、袁某乙诈骗罪一审刑事判决书，(2016)黑 0223 刑初 149 号
[6] 温远宇、唐建生诈骗罪一审刑事判决书，（2017）琼 9003 刑初 200 号

victims phoned the number, the defendants pretended to be a member of the airline staff and asked the victims to pay an ‘administration fee’ or the ‘tax’ to get their refund. When the money was transferred to the provided account, the defendants immediately cashed the money and disappeared.

Intimidation Scams

In intimidation scams, the perpetrator employs scare tactics, fabricating scenarios designed to threaten the victim and coerce them into parting with their money. The scammer may pose as a police officer investigating the victim, a person claiming to have evidence of the victim's illicit activities, or an individual asserting control over a family member in danger (for instance, a mafia member claiming to have kidnapped a relative, or a doctor insisting on immediate payment for surgery needed to save a relative involved in an accident). The aim is to convince the victim to pay in order to safeguard their own or their family member's wellbeing. The ‘government impersonation scam’ is one example. In a case report provided by an interviewee (LECID-11), the victim received a phone call from Beijing. The caller spoke in standard Mandarin, claiming to be a police officer from Beijing Public Security Bureau, and asked if the victim was Liu. Upon confirmation, the caller said the call was being transferred to the office phone line of the Beijing Public Security Bureau. Following some background sounds, another man answered the phone and told the victim that he was involved in a money laundering case and ordered him to go to Beijing Public Security Bureau immediately to cooperate with the investigation. When the victim told him that he was not in Beijing and unable to go to the Bureau any sooner than the next day, he was told to stay alone in a hotel room and keep the whole thing a secret from everyone, including his family, as the case was under investigation. He was also asked to add an official QQ account of the Bureau and check some legal documents.

After adding the provided QQ account, the victim received some legal documents about his case, including a freezing order provided by the Beijing Municipal Procuratorate. The victim was also directed to certain websites to confirm his investigation status. Finally, the victim was asked to open a new bank account, transfer the amount involved in the investigation to the new account and reveal key information about the bank account. When this was done, the victim was told to wait for further instruction, and this never came.

Investment Scams

Investment scams arise when a perpetrator presents a seemingly lucrative opportunity to a victim, such as a high-yield financial investment scheme. In some cases, the victim may earn a small amount of money at the beginning but will eventually lose their investment when the number of investments increases. In *Hou Tao, Huang Bin & Others re Fraud* (Case No. [2020] Su 0114 Xing Chu No.60)[7], Huang Bin, a defendant pretending to be a financial analyst assistant, invited the victims to join QQ/WeChat groups about investment. Hou Tao, another defendant, acted as a financial analyst in the groups, asked the victims to download a fraudulent trading platform and regularly gave instructions about investment on this platform. Other defendants who had already joined the groups pretended to be investors, regularly posted screenshots, and claimed they had made money following the instruction of Hou Tao to persuade the victims to invest. In the end, the victims lost all the investment and finally realised they had been scammed.

Romance Scams

Romance scams happen when a criminal adopts a fake identity and pretends to be in a relationship with the victim for a period of time. They then manipulate the victim to 'lend'

[7] 侯涛、黄兵等诈骗一审刑事判决书，(2020) 苏 0114 刑初 60 号

them money or to invest in a fraudulent website that is controlled by the criminal. The 'pig-killing scam' is a typical romance scam that proliferates in China. In the case of *Liu Zhaopeng re Fraud* (Case No. [2019] Lu 1722 Xing Chu No.589)[8], the victim met a person called Zhang on a matching app. Zhang introduced himself as a successful man who worked in the finance sector. He also sent the victim photos and videos of his luxury mansions and cars. After several days of chatting, they established a romantic relationship and Zhang started to share his tricks to earn money and claimed that most of his assets came from an online gambling platform which he could access from the backdoor and where he was able to get the outcome of each game. Zhang also promised that he would share the resource with the victim and make her rich as a gift to their relationship. Relying on Zhang's promise, the victim downloaded the nominated gambling app and tried it several times with a small amount of money. For the first couple of days, the victim won a great deal of money and started to be deeply attracted to the game and the charming man behind it who was able to make her rich. Subsequently, encouraged by Zhang, the victim gradually increased her gambling investment and even started to borrow money from her acquaintances. Eventually, the victim found that she was unable to cash out the money she won on the platform and Zhang went silent. In the end, when the victim still had around 160,000 yuan (approximately $25,000) in the account of her gambling app, Zhang video-called her and told her frankly that she had been scammed.

Windfall Scams

Windfall scams occur when a criminal makes the victim believe that they could get an amount of money easily, such as asking the victim for a simple favour with a promise to pay high remuneration or convincing the victim that they have won a lottery. The criminal

[8] 刘朝蓬诈骗一审刑事判决书, (2019)鲁 1722 刑初 589 号

then asks the victim to make an advance payment using excuses such as a 'promise fee' or 'validation fee'. In *Zheng Guowen, Zhang Ren Ying re Fraud* (Case No. [2018] Gan 1181 Xing Chu No.26)[9], the defendants published an advertisement in which they portrayed themselves as a 30-year-old affluent businesswoman longing for a child, promising 5 million yuan (approximately $775,590) to a suitable candidate for fatherhood. The victims, believing it was true, called the number posted on the advertisement and provided personal information as requested by the defendants. After informing the victims that they were qualified, they were asked to pay a certain amount of 'promise fee'. Once the money was paid, the defendants told the victims to wait for their visit, and disappeared.

Table 1: Prevalent Scams in China

No.	Types	Prevalent Scams
1	Acquaintance Scams	QQ impersonation scam, Fake boss scam, Who am I scam
2	Shopping/Service -related Scams	Procurement service scam, Prostitution scam, 'Thumbs-up' scam, Overdue scam, Airline ticket refund scam, Social insurance scam, Loan scam, Online shopping scam
3	Intimidation Scams	Government impersonation scam, Fraudulent car accident scam, Mafia scam, Fraudulent surgery scam, PhotoShop scam
4	Investment Scams	Financial investment scam, Pyramid schemes, Click-farming scams
5	Romance Scams	Pig-killing scam, Tea leaves scam
6	Windfall Scams	Money-for-child scam, Recruitment scam, Lottery scam

Table 1 above summarises the different types of prevalent scam and their variations in China. Looking at the scam types, there are no significant differences between these and long-existing scams worldwide. Similar types of scam have been reported and studied by many scholars (Button & Cross, 2017; Lusthaus, 2018; Whitty, 2018; Bidgoli & Grossklags, 2017; Leukfeldt, 2014; Lusthaus & Varese, 2021). For instance, online shopping and auction-related scams and advance fee-related scams were also two prevalent types of fraud in the UK, which accounted for 11.6% and 14.1% of the overall reported fraud cases in 2016 respectively (Levi et al., 2017). These fraudulent schemes also operate

[9] 郑国文、张任英诈骗一审刑事判决书，（2018）赣 1181 刑初 26 号

on the same underlying mechanisms, even though their specific methods of execution may differ. For instance, many scams involving an upfront payment, such as the 'lottery scam', 'money-for-child scam', and 'click-farming scam', appear to be contemporary iterations or evolutions of the traditional '419 scam'. This scam, typically associated with Nigerian offenders, involves the criminal persuading the victim to forward money under the promise of receiving a substantially larger return in the near future (Isacenkova et al., 2014; Chawki et al., 2015).

The parallels between the *modus operandi* of cyber fraud in China and worldwide can potentially be attributed to two factors. Firstly, these scams might have independently developed within China, bearing a resemblance to those in other regions due to a limited number of feasible scam types that can be executed. Secondly, there may exist a diffusion process whereby these scams are learned from and imported by Chinese cybercriminals. The empirical data suggest that both the independent development and the diffusion process may be occurring simultaneously. On one hand, some frauds have their roots in traditional schemes that first appeared in China and were later adapted for cyber fraud. For instance, officer Zhenqiang posited that the 'Incense Sticks Scam', a traditional face-to-face fraud scheme that once thrived in his city in Guangxi Province, could be the predecessor of today's online investment scams. He wrote:

> This place historically was a battlefield of the Communist Party and the Nationalist Party. When the Nationalist Party fled, they left a lot of US dollars and many of them were picked up by the locals. A scam then arose. The criminals would use the US dollars to light up cigarettes in front of local businessmen to attract their attention. They would claim that there were a lot of US dollars left in their house and that they didn't have a chance to use them and invited the victim to trade with them using Chinese currency at a low exchange rate. They would invite the victim to their house and show them the box full of dollars. In fact, only the first couple of layers were real dollars. The rests were newspapers or something else. Here we also have a custom, which is that while doing the currency exchange both parties would take the money to a cave, light up some incense sticks, do a ceremony and leave the money in the cave for three days. However, the geographical characteristic of this area is called Karst. The caves normally have a

> hidden back entry. So the criminal would sneak in using the back entry and steal the money (GX-P-2).

The foundational mechanism of this fraud – fostering a sense of mutual commitment – has been preserved and transformed into online financial investment scams (GX-P-2).

On the other hand, some participants noted that certain scams, such as the government impersonation scam, have their origins in Taiwan and were subsequently adopted in mainland China (HEB-P-1, GD-CSP-2, SX-P-1). This aligns with various news stories and government reports that document the apprehension of Taiwanese fraudsters (Han, 2016; Government of the People's Republic of China, 2018). In the case of *Wu Junyi re Fraud* (Case No. [2017] Yue 04 Xing Chu No.171)[10], the leader of the cyber fraud group that specialised in the government impersonation scam was also from Taiwan. The evidence presented above suggests that there is some degree of interaction and influence exchange between cyber fraudsters in China and their counterparts in regions beyond mainland China, leading to a diffusion process whereby some scams are imported from international cybercriminals.

In summary, this section has introduced prevalent scams in China. Upon comparing these with long-standing scams from overseas, although the execution of the scams may differ, no substantial differences are apparent in terms of their underlying mechanisms. The empirical data suggests that this resemblance could be the result of both the limitation of feasible scam types and a global diffusion process.

[10] 吴俊仪诈骗一审刑事判决书, (2017)粤 04 刑初 171 号

3. Exploring Socio-economic Drivers of the Cybercrime Industry

Criminological research indicates that understanding the formation and proliferation of specific crime patterns within a region necessitates an analysis of underlying socio-economic factors. These can include shifts in daily routines, as well as broader social and economic transformations (Felson, 2016; Gambetta, 1996; Varese, 2001; Wang, 2017). The same approach has also been used in the analysis of cybercrime (E. R. Leukfeldt & Yar, 2016; Williams et al., 2019). Following this line of thought, this section will delve into several socio-economic factors that could potentially influence the structure of China's cybercrime industry.

3.1 The Transition of Traditional Crime to Cybercrime

The social changes and the availability of digital technologies in detecting and combating traditional crimes are primary factors impacting the landscape of cybercrime in China. On the one hand, the proliferation of cashless payments has reduced the opportunity for profit-driven street crimes, as few people have cash on them today. As Jinghui, a police officer, noted: "I believe it is the cashless payment that has defeated the street crimes. Nowadays, we don't carry money when we go out. Even if you were to rob someone, what could you possibly steal (GD-P-9)?" On the other hand, recent advancements in digital technologies, such as facial recognition systems and the ubiquitous deployment of surveillance cameras, coupled with stringent crackdowns on crime in China, have further limited profit-driven traditional crimes. This pressure has subsequently compelled a shift in these activities towards the online sphere. Qiang, a police officer, held:

> When we talked about crime in the past, we mainly indicated violent crimes such as robbery. Twenty years ago, maybe when your father was about your age, who hadn't been robbed on the street? However, today street-level surveillance is so intense. If you steal a wallet on this street, you won't even be able to run to the next street before you

> get arrested. The risk of arrest is so high that traditional criminals can hardly survive (GD-P-22).

In keeping with Qiang, Hanling, another police officer, added:

> The surveillance in our city has improved significantly. First, the definition of CCTV has improved, and its coverage density has increased. Second, the facial recognition system has also been implemented. Thus, traditional street crimes have little room to survive. Gradually the number of cases has become less and less in these years (GZ-P-4).

Furthermore, Siwen's experience provides support for the above arguments. A police officer in an anti-cybercrime department, Siwen claimed: "I was at the department of anti-theft, anti-robbery and anti-vehicle crimes. However, the whole department is now dismissed because these crimes are almost extinguished (GX-P-3)." The above statement is in line with the work report of the Supreme People's Procuratorate in 2020, which showed that the number of street crimes had dropped significantly in recent decades. From 1999 to 2019, the number of individuals prosecuted for crimes that seriously harm social order decreased from 162,000 to 60,000, with an average annual decrease of 4.8% (The Supreme People's Procuratorate of the People's Republic of China, 2020).

To compare, cybercrime seems to have become one of the most popular options for traditional criminals during the transition process. As the Supreme People's Court of the People's Republic of China's report showed (2022), from 2017 to 2021, the number of cybercrime cases rose year-on-year in China by 51.18%, 28.43%, 20.9%, and 104.56% respectively, and approximately 40% of these cases were cyber fraud. Among other cybercrimes, the feature of having a low entrance hurdle, low risk, low cost, and relatively modest criminal consequences makes cyber fraud so attractive to traditional criminals, especially those who already have experience in committing fraud (GX-P-2, GD-P-4, GD-P-5 GD-P-10, GX-P-3, GZ-P-10). Siwen wrote:

> Cyber fraud has a very low entrance hurdle. Setting aside the degree of its complicity, criminals can find modus operandi online. Once the modus operandi is found, what criminals need to start the crime is simply some friends and relatives. Also, the profit of cyber fraud is extremely high. It sometimes even overcomes drug distribution. A case our department tackled involved more than a thousand million Chinese yuan, and the cost was simply some phones and some SIM cards. This is why there are so many traditional criminals who have stopped committing theft, running casinos, and selling drugs, but have started committing cyber fraud instead. Since they are making illegal money anyway, why not choose cyber fraud that has a lower cost, lower risk, and no death penalty even if they get arrested by the police (GX-P-3)?

Daihui, a police officer, provided an example of a village transitioning from a hotspot of hosting casinos to one of cyber fraud:

> This thing [cyber fraud] is like drug dealing. On the one hand, it has something to do with the local atmosphere of 'reaping without sowing'. On the other hand, it is associated with the existence of many idle young people... In this case, even if there wasn't the Internet, people would do something else, like hosting casinos or something. Oh, this reminds me, one of the villages in our town that is famous for cyber fraud used to be well known for hosting a casino (GD-P-5).

On the whole, advanced digital technologies used to detect traditional crimes have reduced opportunities for traditional crime, pushing individuals who would have committed traditional crimes towards cyberspace. Due to its low barrier of entry, minimal risk and cost, as well as moderate legal penalties associated with cyber fraud, it has become a prevalent choice for cybercriminals lacking technical expertise. This could be a primary factor that is contributing to the current cybercrime landscape in China.

3.2 The Issue of Personal Data Protection

The surge in personal data generation in China, coupled with inadequate public awareness and legislation around data protection, has significantly expanded opportunities for cyber fraud. Digital technologies, such as quick response code technology, data mining and face perception, are extensively used in business today in China. The commercialisation of these

technologies has generated a large amount of personal data (SX-P-1, GD-CSP-1, GD-P-4, GD-P-10, SX-H-1, SX-H-2, SX-H-3, SX-H-5, SC-H-1). These data can be used for a variety of purposes, spanning from legitimate to semi-legitimate, and for illegal activities, including promotional campaigns, private detective services, and, inevitably, fraudulent activities. With the utilisation of personal data, the success rate of cyber fraud significantly increases: cyber fraudsters are not only able to target certain groups of victims who are more likely to fall for their scams; they can also tailor their scams to specific individuals using their names, citizen numbers, social relationships, and even recent activities (LECID-9, SX-H-1, SX-H-2).

However, public awareness of personal data protection is rather low in China. A large portion of individuals seem to be unaware of the need to protect their personal data. The following interesting interaction between a former hacker, Haoming, and a taxi driver illustrates this point. Speaking to me in a taxi of how data protection is an issue in China, Haoming said:

> You know how those shared power banks ask for access to your personal data when you scan the QR code to borrow them, right? I doubt that most companies setting up these power banks ever implement measures to protect your data. That power bank we just saw might be holding millions of personal data records, and they might have been stolen many times (SX-H-3).

The taxi driver sitting at the front overheard our conversation, turned his head back and said to us, "Don't worry about it. You are thinking too much. It is not going to happen!" "OK," Haoming answered.

The example provided by police officer Mandong also reflects this issue. He noted:

> I learned yesterday that in other cities – because we have a colleague from out of town – his mother encountered a situation where a merchant was holding an event, and many people joined. The merchant said, 'Come over, do a little thing, and we'll give you some small gifts.' And how did they do it? They asked you to register SIM cards and gave the cards to them. They promised you the process was free and that they would cancel the

> SIM cards after three months. All you had to do was present your citizen identity card and sign an agreement (GZ-P-9).

Engaging in the event, the participants unwittingly handed over their personal data, which included their full names, associated identification numbers, and dates of birth. These personal data and the registered SIM cards can be subsequently sold on the illicit market for cybercrime. The popularity of the event suggests a common lack of awareness of personal data protection among individuals in China.

Companies, too, have the same issue. Cybersecurity seems to be often neglected by commercial companies in China (GD-CSP-2, SX-H-3, SX-H-4). Haoming and Qinglan, two former hackers, believed that most small companies do not employ cybersecurity practitioners, so hackers can easily break into the companies' systems. Therefore, stealing personal data from small companies and selling it on the criminal market has become a profitable business for many Chinese hackers (SX-H-3, SX-H-4).

Due to the general lack of public awareness concerning data protection in China, acquiring personal data proves to be relatively straightforward. As demonstrated in the examples above, personal data can be obtained either through technical means online or non-technical approaches offline.

Additionally, legislation regarding personal data management, protection, and use has lagged far behind in China. As Geller (2020) pointed out, the Chinese data protection regime has suffered from several deficiencies, including a lack of unified law, an absence of clear definitions, and a lack of a central authority to monitor the responsibilities and enforce the law. These problems have only started to be solved by enacting The Data Security Law of the People's Republic of China in 2021. As a result, a considerable amount of personal data has been collected by various public and private institutions. Kaile, a police officer, wrote:

> Nowadays, the invasion of privacy in China is a prevalent thing. It is very likely that the apps on your phone have already collected a lot of your personal data, including your location, your dial history, your messages, and even your photos and videos. You are essentially living in a glass house in this digital society. Also, if you visit a real-estate website and put down your phone number, and then search for a pair of shoes on an online marketplace, you will soon find out that the information about real estate and shoes is all over the place on your browsers and apps. That is because these companies have collected your personal data without your permission (SX-P-1).

The collected personal data by these institutions are then sold to the market for numerous legal or illegal purposes, such as business promotion, private detective services, and most often fraud (HEB-P-1, GD-P-4, GD-P-10, GZ-P- SX-H-1). Given that the legal framework in China concerning personal data protection, along with its enforcement, is not comprehensive, certain companies and institutions might even sell such data openly. As a police officer, Zhimei, wrote:

> I found several industries where the selling of personal data is particularly prevailing: vehicles, real estate, stock exchange, and insurance. I guess that is because the personal data collected by those companies are more precise. Many personal data sold online are from these industries. However, a lot of personal data are sold offline. You put down your information at the reception, and they may sell it at the back door right after you leave. I have seen some personal data sold as an Excel spreadsheet, printed, and on the top of the sheets, the companies' names were still on it [suggesting that the data were sold offline directly by the companies] (GD-P-10).

In line with Zhimei, Ruimin, a director of a police station in a small town in Guangdong Province, added that personal information is even easier to get in small towns because most people there have limited knowledge about IT and therefore have no idea what their personal data can be used for (GD-P-4).

Consequently, the rich amount of personal data, the lack of public awareness, and the lack of legal protection lead to the proliferation of personal-data businesses in China. Participants in this market include not only hackers who acquire personal data through

technical means but also include other individuals who acquire personal data from the public offline. While the rise in personal-data business fuels cyber fraud, the increasing prevalence of cyber fraud concurrently generates more demand for personal data, thereby also stimulating the growth of the personal-data business.

3.3 The Under-regulated Telecommunication Sector

Like personal data protection, the telecommunication sector in China also suffers from a lack of regulation. It mainly concerns machines that are often misused by cybercriminals to conduct cyber fraud. Cyber fraudsters often exploit a specific type of machine that enables them to make phone calls with multiple SIM cards, using only a phone or a computer. By setting up the machines remotely, they are able to hide their location so that criminals can communicate with each other and their victims in a relatively safe way (GZ-P-4, GZ-P-9, GZ-P-10). The use of these machines is legal in China, and many commercial firms such as travel agencies use them to run their businesses (GD-P-2, GZ-P-4, GZ-P-10). Hanling, a police officer, said:

> Many machines can be used for legal purposes. For example, I have a lot of SIM cards. To make my life easier, I don't want to use so many phones. So, I use a machine, download an app, connect it to the Internet, and put all my SIM cards on this machine. This kind of machine is totally legal, and you can buy it online. The function it achieves is just to enable you to make phone calls remotely using different phone numbers...There is another type of machine that even allows the SIM cards and the machine to sit in different locations. This is mainly used by travel agencies (GZ-P-4).

However, a lack of regulation to prevent these machines from being misused by criminals becomes a serious issue, as policeman Ruoxun said:

> These machines are widely used by travel agencies, especially those with business aboard. These agencies either provide remote calling services or use the machines themselves. Call centres also need these machines to run their businesses. Theoretically, the parties should have professional certifications to sell and buy these machines. But I

> have doubts about the examination process. There is also another problem. People may buy these machines sneakily from companies that have certifications and do something illegal (GZ-P-10).

It is unclear what regulations should apply to deal with these situations and what punishments can be applied to violators. It is also unclear which department is supervising the transaction of these machines and enforcing the regulations (if there are any). What the police often do when they find that suspects of cyber fraud are ordering these machines is intercept them. Nevertheless, police interception not only causes direct loss to the manufacturers and the distributors of the machines but also leads to a dramatic increase in product price, which subsequently imposes burdens on the legitimate companies using them. Hanling said:

> We have intercepted two SIMBOX [a machine containing multiple SIM cards from various mobile operators] this month. They were sold online and used to be very cheap, about 200 to 300 yuan for each machine. It now becomes 700 yuan...Interception has problems. The manufactories complain to us all the time, saying that they are selling these machines online legally. Because the products were intercepted by us and cyber fraudsters did not receive them, they made claims on the online platforms and asked for a refund. As you can see, the final victims are the manufacturers and the distributors (GZ-P-4).

The police have realised that there has been business in the telecommunication sector. However, law enforcement found that there was a lack of suitable regulations and laws to define many activities, such as selling, renting and letting machines. Consequently, stopping these businesses becomes a big challenge (GZ-P-10).

Insufficient regulation in the telecommunications sector has given rise to numerous businesses operating in legal grey areas, which in turn facilitates cyber fraud activities. As a result, individuals who are not inherently cybercriminals are drawn into the cybercrime industry, contributing to its rapid growth in scale.

3.4 The Proliferation of Mobile Payments

Mobile payments have become increasingly popular in China. A report published by China UnionPay (2022) revealed that in 2021, mobile payments accounted for approximately 80% of the monthly consumption total among those surveyed in the most economically developed cities, with the average monthly consumption exceeding 5,300 yuan. In smaller cities, mobile payments even made up over 90% of the monthly consumption total, with an average monthly consumption of approximately 3,200 yuan.

The widespread adoption of mobile payments in China has mainly accelerated cybercrime by enhancing the efficiency of money laundering. By using mobile payments, cybercriminals can easily disperse money across numerous bank accounts with a few mobile phones. This money dispersion process makes it difficult for law enforcement to trace the money (GD-P-20, GX-P-1, GX-P-3, GZ-P-8). Furthermore, third-party payment systems like Alipay and WeChat Pay are commonly used mobile payment methods in addition to bank transfers. With the assistance of these third-party payment platforms, the process of money laundering becomes even more covert (GD-P-20).

The convenience of the money laundering process facilitated by mobile payments also enables the emergence of specific money laundering services that exploit the concept of crowdsourcing. This way, a wide range of individuals have been attracted to the business of money laundering. The most notable example is the 'point-running platforms' developed by money laundering groups. In essence, point-running platforms allow users ('point runners') to upload their bank account numbers and the QR codes of their third-party payment platforms, such as Alipay. The money laundering groups then provide these bank account numbers and QR codes to cyber fraudsters to receive the money transferred from the victims and use them as a part of the money-laundering process. The point runners earn a commission base on the amount involved in each transaction. They are required to pay a

deposit that equals the money they will receive before the transaction. Money laundering groups often portray the platforms as part-time earning platforms in their advertising. As such, many point-runners are unaware that they are assisting money laundering schemes (SC-H-1, GZ-P-8, CSCR-3; Fang, 2021). The crowdsourcing model adopted by the money laundering groups also exists in several different forms, such as P2P (peer-to-peer) currency exchange platforms (GD-P-22) and digital currency exchange platforms (GD-PST-5) with the same idea.

4. Challenges in Controlling Cybercrime

China has a reputation for having a distinct internet infrastructure, which features a strong online surveillance system. The internet infrastructure, however, does not seem to function as well as it should in theory. This section analyses the practical challenges to the Chinese government and explains why the internet infrastructure and the state intervention in recent years have not been effective enough to contain cybercrime.

First, it is challenging to make the online surveillance system fully function in practice. On the one hand, there are many ways to evade the control of the real-name registration system. Criminals may buy or rent SIM cards, credit cards, and national identity cards from others. With these materials, criminals can create online accounts using other people's identities (GZ-P-10, GD-P-19, GX-P-3, GD-P-15). Therefore, officer Youpu concluded, "the real-name registration system is not real" (GD-P-19). Moreover, the burden of checking user identities is placed upon online service providers. Since strictly checking user identities brings little revenue to their business; there is little motivation for service providers to do it, as Rouxun said:

> Considering you are a landlord who has a lot of empty apartments to let, you may concern yourself more about letting your apartment than the regulation. When a guy shows up with a national identity card, you may simply glance at the card, and will not bother carefully examining whether they are really the same person (GZ-P-10).

The inadequacy of the real-name registration system compromises the effectiveness of online surveillance, thereby significantly reducing the risks associated with illegal online collaboration. As will be discussed in a subsequent section, a substantial amount of online collaboration between Chinese cybercriminals still occurs on local internet platforms. On the other hand, VPN providers have been constantly trying to evade the government ban through technical means, such as disguising their VPN connection methods. Therefore, the fight between the Chinese government and the VPN providers has become a 'cat and mouse' game, making it challenging to completely block VPN access (GD-CSP-1, SX-H-1). Consequently, the online surveillance system in China is not as robust in practice as it is in theory.

The second issue is the lack of resources within law enforcement. Participants from law enforcement noted that there is more content on the Internet than the human resources of the police force can handle. It is therefore almost impossible for police in China to monitor everything (SX-H-1, GZ-P-4, GZ-P-10, GD-P-20). Hanling, a police officer, wrote:

> Our police station cannot handle cybercrime well. It is not because we don't have the skills, but it is because we don't have enough people. There are only a few people in our anti-cybercrime sector. Think about it, this year in our region there are 1,500 cyber fraud cases, and we have only three people…These are only cyber fraud cases, and I haven't counted the cases that involve cybercrime products, online political events, and other cases that we are told to solve by our boss…We simply can't handle that many cases (GZ-P-4).

In line with Hanling, Rouxun, another police officer, put: "If I have to check the identity each time of someone saying that he was looking for a part-time employee […] in a QQ group, can you imagine how much work I would need to do? This is simply not realistic"

(GZ-P-10). Similarly, investigating VPN usage is also a highly resource-intensive task, and so the police tend to turn a blind eye to it. The lack of resources within law enforcement further undermines the efficiency of online surveillance and the state's control over online cybercrime activities.

Third, cybercriminal activities span across the jurisdiction of numerous companies and departments, including IT companies, telecommunication companies, banks and the police. A lack of coordination among various stakeholders has notably undermined the effectiveness of cybercrime control. For instance, Siwen, a policeman from Guangxi Province, complained that he often had to travel to different technology companies to extract evidence when investigating cybercrime cases. This process comes with considerable time and monetary costs and therefore reduces the police's capacity to handle a large volume of cybercrime cases effectively. He also complained that the banks were often reluctant to freeze their customers' bank accounts, as frequently freezing bank accounts can disrupt regular business transactions and potentially lead to complaints from customers. As a result, cybercriminals are often able to move around the money before the accounts are frozen by the banks, and the victims can hardly claim their money back (GX-P-3). Similar complaints have been reported by several police officers nationwide, suggesting that this difficulty is prevalent among law enforcement agencies (GZ-P-4, GZ-P-9, SX-P-1, GD-P-7). The conflict of interest among stakeholders and the resulting lack of a coordinated response forms a huge challenge for the state to contain cybercrime as a whole.

Overall, while the online surveillance system may force cybercriminals in China to invest more in navigating ways around it, the internet infrastructure in the country is not as stringent as theoretically proposed. The state's capacity to control cybercrime has also been

impeded by several practical constraints. This incapacity provides the soil for cybercrime to survive and proliferate in China.

5. Conclusion

In summary, this chapter provides the background context for the cybercrime industry in China. It shows that the cybercrime industry in China is mainly constructed around cyber fraud. A series of criminal activities, such as scam-promoting, communication transmission support, and money laundering exist to support the successful operation of cyber fraud. After probing the prevalent cyber fraud scams in China, the chapter examined the socio-economic drivers that influenced the current landscape of the cybercrime industry. On the whole, the existing social structure has failed to keep pace with the rapid socio-economic developments of recent years, leading to the rise of cyber fraud and related cybercrimes. These cybercriminal activities, bolstering each other, have grown in scale and in turn have fostered the overall development of the local cybercrime industry. On the other hand, while not fully denying its effectiveness, the online surveillance system in China does not appear to be as strong as it is in theory. This, coupled with the practical constraints on law enforcement, including a lack of human resources and difficulties in collecting evidence, has weakened the state's capacity to control cybercrime. As a result, while the internet infrastructure may compel cybercriminals to invest more in evading state surveillance, cybercrime operations in China are not markedly different from other countries.

Chapter 4. The Actors

The previous chapter provided some contextual insight into the Chinese cybercrime industry and demonstrated that it is primarily structured around cyber fraud. Relying on the empirical data, including the 6,686 court judgments made between 2014 and 2019, the present chapter delves into the actors within the cybercrime industry, who are the fundamental building blocks of Chinese cybercrime. The aim of this chapter is to provide a clear picture of the actors in the cybercrime industry, covering their characteristics and in what form they interact and cooperate. This chapter posits that the actors in the cybercrime industry are highly specialised and professional. However, many of them are not IT talents as one might expect, and share much resemblance to the common image of conventional criminals. Moreover, similar to conventional criminals, cybercriminals cooperate through both markets and firms.

This chapter is split into four sections. The first section inspects the characteristics of the cybercrime offender within the industry, sketching a portrait of the cybercriminals, and showing the existence of specialisation and professionalisation among the offenders. The second and third sections examine the degree of specialisation and professionalisation respectively. The fourth and final section examines how criminal actors in China interact and cooperate, arguing that both horizontal market transactions and vertically integrated cybercriminal firms exist within the industry.

1. The Characteristics of Cybercriminals

By referring to the empirical evidence, this section first provides an overview of the characteristics of cybercriminal offenders in China. Table 1 summarises the criminal

activities brought to the court, as provided in the court judgments. Compared to the criminal sentences, this information is more accurate in reflecting on the actors' criminal activities. For instance, a criminal who is engaged in forging company stamps may be sentenced under the charge of fraud or assisting cybercrime. Echoing the last chapter, this table suggests that a variety of activities are conducted by cybercriminals in China to support the crime of cyber fraud. These activities are directly linked to the different actors in the cybercrime industry. For example, improper credit card usage, concealing crime-related income, and harbouring criminals can be linked to water houses and drivers; trading personal information and illegally acquiring personal information can be linked to material dealers; telecommunication facility sabotage may refer to machine maintainers; illegal business operations and assisting cybercrime can be linked to other activities that are difficult to define, such as providing draining services. Notably, there were a significant number of criminals who conducted multiple activities. This indicates the existence of multifunctional criminal groupings, such as a fraud group that has teams that conduct hacking, forging, scamming, and money laundering.

Table 1. Activities Brought to the Court

Activities	N
Fraud	14670
Improper Credit Card Usage	364
Multiple Criminal Activities	325
Concealing Crime-related Income	220
Trading Personal Information	199
Illegal Business Operations	129
Hacking	97
Telecommunication Facility Sabotage	67
Harbouring Criminals	51
Forging Official Documents	32
Illegally Acquiring Personal Information	30
Forging Financial Instruments	16
Assisting Cybercrime	13
Forging Company Stamps	10
Forging Currencies	6
Forging/Trading Citizen IDs	6
Sum	16235

As shown in Tables 2a and 2b, the minimum age of cybercriminals at the time of offending was 16 years and the maximum was 67 years, with the average age being 29.9 (N=16235). The age distribution is left-skewed. Over half of the offenders are in the 21–30 age group and about a quarter of the offenders are in the 31–40 age group for both genders. The offenders are predominantly male (89.2%, N=14489), with only a small number of females (10.8%, N=1746). The likelihood of participating in cybercrime drops significantly after the age of 41.

The gender distribution and age curve are generally in accordance with most of the research on traditional crime, where the age curve is left-skewed with a spiked young-age peak and a decline into old age. Yet the lower peak for cybercrime commitment also appears to be higher than what can be found with traditional crime, as points relating to traditional crims were usually around the age of 20 to 30 (Hirschi & Gottfredson, 1983; Cohen & Land, 1987). While admitting that the arrest rate can have a significant impact on the age curve (Marvell & Moody, 1991; Steffensmeier et al., 2017), this could be due to

the fact that cybercriminal operations require less physical ability. Therefore, age has less of an impact on the criminals' capability to commit cybercrime.

Table 2a. Offenders by Age

	Minimum	Maximum	Medium	Mean
Age (N=16235)	16	67	29	29.9

Table 2b. Gender and Age Distribution of Offenders

Age Group	Female	Male	Sum
16–20	30 (0.2%)	317 (2.0%)	347 (2.1%)
21–30	962 (6.0%)	7892 (48.6%)	8854 (54.5%)
31–40	538 (3.3%)	4701 (29.0%)	5239 (32.3%)
41–50	169 (1.0%)	1289 (8.0%)	1458 (9.0%)
51–60	39 (0.2%)	265 (1.6%)	304 (1.9%)
60+	8 (<0.1%)	25 (0.2%)	33 (0.2%)
Sum	1746 (10.8%)	14489 (89.2%)	16235 (100.0%)

As shown in Table 3, 93.0% (N=16235) of the cybercriminals did not have any history of crime or public order violation. As for offenders with records, most of these had previously committed fraud. However, it is unclear how many of these records were for committing cyber fraud. Following fraud, criminals with a history of violent crimes, theft, and drug-related activities were the second largest group. There is also a significant number of criminals with records of forgery, which is an essential skill for conducting cyber fraud. These numbers support the argument made in the previous chapter that cybercrime has become a lucrative criminal industry that attracts many traditional criminals. However, according to the court judgments, the majority of known cybercriminals in the Chinese cybercrime industry have no record of crime or public order violation, suggesting that there is a lack of direct involvement of traditional organised crime groups (OCGs) in cybercrime, as criminal records and prison experience are often deemed to be an important prerequisite for joining OCGs (Gambetta, 2009).

Table 3. History of Crime and Public Order Violations

Record	N	%
Fraud	337	2.1
Violent Crimes	233	1.4
Theft	200	1.2
Drug-related Activities	141	0.8
Unlawful Business Operations	77	0.5
Forgery/Trading Counterfeit Products	70	0.4
Vehicle-Related Crimes	29	0.2
Sexual Crimes	14	<0.1
Illicit Lumbering	12	<0.1
Assisting Crimes	12	<0.1
Corruption-related Crimes	8	<0.1
Trading Personal Information	4	<0.1
Multiple Records	16	<0.1
No record	15082	93.0
Sum	16235	100.0

Tables 4a and 4b provide the education level and occupation of the offenders. According to the tables, the average level of education of cybercriminals is low: fewer than 5% of the 16235 offenders had degrees. Almost half of the offenders (49.1%) only acquired secondary-school-level education, and around 15% of them had even lower education levels. Correspondingly, there is a significant number of offenders who were unemployed at the time of committing the crime, which accounts for 46.1% of all offenders. As for other offenders who were employed, most of them did not have a permanent job: 10.1% worked part-time and 3.8% were self-employed. Of offenders who had a relatively steady job, 6.3% of them were migrant workers who had suffered from a general lack of certainty, discrimination, and rights deprivation (Myerson et al., 2010; Chan & Siu, 2012).

Surprisingly, 22.1% of the offenders were farmers. There are two possible explanations for this. First, in judicial practice, law enforcement, prosecution and the court in China may sometimes mark jobless individuals, who live in rural areas and are belong to agricultural

households (农业户口)[11], as farmers. There is also the lack of a clearly defined boundary between farmers and migrant workers, as the latter term often refers to agricultural households who seek employment (often unstable) opportunities in urban areas. Because of the instability of their employment, migrant workers who are temporarily not working may also be classified as farmers (GZ-P-12, GD-P-20). Second, farmers who have limited knowledge of technology and legal awareness are often employed by cybercrime groups to conduct activities that assist criminal operations. An article provided by Hu (2020), a newspaper publisher in China, reported that farmers are largely employed by cybercrime groups for illicit activities such as cashing out, bank account dealing, and promoting. This report is supported by several interviews (GD-CSP-3; GZ-P-8; GD-P-20; SX-P-1) and court judgments. For instance, in *Su Lianpei re Fraud*[12]*,* the offender was a farmer. He was employed by a cyber fraud group to cash out their criminal proceeds. Interestingly, the offender in the case was 56 years old, one of the few older criminals found in the dataset, and the cyber fraud group that employed him was formed by his son and daughter-in-law. The involvement of family members in cybercriminal groups will be further discussed in Chapter 6.

Overall, the distribution of education level and occupation of the cybercriminal offenders appear to suggest that there is a large degree of professionalisation within the cybercrime industry, with numerous criminals relying on cybercrime as their primary occupation or as a substantial source of revenue.

Table 4a. Distribution of Education Level of Offenders

Education	N	%
Postgraduate	28	0.2
Undergraduate	735	4.5

[11] A special type of household within the *Hukou (户口)* system in China. See Chan & Zhang (1999), Cheng & Selden (1994) and Song (2014) for more details of the *Hukou* system.
[12] 苏连培诈骗罪一审刑事判决书, (2019)闽 0481 刑初 196 号

Technical diploma	1493	9.2
High school	1943	12.0
Technical high school	1601	9.9
Secondary school	7973	49.1
Primary school	2376	14.6
Uneducated	86	0.5
Sum	16235	100.0

Table 4b. Occupation Distribution of Offenders

Occupation	N	%
Teacher	18	0.1
Government official	52	0.3
Entrepreneur	219	1.3
Self-employed	615	3.8
Migrant Workers	1019	6.3
Company Employees	1480	9.1
Part-time Workers	1751	10.1
Farmer	3595	22.1
Unemployed	7486	46.1
Sum	16235	100.0

Table 5a and Figure 1 illustrate the geographic distribution of the offenders at the provincial level. Offenders are widely distributed among the Chinese provinces[13]. Tibet is the only province where no cases were reported between 2014 and 2019. A potential explanation could be that the economic development in Tibet is rather low. Tibet ranked last of all 31 provinces in China in terms of GPD in 2022. Moreover, the general level of internet information technology is very low there (Chen & Palaoag, 2022).

The overall distribution generally coincides with the level of economic development: there are significantly more offenders in the top 10 provinces in terms of overall GDP in 2022 such as Guangdong (8.3%), Henan (9.1%), Hubei (8.4%), and Fujian (15.0%). Nevertheless, outliers exist. Although Guangxi (5.5%) and Hainan (4.6%) have relatively low levels of economic development, many cybercriminals reside there. In fact, the interview data also suggest that there were several cyber fraud hotspots in Guangxi and

[13] Including five autonomous regions and four municipalities directly under the jurisdiction of the central government, but excluding Hong Kong and Macau, as they are in separate jurisdictions. The GDP data is provided by *Jiang* (2023).

Hainan Provinces (GD-PST-4, GD-CSP-3, GD-CSP-4, SX-P-1, GX-P-2, GX-P-3). While criminals in Guangxi were famous for conducting QQ impersonation scams (GX-P-2, GX-P-3), criminals in Hainan were well known for conducting Airline ticket refund scams (GD-CSP-3, GD-PST-4). At the opposite end, there are far fewer offenders in provinces with a lower level of economic development, such as Gansu (< 0.1%), Ningxia (< 0.1%) and Qinghai (< 0.1%). The reason why there are overall more cybercrimes in economically developed provinces could be because these provinces have better cybercrime "infrastructure", which includes not only the physical system (i.e. the Internet development) but also the availability of human resources to provide cybercrime-related services (Collier et al., 2021). For instance, it is perhaps easier to recruit a hacker in cities in Guangdong province than in Qinghai province, as there is not only a worse internet connection in the latter province but also a general lack of individuals who know about cybercrime and the Internet.

At the city level, however, the spatial distribution does not correlate with the level of economic development. As can be seen from Table 5b, most cybercriminals resided in relatively economically underdeveloped cities: over 50% of cybercriminals domiciled in Tier 3 and Tier 4 cities instead of the top tier cities[14]. A possible reason could be that these cities are big enough for cybercriminals to hide in – they can rent spaces in office buildings and pretend to be legitimate companies, for example – and small enough to acquire protection from local government agents.

Table 5a Spatial Distribution of Offenders at the Province Level

Rank (Overall GDP in 2022)	Province	N	%	Rank (Overall GDP in 2022)	Province	N	%
1	Guangdong	1356	8.3	17	Liaoning	284	1.7

[14] The Tier system is widely adopted in China to classify the economic status of prefecture-level cities. The official classification is provided by the *Xin* (2022), which is a government-owned organisation.

2	Jiangsu	575	3.5	18	Yunnan	203	1.3
3	Shandong	536	3.3	19	Guangxi	899	5.5
4	Zhejiang	388	2.4	20	Shanxi	140	0.1
5	Henan	1485	9.1	21	Inner Mongolia	127	0.1
6	Sichuan	627	3.9	22	Guizhou	364	2.2
7	Hubei	1358	8.4	23	Xinjiang	26	<0.1
8	Fujian	2376	15.0	24	Tianjin	106	<0.1
9	Hunan	1166	7.2	25	Heilongjiang	413	2.5
10	Anhui	715	4.4	26	Jilin	250	1.6
11	Shanghai	62	<0.1	27	Gansu	55	<0.1
12	Hebei	614	3.8	28	Hainan	754	4.6
13	Beijing	107	0.6	29	Ningxia	27	<0.1
14	Shaanxi	238	1.5	30	Qinghai	6	<0.1
15	Jiangxi	672	4.1	31	Tibet	0	0
16	Chongqing	306	1.9	**Sum**		16235	100.0

Note. Beijing, Shanghai, Tianjin, and Chongqing are four municipalities directly under the jurisdiction of the central government. They have the same administrative division as provinces.
Source: *Jiang, 2023*

Table 5b. Spatial Distribution of Offenders at the City Level

City level	N	%
T1	449	2.8
Semi-T1	1667	10.3
T2	2935	18.1
T3	4018	25.0
T4	4133	25.5
T5	1959	12.1
County level	1074	6.7
Sum	16235	100.0

Source: *Xin,* 2022

Combining the above data together, a criminal portrait for reported offenders can be sketched. Most of the offenders are socially disadvantaged individuals with a medium-to-low level of education and no history of crime or public order violation. They commonly live in small cities and economically developed provinces. Furthermore, the data suggest that these offenders possess specialised skills to commit crime, even if those skills are not technical in nature. The majority of them also appear to be professionals who depend on cybercrime as their main job or as a significant source of income. The following two sections further probe into the degree of specialisation and professionalisation among these actors.

2. Role Specialisation in the Cybercrime Industry

Stemming from the empirical evidence, the value chain in the Chinese cybercrime industry is exceptionally extensive, and the number of participating parties is substantial. Drawing upon the empirical data, this section examines the degree of specialisation within the industry. The primary actors within the cybercrime industry are identified as follows.

SIM card dealer. SIM card dealers are one of the core actors in the cybercrime industry. Under the real-name registration system in China, citizen ID must be presented at the counter of the business hall when purchasing SIM cards (Cybersecurity Law of the People's Republic of China, 2016, s.24; Provisions on the Registration of True Identity Information of Telephone Subscribers, 2013, s.3; s.5; s.6). The rationale behind this regulation is to ensure every phone call is traceable and locatable to an individual by the police for public management and criminal investigation reasons (Lee & Liu, 2016). However, as Yanse said, in reality, there were countless phone numbers in the police tracking system with incorrect information or with no information at all. The numbers are called ‘black cards’ by the police (GZ-P-10, GD-P-20). There were various sources where these black cards could possibly come from. Some may be leaked by insiders of mobile telecommunication companies. For example, when a customer registers phone numbers at the counter, the teller may register an extra SIM card covertly with the provided ID information and sell it (GZ-P-10, GD-P-20); others may be purchased from individuals, such as university students who want to earn extra money (GZ-P-4), people who are living in extreme poverty (GD-P-2), and senior adults who live in the countryside and who are unaware of the risk of selling their SIM cards (GZ-P-9, GZ-P-11, SX-P-1). Collecting black cards from various

different sources and selling them in packs is the main business of SIM card dealers. There are many potential customers of SIM card dealers who need black cards. For instance, in legal sectors there are telemarketers who need to change their phone numbers regularly to prevent being blocked by potential customers (GZ-P-12); in illegal sectors, there are cyber fraudsters who wish to conduct cyber fraud with black cards directly, and there are SMS verification platforms that use the phone numbers to conduct online-account-registration business (SX-H-1, GD-P-20, GZ-P-12).

SMS Verification Platform. The short message service (SMS) verification platforms run their business to help people to register different Social Networking Service (SNS) accounts. Under the real-name registration system in China, not only SIM cards but all online accounts must be bound to citizen IDs (Cybersecurity Law of the People's Republic of China, 2016, s.24). In practice, this is done via SMS verification. By linking the online SNS accounts to offline phone numbers, which are supposedly connected to citizen ID cards, the real-name system seeks to take public control over the virtual space as well as the offline dimension. However, just like there are black cards, there are also 'black SNS accounts'. By purchasing large numbers of black cards from SIM card dealers, the SMS verification platforms are able to provide services online for whoever wants to register black SNS accounts, by giving out phone numbers under their control and returning the verification codes received by their phones (Lee & Liu, 2016).

Account Dealer. Account dealers are the biggest customer of the SMS verification platforms. Similar to SIM card dealers, they do business by registering SNS accounts and selling them in packs (CSCR-5). Moreover, in order to make the accounts akin to ordinary accounts used by normal online users and to avoid the detection system adopted by the

SNS platforms to detect suspicious accounts, the account dealers often also conduct ‘account farming’ after registration. Such activity includes regularly posting content that matches the online identity created by the SNS account, to make it ‘look real’ (GX-P-1, GZ-P-6, LECID-2). After a period of account farming, the accounts are then sold to the customers. In addition, some account dealers also purchase stolen accounts directly from hackers at the same time. The benefits of the stolen accounts are not only to save time otherwise spent account farming but to serve as an important tool for excising scams that involve impersonating a victim’s acquaintance (SX-H-1). While some accounts collected by account dealers are sold to an ‘internet online army’ to conduct activities such as posting feedback on online commercial sites, some are sold to deal-hunters to stack up coupons or discounts, and most of the accounts are purchased by cyber fraudsters (CSCR-4; US-CSP-1, SX-H-1).

CAPTCHA Solving Platform. After acquiring account information, logging into an account to examine its status and check the accuracy of the password is essential to both the hackers’ and account dealers’ businesses. Since the parties are located in different geographical spaces with different logging equipment, CAPTCHA verification is often required while logging into the accounts. The CAPTCHA Solving Platforms have hence become popular for parties who want to quickly log into large numbers of accounts (CSCR-5).

Hacker. Most hackers are “essentially businessmen with IT skills” (SX-H-1). Although there are specialisms among hackers, at the end of the day, hackers go where "big money" is. And in recent years, "big money" has been found in the data business (GD-CSP-1, SX-H-1, SX-H-3, SX-H-5). Breaking into servers and websites is undoubtedly one direct way

of extracting data, and stolen SNS accounts are another valuable data source. For instance, a single SNS account may enclose data such as customary usernames, passwords, genders, ages, hobbies, and phone numbers (GD-CSP-1). On the one hand, these stolen data may be used to build a social engineer database that aggregates a large quantity of data from different individuals across a wide range, including name, job, SNS account, birthday, customary password and security question, to be used for future attacks or other business purposes; on the other hand, they may also be packed in different combinations and sold to various parties accordingly, such as marketing companies, casinos, private detectives and of course, cyber fraudsters. Nevertheless, most of the data are delivered to the parties through professional material dealers (SX-H-1, SX-H-3, SX-H-5). In addition, as in the above-mentioned case *Jin Huan, Li Rongkang, Sun Lei & Others re Concealing Crime-related Income,* some hackers also provide direct technical support to cyber fraudsters. Their services often include hosting VoIP servers – a technology that is often adopted by cyber fraudsters to enable them to make phone calls on computers and hide their call location, and develop and lend fraudulent websites or apps (GZ-P-10, SC-H-1, SX-H-5).

Material Dealer. Material dealers are often called 'agents' who collect various 'materials' that could be used to conduct crime (SX-H-1, SX-H-5, GZ-P-8, GZ-P-11). Materials sold on the market cover both online data and offline entities, and commonly include citizen IDs, bank accounts, bank cards with security devices, business licences, and other personal data (GD-PST-4). There are three main customers of the material dealers, all of whom need different materials: account dealers, cyber fraudsters, and 'water houses' – a commonly used name in China for money launderers (GD-P-2). For account dealers, filling in bank information for SNS accounts with citizen IDs and corresponding bank accounts can increase the creditability of the accounts and avoid detection more effectively,

thus subsequently increasing the value of the SNS accounts (SX-H-5); for cyber fraudsters, acquiring personal data such as victims' names, IDs and bank details enables them to conduct scams more effectively, and this acquisition is also essential for certain types of scam (GD-CSP-3, SX-H-5); for water houses, entities such as bank cards, USB security keys and business licences are all necessary tools for money laundering (GZ-P-8).

Account Problem Solver. For some of the interviewees, account problem solvers are new business entities that they "don't know how to define" (GZ-P-6, GZ-P-9). When the account dealers pass accounts into the hands of cyber fraudsters, they give instructions on how to avoid being detected and banned from the SNS platforms. For example, it is often advised by the account dealers that the user should not change the nickname or profile photo for a period of time, and that the user should also post content on the account on a regular basis. Nevertheless, most cyber fraudsters do not listen, and this leads to a lot of accounts being banned (GZ-P-9). The account problem-solving business has consequently arisen to help negotiate with the SNS platforms and to deal with the unblocking process online.

Cyber Fraudster. Cyber fraudsters are the main actors in the cybercrime industry. Most actors have risen and flourished in the industry because of the proliferation of scam operations in China over recent years (GD-CSP-2, SX-H-4). Although the modus operandi of the scams is sometimes rather simple, they are extremely risky and easy to tackle if each step is not done professionally. Hence, while lone wolves may still exist, most cyber fraudsters work in groups, with a division of labour (GD-P-19). Subject to the scale and variation of the cyber fraud groups, common roles include the investor, who is the organiser of the cyber fraud group; the manager, who oversees the scam operation and recruits

members; the chatter, who is responsible for chatting with the victims and luring them into transferring money; the technician, who helps with operating and maintaining software and digital devices, such as apps rented from the IT company; and logistics, who is responsible for collecting various tools and 'materials', such as SNS accounts, that are necessary for the scam (GD-P-19, HEB-P-1, GD-P-15). Some large-scale fraud groups also assign members to conduct money laundering to avoid police detection (HEB-P-1, GD-P-21). At the same time, cyber fraudsters may also seek help from other parties outside of their group.

Machine Maintainer. For scams that involve telephones, some cyber fraudsters choose to use machines such as SIMBOX, which contains a VoIP protocol and allows them to conduct phone calls remotely using a computer to hide their location (these machines are themselves legal in China and are used in many business sectors; they are however often exploited by criminals for malicious purposes) (GZ-P-4, GZ-P-9). At the same time, some cyber fraudsters also recruit machine maintainers to switch the SIM cards installed in the machines, maintain the machines, and change their location regularly to avoid detection by the police and therefore maximise their safety (GZ-P-9, GZ-P-10).

Drainer. Drainers are criminals who provide traffic-referral services to cyber fraudsters. They run their business by attracting potential victims and luring them to add a cyber fraudster's SNS account to their friend list (GD-PST-2, GX-P-2, GZ-P-6). Methods adopted by the drainers to attract victims are numerous. Common methods include publishing articles or news about investments with QR codes that connect to the cyber fraudsters' SNS accounts or conducting streaming to attract an audience and later inviting them to add the streamer's SNS account, which is in fact controlled by cyber fraudsters (GX-P-2, GZ-P-6).

Water House. As mentioned above, a water house is an alternative name for a group that provides money laundering services in China. One of the common money-laundering processes is to collect bank cards from material dealers and use them to dissemble the money. For example, a hundred dollars could be dissembled into nine lots of ten dollars and transferred into ten different bank accounts, and the remaining ten dollars could again be dissembled into ten lots of one-dollar payments and transferred into another ten different accounts. After repeating the process three to five times and mixing the money transfers with numerous daily expenses in each layer, the money originally paid from the victim becomes difficult to trace (GD-P-20, GX-P-1, GX-P-3, GZ-P-8). What's more, on top of the money dissembling, some water houses may add fake digital currency or virtual property transactions at certain stages to conceal it even further (GD-P-22, LECID-5).

Point Runner. Point runners are individuals who assist water houses in money laundering by making money transfers using their bank accounts or digital wallets such as WeChat Pay or Alipay (CSCR-3). Instead of purchasing bank accounts from material dealers and conducting the money-dissembling process themselves, some water houses develop 'point-running platforms'. In essence, these allow users ('point runners') to upload their bank account numbers and the QR codes of their mobile-payment platforms, such as Alipay. The money-laundering firms then provide these bank account numbers and QR codes to cyber fraud firms to receive the money transferred from the victims and use them as a part of the money-laundering process. The point runners earn a commission based on the amount involved in each transaction. They are required to pay a deposit equal to the money they will receive before the transaction (CSCR-3; GD-P-20, GD-P-22).

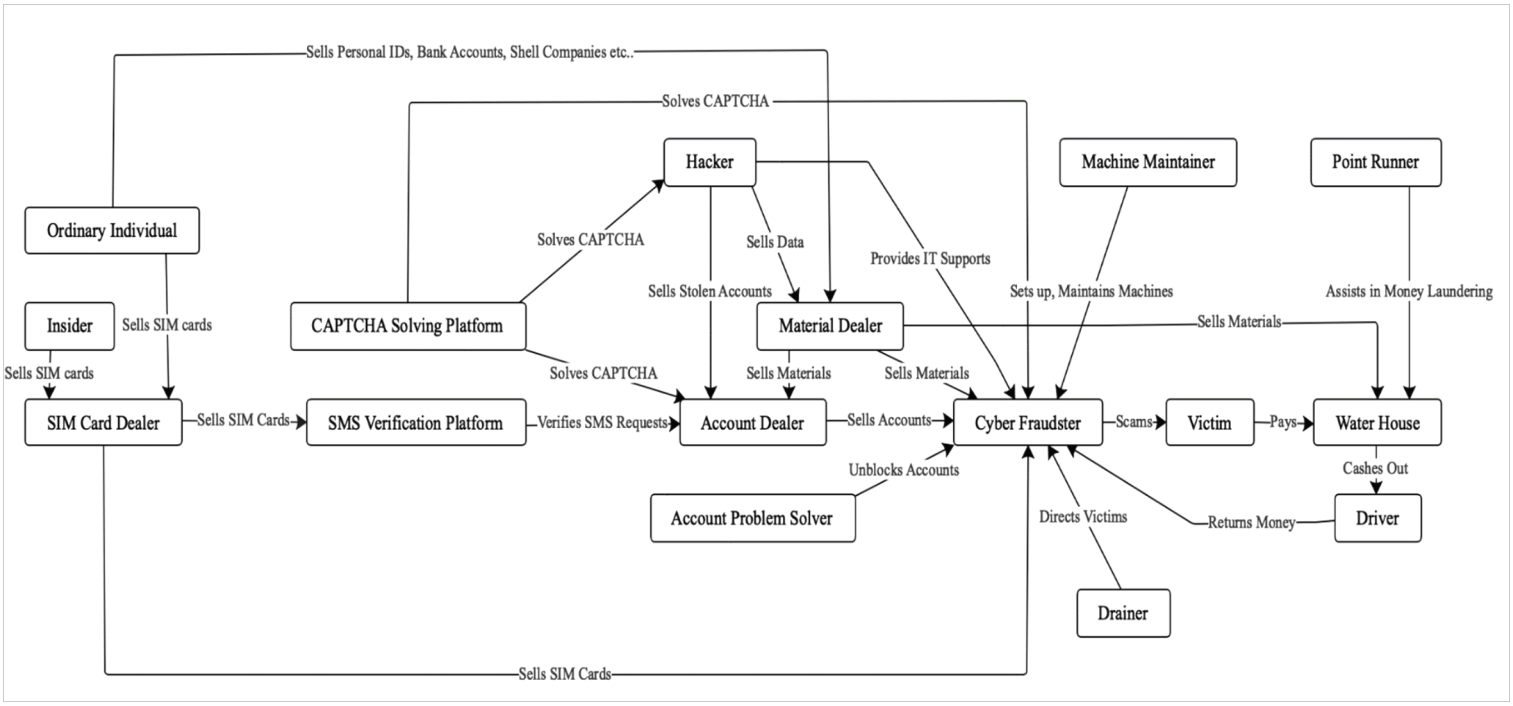


Figure 1: Actors within the Chinese Cybercrime Industry

Driver. In many money-laundering operations, 'drivers', also known as money mules or arrows (Leukfeldt & Kleemans, 2019; Lusthaus & Varese, 2021), are recruited to cash out the money that is assembled and transferred to various accounts. Drivers are often asked to collect money from ATM machines located in different locations and hand over the cash to cyber fraudsters (GX-P-3, GD-P-21).

Figure 1 summarises the actors introduced above and illustrates how this wide range of actors connect to form the cybercrime industry. What is shown in the figure is that there is a high level of specialisation among the actors within the cybercrime industry. What can also be seen from the above findings is that not all criminal actors are individuals with advanced technical skills. Most cybercriminal activities appear to have a low entrance hurdle and can be carried out by individuals without strong computing abilities. It should be noted that the actors introduced above are not exhaustive, and the list does not capture all criminals within the industry. The cybercrime industry is dynamic: what can be

observed now is already very different from how it looked in the recent past, and its features will surely change again in the future (HEB-P-1, GD-CSP-1, GD-PST-2, US-CSP-2).

3. Professionalisation

This section examines the degree of professionalisation within the cybercrime industry. In line with the evidence presented in court judgments, the interviews suggest that a significant number of cybercrime offenders are professionals, meaning that they commit cybercrime as a full-time job or rely on it as a primary source of income. Ruimin, the director of a police station, depicted many cybercriminals as jobless individuals who are "floating" on the street. While identifying criminal opportunities, they fully immerse themselves in exploiting them. Ruimin stated:

> People in the towns often gather on the streets and think about how to make money...These people are floating; what they do depends on where they land. If they land on a group that does drugs, they start selling drugs; if they land on a group that does fraud, then they do fraud. (GD-P-4)

Echoing Ruimin, Rubo, a Chinese cybersecurity practitioner who worked in the US also believed most cybercriminals are specialised professionals in China. He argued that it is the industrialisation of cybercrime that pushes cybercriminals toward professionalisation. Within the cybercrime industry, each specialised field of expertise, regardless of the technical elements involved, possesses complicated skillsets; "deal-hunting has its 'daodao' [tricks], credential-stuffing also has its ‘daodao'", said Rubo (US-CSP-1). These complexities present a challenge for amateurs attempting to contend against the professionals and survive in the criminal market.

The existence of a clear career path in many domains of expertise further underscores the extensive professionalisation embedded within the industry. Former hackers Haoming,

Sugar and Youlv pointed out the career path of hackers. One may begin a career as a freelancer or a member of a hacking group. After accumulating a certain level of social resources, they could assume the role of a group's 'exit' – the individual who accepts business orders and interacts with customers. Ultimately, they could even become a middleman, earning a livelihood by supplying information and enforcement services (SX-H-1, SC-H-1, SX-H-5). Similarly, a confidential investigation report reveals the career path of one cyber fraudster. Lang, the leader of a business unit comprising 41 members that was part of a larger cyber fraud organisation (the structure of criminal groups will be discussed further in Chapter 6), confessed under police interrogation:

> I used to be an assistant in Wang's casino, which was in reality a fraud group, until I was let go. I then started working as a foreman in Lian's group following a job in another group owned by a fellow townsman. However, none of them gave me any money, and that's why I ended up here as the leader of this group. (LECID-1)

Setting aside whether he received money from the fraud groups, Lang's assertion clearly outlined his career path: he began his career as an assistant, accumulated experience, hopped between various cyber fraud groups, and eventually ascended to the position of group leader, overseeing a unit of 41 members.

Having said that, the interview data show that non-professional cybercriminals still exist. These individuals seem to be concentrated in the business of hacking. Haoming also noted that not all hackers are professional criminals. Some of them have legitimate jobs in the IT industry and conduct illicit, hacking-related activities to earn extra income. The primary reason might be that the skillset required for many IT roles significantly overlaps with those necessary to become a hacker, as Haoming wrote: "The line between black [legality] and white [illegality] is as thin as a sheet of paper, one could cross it simply by turning over in their sleep" (SX-H-1). Supporting Haoming's view, Xinyu, a cybersecurity engineer,

suspects that some practitioners within the IT industry, especially those who are specialised in ethical hacking, may sneakily carry out some "part-time jobs". He said:

> I am 100% innocent, but I am not sure about those ethical hackers. Of course, I am not saying that they would [commit crimes] ... I mean, they have the skillsets, they are familiar with the tools, and they know how to do things. They certainly have the ability, but whether they have been sneaky, for example, having some part-time jobs, I don't know about that. At the end of the day, these part-time incomes can be 10 times, or even 20 times higher than their regular salaries. With just one big successful deal, they could just retire. (GD-CSP-1)

Nevertheless, IT workers with higher education levels and employment in well-known companies appear less willing to engage in part-time criminal activities as they are less likely to risk their established social status (SX-H-1, SX-H-4, SC-H-1). Haoming also asserted that most of the hackers he encountered were individuals with a limited viewpoint, seemingly lacking a solid educational background (SX-H-1).

4. Interaction and Cooperation Between the Actors

In Chapter 1, I reviewed the economic concepts of markets and firms. In a broad sense, a market is where social actors interact and conduct business transactions, and a firm is an economically driven organisation that produces goods and services in a market (Coase, 1937; Holmstrom & Tirole, 1989; Williamson, 1996). Firms emerge to reduce uncertainty and to lessen the transaction costs that arise from the market, which may include the cost of information seeking, negotiating, contract signing and execution (Coase, 1937; Williamson, 1996). These two concepts have also been successfully applied to the analysis of various criminal industries. In the case of criminal industries, the business transactions among criminals on a horizontal level can be classified as a market transaction, and the vertically integrated criminal organisations can be understood as criminal firms (Reuter,

1983). Moreover, in the context of criminal industries, scholars take a rather encompassing approach to the definition of criminal firms. This includes consideration not only of robust and clearly delineated criminal organisations but also of those entities with configurations that manifest structural instability and exhibit fewer internal divisions of labour (Schelling, 1967; Reuter, 1983; von Lampe, 2015; Morselli et al., 2007; Lusthaus et al., 2018). In this section, I argue that the two economic concepts of markets and firms can also cover the forms of interaction and cooperation among criminal actors within the Chinese cybercrime industry.

In agreement with existing research, the data highlight the role of online forums and chat groups as essential marketplaces for cybercriminals, facilitating interactions and cooperation between actors in the cybercrime industry (Soudijn and Zegers, 2012; Leukfeldt, Kleemans & Stol., 2017; Lusthaus, 2018; Leukfeldt et al., 2019). A number of individuals, driven by the desire for monetary gains, navigate these marketplaces seeking criminal opportunities, acquiring knowledge, and exchanging products (SX-H-1, GZ-P-12, SX-P-1, GD-CSP-1, GD-CSP-3, GZ-P-6, GZ-P-10, GD-P-20). As provided in Section 2 above, the cybercrime industry in China has matured to a high degree of specialisation. Complicated criminal activities have been compartmentalised into simpler, discrete tasks that can be undertaken by ordinary individuals. Consequently, through the use of these marketplaces, those intent on engaging in cybercrime can relatively easily ascertain market demand and create new ventures to contribute to the cybercrime industry. Online tools and tutorials found on marketplaces also aid these individuals with acquiring the knowledge needed to start their criminal professions (GD-CSP-1, SX-H-1). Therefore, even those with no prior knowledge or experience in crime can find a way into this profession. Patience and persistence are all that are required (GD-CSP-1, GD-CSP-2, GZ-P-12). Stressing this

point, Xinyu even viewed online marketplaces as a "less mature criminal education system". He noted:

> You can enter a forum, and there might even be simple guides, basically laying out various strategies for you. A novice can go in, learn by following those guides, and will basically start to grasp some haphazard methods. More importantly, they can acquire some tools, like the Trojan horse I mentioned earlier. They can simply download and upload it to complete an attack (GD-CSP-1).

The data also point out that professional criminal forums and chat groups are not the only marketplaces where actors interact in China. Business transactions may also take place in forums that primarily host mainstream content, such as those dedicated to gaming, part-time job-related matters, and local community interactions. What is more, advertisements of illicit products can also be found on random websites and even on the street (GZ-P-10, GD-P-20, GD-CSP-5, GZ-P-12, SX-P-1). The presented evidence points unequivocally to the existence of a criminal market on a large scale in China.

Moreover, in a highly professionalised environment, vertically integrated criminal firms have also emerged. Almost all the market actors displayed in Section 2, such as hackers, SIM card dealers, drainers, cyber fraudsters, and money launderers, can assemble into the form of criminal firms (GZ-P-6, GZ-P-10, US-CSP-1, SX-H-4). According to a government report, the Chinese police cracked down on 39,000 groups conducting illicit SIM card and bank account business in 2021 (Central People's Government of the People's Republic of China, 2021). An article published in CCTV also revealed that in the same year, around 180 groups that provided ‘draining’ services were taken down (CCTV, 2021). Such groups are structured as legitimate companies and have a clear internal division of labour. For instance, as highlighted in the aforementioned CCTV article, one particular group had established branches in both Sichuan and Jiangsu Provinces. This group featured distinct roles such as the organiser, technicians, and business promoters.

Furthermore, the forms of cooperation between actors can be affected by the intervention of the state. On the one hand, state intervention encourages criminal cooperation in the markets due to the necessity of avoiding detection. On the other hand, state intervention also pushes the market actors who specialise in the same business sector to group up and cooperate in a more coordinated way. They escalate the complexity of their modus operandi to avoid detection. Fengshu and Kaile, two police officers, claimed that many business sectors in the cybercrime industry are now performed by professional firms rather than individual criminals to increase the sophistication of the operations (GX-P-1, SX-P-1). Kaile said: "These people know what they are doing. They also know how to take measures to avoid detection. If you [an individual criminal] want to do the same business by yourself, you are going to be arrested by the police with no difficulty" (SX-P-1). As a result, when state intervention is strengthened, criminal operations are broken down by the actors in the cybercrime industry into numerous business sectors. Criminals from different business sectors cooperate in the markets. At the same time, criminals who work in the same business sector tend to group up and cooperate in the form of firms. Ultimately, under the state intervention in China, there is a tendency to have a lot of small business sectors with many criminal firms working in each sector in the cybercrime industry.

5. Conclusion

This chapter provides insight into the actors within the cybercrime industry in China. It started with an analysis of the characteristics of cybercrime offenders. In doing so, this section sketched a criminal portrait of Chinese cybercriminals, who are socially disadvantaged individuals from small cities in economically developed provinces with a medium-to-low level of education and no history of crime public order violation. While the

statistical figures highlighted the presence of specialisation and professionalisation within the cybercrime industry, the subsequent sections provided a more detailed examination of these aspects, exploring the degree to which they exist among the actors involved. The second section showed that the level of specialisation is high. A successful cyber fraud operation involves a wide range of criminals specialising in different areas of expertise. Some acquire technical IT skills, while others do not. Without the assistance of the various actors, cyber fraud could not be carried out successfully on such a large scale. Subsequently, the third section reflected that a substantial portion of these experts also engaged in criminal activities as professionals, committing cybercrime as either a full-time occupation or as a primary source of income. Finally, in light of the theories of industrial economics, the last section analysed two forms of criminal cooperation within the cybercrime industry – the market and the firm. It also discussed how state intervention might affect the forms of cybercriminal cooperation and subsequently shapes the structure of the cybercrime industry.

In conclusion, this chapter showed that the actors in the cybercrime industry are mostly professional criminals with specialised expertise. Contrary to common expectations, many of them are not IT experts, and their profiles closely resemble those of conventional criminals. Moreover, like conventional criminals, cybercriminals cooperate in the form of markets and firms. The next two chapters will closely examine the two forms of criminal cooperation and analyse how governance is successfully achieved among cybercriminals in these respective contexts.

Chapter 5. The Market

As previous chapters have shown, the business of cyber fraud is thriving in China. Thousands of professional cybercriminals come from different backgrounds, with different skill sets, and work in different sectors to make cyber fraud happen smoothly and safely. For such a sizeable cybercrime market to exist and thrive, a degree of governance to enforce property rights must be present. When governance is absent, people are discouraged from engaging in production and trading, especially for goods and services of higher value. Moreover, the division of labour is only attractive when promises can be enforced (Shortland, 2019; Skarbek, 2014; Gambetta, 1996; Varese, 2001). When cybercriminals cannot rely on the government to provide governance, they must seek it elsewhere.

This chapter examines the governance systems in the Chinese cybercrime market. It first introduces the market structure in China. Through the lenses of governance theories, the following two sections study how governance is achieved to maintain order in both the market's online and offline dimensions. Drawing upon empirical findings, the fourth and final section compares and discusses these discoveries alongside prior research on cybercrime and governance theories. This section also offers reflections on the Chinese case in light of these theoretical perspectives.

1. Market Landscape

This section explores the structure of the Chinese cybercrime market. The empirical data suggest that cybercriminal trade has both online and offline dimensions in China. On the Internet, most business transactions are conducted on marketplaces, while offline there is no marketplace, and trade is conducted in random locations. In general, cybercriminals in China predominantly engage in transactions with their Chinese counterparts (GD-CSP-2,

GD-CSP-3, SX-H-1). There are two potential reasons for this observation. First, most Chinese cybercriminals do not speak English. As Chapter 3 revealed, most cybercriminals in China have a low level of education. It is therefore difficult for them to communicate with their overseas peers. Second, most products being traded among Chinese cybercriminals, such as Chinese SIM cards, personal data of Chinese citizens, and Chinese SNS accounts, are less popular overseas. Therefore, these products are less likely to be sold aboard.

1.1 The Online Market

The empirical data found that cybercriminals mainly conduct business activities on forums and chat groups found on various Instant Messengers (IM). Local forums that host regular content used to be frequently exploited by cybercriminals to conduct illicit trade. Baidu Tieba, as previously identified by Yip (2010) and Zhuge et al. (2009), was the largest (SX-H-1, SX-P-1, GD-CSP-3, GZ-P-6, GZ-P-10, GD-P-20). In a nutshell, Baidu Tieba is a publicly accessible discussion forum that allows users to create sub-forums. The sub-forums can be found through a built-in search engine. Cybercriminals would create sub-forums using jargon or abbreviated words to host their illicit transactions. For instance, criminals might have created a sub-forum named ‘CVV’ or ‘visa’ for stolen credit cards (Yip, 2010) or a combination of ‘wash’, ‘materials’, and some other words for money laundering (Zhao et al., 2016). In response to the state policy of countering cybercrime, Baidu Tieba has since strengthened its censorship of the content created by users over the past few years. This led to the shutdown of many sub-forums used for malicious purposes. Consequently, although some criminal activity still happens on Baidu Tieba, the volume remains at a low level (SX-H-1, GZ-P-4). With the use of a VPN, foreign forums are

another option for Chinese cybercriminals. In addition to English-speaking forums, there are also a few Chinese-speaking forums hosted overseas (SX-H-1, SC-H-1).

As for chat groups, Yip (2010) and Zhuge et al. (2009) found that QQ was the leading IM that hosted the most illicit transactions in China. In line with their research, the empirical data suggested that a significant number of chat groups still serve as cybercrime marketplaces on QQ. Nevertheless, criminals now have more choices. Many other IMs, such as WeChat and Telegram, are also prevalent (BJ-CSP-1, SX-H-1, GD-CSP-3, GZ-P-6, GZ-P-10, HEB-P-1, LECID-8). Xiangwei, a cybersecurity practitioner, introduced the topic:

> There are many chat groups [that host illicit content] …You can see people talk about these things on websites and forums, like technical-related issues … Some people put down a contact number, such as a QQ number, a WeChat number, or a phone number. [When you search the number,] you will find a chat group. (GD-CSP-3)

Some chat groups have over a hundred members and are open access or easily accessible (by answering simple questions or clicking links shared on websites or forums) (GD-CSP-1, LECID-8). On the other hand, other chat groups may be much smaller, and members can only join by invitation (SX-H-1, SX-H-2). Lusthaus (2019) found that online marketplaces are normally structured in four different layers: 1) the top layer, which holds the most open forums and marketplaces; 2) the middle layer of more closely vetted forums; 3) the bottom layer of even smaller and more closed groupings; and finally, 4) the molten core, which centres on the offline organisation of cybercrime, and members in this layer often know each other offline. In agreement with Lusthaus, this study's empirical data suggest that these closed chat groups resemble the middle and bottom layers of online marketplaces. They are the essential business realm where cybercriminals operate.

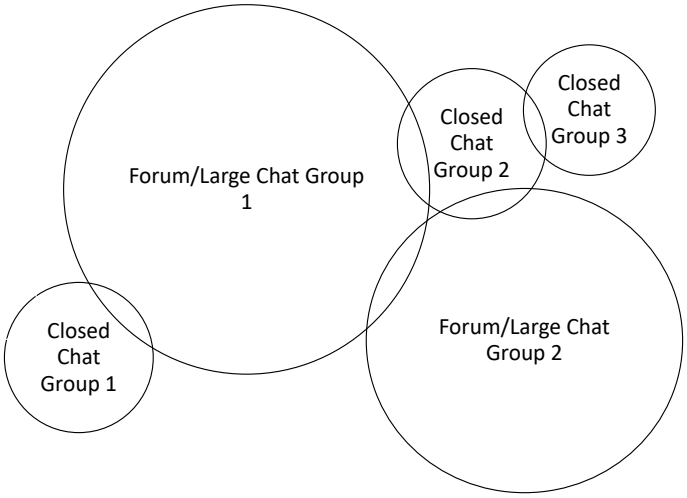
In closed chat groups, business with complex tasks is more frequent, as cybercriminals perceive them to be a more reliable place for their business (SX-H-1, SX-H-4, SC-H-1, GD-CSP-1). Haoming said: “Those big groups are never reliable. Most serious business is done in small groups” (SX-H-1). Criminals are more likely to trade tailored services and goods in closed chat groups. Taking personal data as an example, a selection between forums and large chat groups or closed chat groups often depends on whether the criminal wants to acquire a specific set of data, or whether he/she wants to explore what personal data are for sale (SX-H-1). Thus, being a member of a few closed chat groups is critical for criminals who want to be successful in the market.

When a criminal establishes a good reputation on a forum or large chat group, he/she will eventually be invited into a closed chat group (GD-CSP-1, SC-H-1, SX-H-2). Xinyu, a cybersecurity practitioner, said:

> In the beginning, you start somewhere [any online marketplace]. Then there are a lot of members, right? You will engage with many cybercriminals, including some experienced ones. These people have more underground connections, such as closed chat groups. When you build some reputation, you will eventually be invited into these groups. (GD-CSP-1)

This invitation process is reciprocal, with members from closed chat groups also being invited to join various other forums/large chat groups and also additional closed chat groups (SX-H-2). This invitation system makes different chat groups and forums interconnected and forms a complex web, as shown in Figure 1 below.

Figure 1: Connection between Marketplaces and Chat Groups



Since the invitation is often followed by an introduction, when a criminal who operates on a forum or a large chat group is invited to a closed chat group (e.g., Closed Chat Group 1), the inviter always introduces him/her using his nickname on the previous marketplaces. The same happens when he/she is later invited into another closed chat group (e.g., Closed Chat Group 2) by a member who operates in both chat groups. As a result, a criminal's nickname is no longer associated with only one marketplace. Therefore, using different 'handles' for different marketplaces becomes difficult (Lusthaus, 2018, p.110).

In addition to forums and chat groups, a few online business activities can take place outside of these underground marketplaces. For example, advertisements about cybercrime-related products and services can occasionally be found on websites that pop up through Google searches using specific keywords (SX-CSP-1). They may also appear in online chat groups hosting regular content such as gaming discussions, part-time job discussions, and local community discussions (GD-P-20, SX-H-1), as well as in text messages (SX-H-1). In these cases, a contact number, which is normally a QQ number, is attached. Whoever is interested in the products and services can make direct contact with the advertiser. The randomness and concealment of this type of transaction bring even more

difficulties to investigations compared to those that happen on marketplaces. Yanse, a police officer, complained:

> What I hate the most is when I hear a criminal say he sold the product to a random guy called 'A Long' [a popular street name in China]. This 'A Long' is from an online chat group where people discuss where to find local stalls that sell delicious 'stinky tofu' [a popular street food in China]. In this case, it is difficult for us to find information about his partner. (GD-P-20)

1.2 The Offline Market

In addition to the online market, criminals also carry out business activities offline. There is no marketplace in the offline world in China for cybercriminals to meet and trade. Therefore, finding a trading partner is a challenge for many. Cybercriminals often rely on three ways to locate their potential collaborators: offline social networks, online marketplaces, and random encounters.

As for offline social networks, Leukfeldt's (2014) study on cybercriminal networks in Amsterdam discovered that the exchange of services took place among numerous criminals connected through various real-world social networks, including friendships and ethnic ties. Similar observations were also found in Romania and Nigeria (Lusthaus, 2018; Lusthaus & Varese, 2021). In line with these studies, the same type of offline social network was observed in China. Rouxun, a police officer, found that cybercriminals often cooperate with those who live in the same region, graduate from the same school, or work in the same company. They often "find each other" when a business opportunity comes along. He said:

> When a criminal gets a VOIP machine, he will use his [offline] social networks to find cyber fraudsters. He will call the fraudsters that he can provide, say, five channels or five seats, that's what they call them, and charge them for a certain amount of money each day. That's how they run business. Criminals often find each other. (GZ-P-10)

An extensive offline social network gives criminals a better chance to succeed in their business, as they can easily find suppliers or customers. Xiangwei, a cybersecurity practitioner who has cooperated with the police to fight cybercrime for many years, told a story about how a trojan writer made a fortune on his trojan by loaning it to friends. He summarised: "Why is his business so successful? Because he used to work in an internet café. He has his social circle [and knows many cybercriminals]. He can use his social circle to promote and sell his product" (GD-CSP-3).

Dealing with people they have already cooperated with on online marketplaces is the second option for cybercriminals. As Lusthaus's studies (2018, 2019) suggested, many cybercriminals would eventually meet their online partners in the real world when the number of interactions increases. This is also true in the case of China (LECID-3, LECID-8, SX-H-1, SX-H-2, SX-H-3, SX-H-4, SX-H-5, SC-H-1). Haoming, a former hacker, claimed that the 'social circle' is small and that many people "just happen to meet each other at the end" (SX-H-1). For another former hacker, Shentu, offline trade provides a sense of security to both parties. He stated: "I am more willing to cooperate with people offline. In this way, I feel the business is safer as my partner is less likely to disappear" (SX-H-4). Thus, when he needed to sell or purchase products and services, he always started with people he had met offline.

In some cases, however, the offline business encounter is somewhat random. Criminals might encounter potential partners while socialising in a bar or by noticing advertisements posted on a utility pole (GD-CSP-3, GD-P-20, SX-CSP-1, SX-P-1, SX-CSP-1). Yanse discovered that in some areas where street surveillance is less prevalent, advertisements related to cybercrime are sometimes disseminated publicly (GD-P-20). Nevertheless, cooperating with random partners carries a much higher risk. People who choose to do so are either left with no other options or lack experience (GD-P-20, SX-CSP-1).

Overall, in line with previous studies on cybercrime, market cooperation between cybercriminals in China takes place both online and offline. Since the activity pattern differs in each dimension, the governance systems are also expected to differ. The next two sections discuss how online and offline business activities are respectively governed.

2. Online Governance

Even though its participants remain anonymous, the online world still provides space for governance. The general impression of a chaotic cybercriminal world is inaccurate. As with conventional criminals (Skarbek, 2014; Wang, 2017; Leeson, 2007; Gambetta, 2009; Shortland, 2019), cybercriminals can also create a governance system to maintain economic order. In general, the empirical data suggest that the online governance system is formed from a mixture of self-governance and third-party governance. Cybercriminals not only rely on a reputation mechanism, norms, and communal punishment to self-govern the market, but also employ third parties to create formal rules, patrol the market, and enforce their agreements.

2.1 Online Self-governance

When dealing with anonymous parties online, direct self-enforcement against the wrongdoer through means such as violence or technical measures resembling violence (for instance, doxing or DDoS) is relatively rare. This is due to the high technical requirements associated with this type of enforcement (SX-CSP-1, SX-H-1). Typically, self-governance in the online market operates on a community level.

Above all, the reputation mechanism plays the most central role in online marketplaces. Cybercriminals often decide to cooperate based on an assessment of their potential partner's reputation ex-ante (Lusthaus, 2018; Yip, et al., 2013; Sebagh et al., 2021). A criminal's reputation can be easily accessed through browsing threads and chat histories on online marketplaces. Owing to the lack of trust in the online business environment, cybercriminals do not cooperate with random people. Instead, they carefully check a potential cooperator's reputation. Shentu, a former hacker, provided an example of how careful he was when he purchased products online:

> I found a guy on an online marketplace selling hotel registration records. He provided some free samples, and they looked extremely detailed. I checked the sample and found that the hotels were booked through different online platforms, and the newest record was yesterday. Therefore, I believe the data came from the police. However, I doubted that police data could be stolen so easily without alerting the authorities themselves. If he was that good, why was he still selling the data in an online marketplace like that and manage to remain unknown? So the most likely explanation was that he was a scammer. Anyway, I checked his online transaction records and searched if there were idiots who bought his products and swore at him (SX-H-4).

In the end, Shentu didn't find any information about this seller as the seller was new to the marketplace. This fortified Shentu's belief that he was unreliable. This example shows how a criminal who does not have a reputation may have a hard time finding collaborators in online marketplaces. Despite offering high-quality free samples, a seller with no established reputation could still be deemed suspicious by potential buyers.

Kaile metaphorically likened the cooperation of cybercriminals online to being in a relationship with someone: "For example, when you have completely no idea about a girl's look, her background, her personality, you don't want her to be your girlfriend, right?" (SX-P-1). He then emphasised: "Why can a criminal successfully cheat on his partner? Because he has convinced his partner that he can do what he said [through his reputation]. For example, he has posted something online for sale, and he has been honest before" (SX-P-

1). In other words, reputation is an essential asset for a cybercriminal. The better a criminal's reputation, the more likely that other criminals will trust him/her and subsequently decide to cooperate (SC-R-1, SC-H-1, SX-H-1, SX-CSP-1, SX-P-1).

Reputation also helps criminals to work in a better business environment and advance their criminal careers. As mentioned in the above section, closed chat groups form an essential part of the online market. Because all members in these chat groups have good reputations, the level of trust is high within the groups. It therefore enables complex (and often more profitable) cooperation. In order to join these elite criminal communities, criminals must first build their reputations. The better a criminal's reputation, the more likely he/she will be invited to more closed chat groups, work in a better business environment, and be exposed to more business opportunities (GD-CPS-1, SX-H-1, SX-H-2). On the other hand, having a bad reputation is worse than having no reputation, as no one will risk cooperating with a person who has a bad reputation (HEB-P-1, GD-CSP-1, SC-R-1, SX-P-1, SX-H-1, SX-CSP-1, GD-P-19).

However, reputation does not simply emerge spontaneously. Criminals need to put effort into the reputation-building process. Criminals take steps such as sharing information for free (GD-CSP-1), advertising (SX-H-1, SX-CSP-1), and even providing free services (SX-H-1) to build their reputation. Therefore, there is a significant sunk cost for cybercriminals who decide to abandon an ID with a good reputation attached.

In addition to the reputation mechanism, cybercriminals also create norms to assist with maintaining order. Like regular business activities that people encounter daily, there are underlying business manners and etiquettes that criminals are expected to follow (SX-H-1, SX-H-3, SX-H-5, GD-P-19, US-CSP-2, SX-CSP-2). Chengzi, a veteran cybersecurity practitioner, said that the cyber fraud market in China is full of norms. He wrote: "There are plenty of norms, but it is hard for me to explain them all in words. It really depends on

the circumstances. There are basic principles, such as not asking sellers where their data comes from and not showing off the stolen data" (SX-CSP-2). There are also norms that regard the use of language during the negotiations (GD-R-1, GD-CSP-3, SX-CSP-2, SX-P-1), the way of providing product samples during a trade (SC-H-1), and the principle of reciprocation (SX-CSP-1). Adherence to the norms not only signals the criminal identity, moral standard, knowledge, and experience of a criminal, but also ensures a safe and smooth cooperation for both parties (SX-CSP-1, SX-CSP-2). Therefore, a cybercriminal who follows the norms is more likely to have repeat customers and make more friends in the criminal community. As Chengzi said: "The more you stick to the norms, the safer you are, and the more successful you will be" (SX-CSP-2). In the same vein, adherence to the norms has an impact on one's reputation. A criminal can develop a bad reputation for behaving counter to professional standards, which can in turn reduce others' readiness to collaborate (SX-H-1, SX-CSP-2).

Yet adherence to established norms is not a primary concern within the criminal market. A cybercriminal may demonstrate improper behaviour yet maintain a good reputation for the products or services they provide, and thus still manage to attract collaborators. Former hacker Youlv, for example, exhibited indifference regarding whether his collaborator adhered to established norms or not. What he only cared about was the quality of the products and if his collaborator could help him to make money. He claimed: "Ten years ago when I just entered this profession, people might still care about these 'spirits'. Nowadays people only talk about money" (SX-H-5). After all, given that marketplaces are online platforms designed for commercial activity rather than daily personal interactions, their social function is inherently diminished. This reduction in social context leads to norms being less important for cybercriminals operating within these online marketplaces. Hence, even though norms retain their functional role, their significance is less pronounced

compared to offline criminal environments, such as prisons, where there are more opportunities for social interaction (Skarbek, 2012).

The functioning of the reputation mechanism and norms are supported by a communal punishment system. Communicating the wrongdoers' deeds to others to impose public shaming, and advocating that others not interact with them are the most common reactions for cybercriminals when serious violation of norms and dishonest behaviour happen (HEB-P-1, SC-H-1, SX-P-1, SX-H-1). A post that complained about one user's suspicious phishing activities on a popular forum wrote:

> Recently I've heard of multiple people (Me included) being contacted by ***. He's using his real PGP Key, his real old email address (He emailed me on ***) and is contacting people at random. He originally messaged me on 16 Aug 2022 but he is now reaching out to more people. Today he put up a page with his new contact email and his old PGP Key (***) and is sending it to people. It should be obvious, but do not talk to him. (CSCR-7)

Collective action may also be taken to isolate the wrongdoers, as Kaile wrote:

> There is an invisible hand that governs the market. If a scam happens, people in the market will notice that you are a scammer. They will exclude you from the market … Therefore, criminals can't make a lot of money by scamming people. As you see, scamming is a one-off trade. If I cheat you today and cheat him tomorrow, the day after tomorrow, I won't be able to cheat anybody as no one talks to me anymore. (SX-P-1)

The structure of online marketplaces also amplifies the consequence and power of collective action. As shown in the above section, because online marketplaces are interconnected, information about wrongdoing in one marketplace can easily spread to others. As a result, a wrongdoer may be excluded from various online marketplaces, and ultimately becomes "socially dead" online (GD-P-17, GX-P-2, SX-H-1). Haoming provided an example of this process:

> Yesterday someone just disappeared. This guy shared a vulnerability on a chat group. But the link was, in fact, connected to a Trojan. Once you click on the link, a Trojan would be automatically downloaded to your computer, allowing him to access and control your system. His scam was later discovered and reported on numerous chat groups. I am not sure how he is doing in real life, but he is entirely dead online now. (SX-H-1)

Nevertheless, self-governance online seems to be deeply rooted in cybercrime-related marketplaces. The reputation mechanism, norms and the communal punishment system have limited governing effects on business activities outside these marketplaces as there is a lack of stable social community. Therefore, it is significantly riskier to cooperate this way. For example, Wangming, a cybersecurity practitioner who has invested significant effort into understanding the cybercrime market, posits that the majority of advertisers promoting their services outside of marketplaces are scammers. Should a cybercriminal wish to collaborate with an anonymous party outside these marketplaces, finding a middleman capable of providing third-party governance is indispensable (SX-CSP-1).

2.2 Online Third-party Governance

In addition to self-governance, cybercriminals rely on third parties to create rules, maintain order, and enforce agreements. In the online market, third-party governance takes place in two forms. The first form is when marketplace administrators create and enforce rules for the marketplace. The second form is when a cybercriminal, often a marketplace administrator or a reputable criminal, provides escrow services to others.

The first form of third-party enforcement exists primarily in forums. While forums often have written rules, chat groups do not (GD-CSP-1, SX-H-2, SX-CSP-1, SX-CSP-2). A possible explanation is that the administrators of chat groups are often also buyers or sellers. They are more interested in their own business than in providing governance services (SX-

H-1, SX-CSP-1, SX-CSP-2). According to Haoming, most administrators of chat groups have an equal relationship with other members. They only take action against group members recognised by the community as "disrupting market orders" (SX-H-1). On the other hand, forum administrators often take a more active role as enforcers. Because running the forum is their business, they profit from these governance services (GD-CSP-1, SC-H-1, SX-H-1). Moreover, while forums have the technical structure to execute various punishments top-down, chat group administrators have limited tools to enforce the rules other than removing the member from the chat group.

Written rules in forums cover plentiful aspects of daily interaction among forum members. For instance, one of the popular forums among Chinese cybercriminals provides a list of 49 forum rules, which are classified into five categories: general rules, posting rules, advertising rules, marketplace rules, and reputation system rules. These detailed rules specify unacceptable behaviour, such as doxing[15], begging, spamming, and cheating. They also define what products users are prohibited from selling, such as drugs and weapons. Moreover, they regulate the format and content of posts, such as forbidding the abuse of emojis and special characters. In addition, they set down the procedure for reporting violations and the potential punishments, such as banishment (CSCR-6). Although there are some variations, some universal rules, such as the prohibiting of spamming, doxing and cheating, can be seen in most forums (CSCR-6, CSCR-8, CSCR-9). Some forums have entrance hurdles to keep away dishonest traders. These include a membership fee or a vetting requirement (GD-CSP-1).

On top of creating and managing forum rules, administrators also actively patrol the forums and take action against apparent violations. They also accept reports from forum

[15] An act of searching for and disseminating private or identifiable details about a specific person via the Internet, generally driven by malicious intent.

members. Reporting to the administrators often leads to a judicial procedure. There is limited data on the intricate process of this procedure, except for the understanding that the arbitration tends to be quite informal (SX-H-1), and in most instances, the burden of proof falls on the reporter (SX-H-1, CSCR-6, CSCR-8, CSCR-9). Since forums have a comprehensive infrastructure with versatile functions, enforcement can take place in different forms to match the seriousness of the misconduct. Typical forms of punishment for violation include deletion of posts, temporary suspension, demotion, and permanent expulsion (CSCR-6, CSCR-8, CSCR-9). An example of a forum user being temporarily suspended by the administrator for breaking forum rules can be seen in the following message displayed under that user's nickname in a post the user replied to: "This forum account is currently banned. Ban Length: (2w, 1d, 10h remaining). Ban Reason: Failure to Follow Forum Rules and spamming appeals" (CSCR-7). Because there is a designated third party to provide governance services and the technical infrastructure of the forums supports it, a stronger sense of order is presented. Participants often use the word 'formal' to describe forums, implying a better-functioning market (GD-CSP-1, GD-CSP-3, SX-H-1, SX-H-3, SX-CSP-1). A former hacker, Qinglan, for instance, claimed that in chat groups, there are inevitably annoying spam messages. In contrast, in forums, there are far fewer of these, as forum administrators often delete spam messages speedily, and senders are swiftly punished (SX-H-3).

Forum and chat group administrators also provide the second form of third-party governance: the escrow service. This is sometimes also provided by "people who have a long-term fixed online identity" (SX-H-1, SX-CSP-1, SX-CSP-2, SC-H-1, SX-H-3, SX-H-5). In this case, the escrow service provider normally holds the money from the buyers until the products have been delivered (SX-H-1, SC-H-1, SX-CSP-1, SX-CSP-2). The presence of an independent third party capable of providing escrow services creates an extra layer

of protection for the safety of the transaction. However, whether or not the third party is trustworthy becomes another challenge to the cybercriminals.

3. Offline Governance

When cooperation (or part of the cooperation, such as delivering physical products) takes place in the offline world, the protection of anonymity is lessened. Cybercriminals also face a different business environment offline. The empirical data showed that a system that combines self-governance and third-party governance could also be discovered offline. Compared with the online market, hostage-taking is commonly used to enhance self-enforcement, and there is reliance on third-party governance.

3.1 Offline Self-governance

Pre-established social relations play an essential role in the offline market. Business partners are often relatives or schoolfriends, or come from the same hometown and speak the same dialect (SX-H-1, GD-R-1). The reputation mechanism functions well when embedded in these pre-existing social relations.

Similar to the online market, staying honest and doing favours for friends help to build a reputation (GD-R-1, GD-CSP-3, SX-CSP-2, SX-P-1, SX-CSP-2). Because of pre-existing social relations, criminals often operate in the same social network within a close-knit community, and a collaborator's reputation can be assessed at low cost. Moreover, warnings about other criminals can be easily communicated to people within the community, and communal punishment such as exclusion can be imposed (GD-CSP-3, GD-CSP-4, GD-P-5, GD-R-1). The embedded social relations also magnify the consequence of developing a bad reputation. A wrongdoer will not only lose his/her

potential business partners in the future but also lose his/her friends. He/she may even lose social status in the community. Daihui believed that the reputation mechanism functions particularly well when two parties come from the same village. In this case, an action of defection can lead to social exclusion against not only the wrongdoer but his/her immediate relatives. Daihui said: “People are afraid of defection. If you become a defector, how will your children live in the village? [People would gossip behind their backs]. Also, nobody wants to be excluded from the spring festival celebration, right?” (GD-P-5).

The same principle applies when business partners have a pre-established social relationship online; in other words, when two parties have done business with each other on online marketplaces. In this case, both parties know each other’s online identity. Thus, information about any wrongdoing can be spread to online marketplaces, and communal punishment will follow (SX-H-1).

The reputation mechanism, however, functions less well offline when pre-established social relations are absent. In this case, information transmission becomes an enormous challenge. A criminal cannot assess his/her potential partner’s reputation ex-ante. Without a shared community, he/she also has nowhere to report dishonest behaviour and cause reputation damage to the scammer. This scenario mirrors the circumstances when a cybercriminal collaborates with an anonymous party online outside of specific cybercrime-related marketplaces.

A good demonstration of this can be seen in a confidential investigation document, which records a case where there was a failure in cooperation (LECID-8). According to the document, a man was charged with selling national certificates. He intended to provide a company registration service to make some quick money, but lost his citizen ID and two SIM cards linked to his ID. The companies he registered were also stolen. With these

documents, the other criminal could conduct criminal activities (such as money laundering) using his identity. The suspect confessed:

> I saw an advertisement about someone looking for a company registration service. So I contacted the buyer and arranged with him to meet at a printing shop. For company registration, he copied my citizen ID and used my ID to do a tax registration. He then bought me to a telephone business hall and used my ID to buy two SIM cards. After that, he took me to a KFC and asked me to scan a QR code to do a real-name authentication [to register companies]. He gave me 200 yuan as a deposit, took my citizen ID, and said he would be back with me in a minute. After one hour, he sent me two QR codes via WeChat and told me to apply for a company modification registration [so that I would become the company owner]. Once I did that, he said he would tell me to do another modification registration in two days to transfer the company to another person and pay me the rest of the money. However, he disappeared after that day. He shut down his phone. I never received my money and only got my ID back until I was arrested by the police (LECID-8).

While he bears some responsibility for his recklessness, his experience nevertheless illustrates the issues inherent in the functioning of the reputation mechanism. The fact that he found this advertisement on a WeChat group posting job recruitment content, instead of a cybercrime-related marketplace, means that he had no prior knowledge of the buyer's reputation and could not assess it. Moreover, after being cheated, he had nowhere to report the scam and impose reputation damage on the buyer.

Cybercriminals may also attempt to enforce contracts by themselves when dealing with offline strangers. As in traditional crime, cybercriminals sometimes adopt hostage-taking to ensure both parties perform the contractual obligations and strengthen the effect of enforcement. Hostage-taking may be conducted in an old-fashioned way, where a person becomes a hostage. For instance, Siwen, a police officer, set forth a case where this method was used to ensure the safety of business transactions:

> Last year I encountered a case that involved money laundering. Some criminals from a village acted as money mules to carry money across the border for cyber fraudsters who operated aboard. The cyber fraudsters asked these criminals to send a person aboard to assist them with management work. But everyone knew this guy was a hostage. If

> problems happen, the villagers must handle them. Otherwise, the hostage's life would be in danger. (GX-P-3)

Hostage-taking can be performed another way, where information is taken hostage (Schelling, 1990; Gambetta, 2009). This works particularly well when the two parties are online partners. For cybercriminals, simply showing up offline reveals much information, such as which city they live in and their accent. Most importantly, street cameras capture their face and movements (BEJ-CSP-1, GX-P-3, SX-H-1). This information can threaten cybercriminals' safety, as Gambetta (2009, p.62−64) puts it: when "identification is at a premium and must be kept secret, just showing one's face is itself like giving a hostage." Haoming wrote:

> I feel that in the real world, many people tend to be restrained because they are exposing themselves. People fear that the other party will do something against them … The logic is that there is a difference between online shopping and offline shopping. When you sell things offline, people know your face, where you work and where you live. (SX-H-1)

Of course, in many cases, the information a criminal exposes may not be comprehensive or precise enough for their partner to locate them after a defection. However, this information may be enough for the police to tackle the criminal (GD-P-22, GX-P-1, GX-P-3, GZ-P-4, SX-CSP-2, LECID-5). Reporting it to the police and letting them do the rest of the work is one way of using the hostage information. Zhenqiang, a police officer, described the action of reporting as "dog bites dog", and believed it is not uncommon among criminals (GX-P-1). In line with Zhenqiang, a confidential investigation document reports a case where a suspect's citizen ID was known to the buyer. The buyer later sent him a threatening message, warning him not to betray them: "If I didn't buy the digital currency for him [and run with his money], he would inform the police", said the suspect (LECID-5).

A similar example was found in another case described by Qiang, a police officer in Guangdong Province, showing that the threat could be real. Qiang noted: “There was a criminal who wanted to launder his money. The launderer took his money and ran away. This angry man called the police, and we arrested them both in the end” (GD-P-22). Although there is the risk of arrest for an informer, the legal consequence may sometimes be less severe, as Chengzi, the cybersecurity practitioner who has worked with the police to fight cybercrime for years, said:

> Sometimes when the amount of money involved in a scam is large, or the criminal knows the other person’s real identity, he may choose to inform the police … In this case, you are a victim of fraud. Of course, under criminal law, you might as well commit the crime, but you are only at the stage of ‘preparation’ or ‘attempt’. This means that you are unlikely to be charged with criminal offences in practice. You will likely only be rebuked by the police or receive public security administration punishments [relatively lighter punishments such as small fines and imprisonments up to 20 days; also, no criminal record is created]. (SX-CSP-2)

It is unknown to what extent the police practice resembles Chengzi's statement and how many criminals are willing to expose themselves to law enforcement agents. Nevertheless, being able to report to the police poses a clear threat. In the worst-case scenario, both parties go to prison.

Hostage-taking can be an efficient way of preventing deception. Handling hostages is, however, costly and requires specific skills (Shortland, 2019). Violence and informing can also be risky. Thus, self-enforcement is not affordable for every cybercriminal. It appears to be more commonly used by cybercriminal firms and high-level cybercriminals who either have "brothers who can fight", or who deal with large amounts of money (SX-H-1).

3.2 Offline Third-party Governance

When Gambetta interviewed a cattle breeder in Palermo, Sicily, the cattle breeder gave a statement with a deep theoretical implication. The statement went: “When the butcher

comes to me to buy an animal, he knows that I want to cheat him. But I know that he wants to cheat me. Thus we need, say, Peppe [that is, a third party] to make us agree. And we both pay Peppe a percentage of the deal" (Gambetta, 1996, p.15). The same scenario described by the cattle breeder frequently happens in China's offline cybercrime market. When the buyers and the sellers are strangers, and neither of them knows if the other party is reliable, a Peppe − in other words, a middleman − can help ensure the success of offline cooperation.

Like this Peppe, there are professional middlemen in the cybercrime market that provide the same services (SX-H-1, SC-H-1, SX-H-2, SX-H-5, SX-CSP-1). The typical profile of a middleman in the offline cybercrime market is an experienced elite cybercriminal who has been active in the market for an extended period of time. He knows the market, has a high degree of social ties, and is influential among cybercriminals (SC-H-1, SX-H-1, SX-H-2, SX-H-5). Interestingly, violence was not mentioned by the participants as an essential property of a middleman. Youlv, a former hacker, put: "A middleman needs to know plenty of people. He must also acquire professional knowledge to identify and solve problems" (SX-H-5). Similarly, Feiyue, another former hacker, said: "A middleman knows many people who work in this market. He must have some energy to gather everyone around him" (SX-H-2).

Services provided by middlemen come in two forms. First, middlemen can help a client to locate a reliable partner (SX-H-5, SC-H-1, SX-H-1). For example, Youlv, a former hacker, provided: "A wants to sell a product, he finds B, the middleman. B checks his product to see if it matches the description. If B is satisfied with the quality, he connects A with C, D, or E, who wish to buy the products for the trade" (SX-H-5). Second, he/she can help a client to enforce a contract if a defection happens. In rare cases, this means violent punishment (SC-R-1, SX-H-1). However, in many other cases, reputational damage is

imposed (SC-H-1, SX-H-1, SX-CSP-1, SX-CSP-2). Haoming wrote: “When conducting business offline, having a middleman to enforce the contract is important. He doesn’t have to act violently. If you do not fulfil the contract obligations, all he needs to do is to let everyone know you are not reliable” (SX-H-1). Because of the number of people that the middleman knows, by utilising his/her social network, he/she is able to make sure the information spreads and reaches enough people around the wrongdoer. Collective punishment can then follow.

What is more, in some cases, when the middleman also knows the online identity of their customer, the power of enforcement becomes even stronger, as the middleman can also spoil the wrongdoer’s online reputation (SX-H-1). When information transmission is a problem in the offline world, middlemen fill the gap by either directing the clients to reliable collaborators or enforcing the contract. Middlemen act as information disseminators. As Wangming concluded: “Middleman makes money with information” (SX-CPS-1). This enables the reputation mechanism to function.

Nevertheless, relying on a middleman does not always guarantee the success of a cooperation. There are two risks. First, the middleman may not be reliable. He may also act as a defector, take the commission fee, and flee. In this case, the information transmission problem again becomes a threat: the person who suffers the loss has no one to report it to. The second risk is that the middleman may be incapable of recovering the client’s loss. Haoming, a former hacker, provided an example of failure:

> A stranger [a buyer] contacted a middleman, and this middleman found me. We agreed that I would charge him [the buyer] 200 thousand yuan in total [for my service]. He would pay me half of the price first. When my task was completed, we would let the middleman check the quality. If there was no problem, I would give him the data and he would pay me the rest. However, after I finished my job and sent him [the buyer] the data, he just ran away with it. The middleman couldn’t do anything to him because that guy appeared to have some mafia background. So I never got my full sum (SX-H-1).

Therefore, cybercriminals need to be careful when selecting middlemen offline. Again, criminals may rely on self-governance. Finding a middleman through pre-established social relations and making use of the reputation mechanism is the smartest choice (SX-CSP-2).

4. Discussion: The Case of China and Reflections on Theory

On the whole, when compared with the identified cybercrime markets worldwide, the market in China appears to place a stronger emphasis on local IM-based chat groups rather than formal forums. Undoubtedly, China's internet environment contributes to this phenomenon. The online surveillance system makes operating any public cybercriminal activity, such as hosting cybercrime marketplaces within China, both challenging and fraught with significant risk. At the same time, while looking to utilise marketplaces hosted abroad is an option, the products being traded are less popular overseas. Language barriers further elevate the difficulty for criminals to communicate with their global counterparts. However, while government surveillance can be conducted relatively easily on websites, it becomes more challenging with chat groups as they are privately owned. The use of mobile phone numbers and citizen IDs purchased on the market can also circumvent the real-name registration system. Furthermore, in instances of using foreign IMs, like Telegram, these issues are further mitigated. Consequently, conducting business on chat groups can be a comparatively safer option for Chinese cybercriminals.

In relation to governance, the findings support most of the existing studies. As for online governance, in line with existing literature, the reputation mechanism plays a central role. It enables cybercriminals to self-govern the market and avoid being cheated by someone else (Espinosa, 2019; Wehinger, 2011; Ferguson, 2017; Lusthaus, 2018; van Waardenberg,

2021). It functions by enabling cybercriminals to make decisions on cooperation carefully by estimating the risk ex ante and imposing threatening communal punishment ex-post (Lusthaus, 2018; Skarbek, 2014). Because of the potential consequence of spoiling a (future) relationship with not only a partner but also anyone who finds out, even if the two parties are strangers and do not expect future interactions, the reputation mechanism creates an incentive for them to be cooperative (Stringham, 2015). In addition to the reputation mechanism, third-party governance plays a role in the governance system. It facilitates scalable trading in an online marketplace by providing escrow services, enacting and enforcing rules, and promptly eliminating dishonest traders (Yip et al., 2013; Lusthaus, 2018). However, in comparison to the cybercrime market outside of China, the chat-group-based market landscape within the country seems to place greater emphasis on self-governance, largely due to the absence of formal functional architecture within these chat groups. Moreover, the structure of the Chinese cybercrime market, characterised by reliance on chat groups and the interconnection between chat groups and forums, appears to augment the effectiveness of the self-governance system. In this market structure, a criminal's nickname is not confined to a single marketplace. This makes the process of registering multiple nicknames and employing them for different marketplaces prohibitively costly. As a result, communal punishment of dishonest behaviour can generate a ripple effect, leading to widespread exclusion. This scenario poses a considerable threat to cybercriminals since they risk not just their reputation on one marketplace but on all. They also cannot enter the same chat groups using new nicknames as they may not encounter the same criminals who can reintroduce them into the same groups.

Regarding offline governance, even though there is not much research specifically addressing the offline dimension of cybercrime governance, the findings from China align

with most existing studies. Social ties and pre-existing relationships play a critical role in offline governance, as they establish social bonds between cybercriminals. These bonds facilitate the application of social sanctions, thereby enabling the reputation mechanism to function effectively (Leukfeldt, 2014; Lusthaus, 2018; Leukfeldt, Kleemans & Stol, 2017). In addition, offline interactions allow individuals to enforce measures directly against dishonest partners, making hostage-taking a potentially effective strategy to deter dishonest behaviour (Lusthaus, 2018). Gambetta's (2009) concept of an 'information hostage' also largely applies to the Chinese cybercrime market. Lastly, consistent with Lusthaus's (2018) findings, the involvement of organised crime in providing third-party governance services is rare in China.

In addition, there are also a few reflections on the theory of governance that are worth discussing. First, literature on self-governance has found that the reputation mechanism works well when information transmission is unobstructed. In other words, information about dishonest behaviour must be disseminated to enough people easily for communal punishment to be applied. For this reason, the reputation mechanism works best in close-knit communities or within a particular geographic boundary (Leeson, 2014a; Stringham, 2015; Catino, 2019; Landa, 1981; Skarbek, 2012). The presence of online marketplaces solves the problem of information transmission among strangers across different geographic boundaries: the reputation of a criminal can be assessed at low cost by browsing previous posts or chat histories. Therefore, a message that reports dishonest behaviour can be quickly communicated to all members of an online marketplace. Furthermore, once a message is sent to a chat group or once a post is made, it stays for an extended period, if not forever. Thus, the reputation mechanism functions well in online marketplaces, even when participants are anonymous and exist in different locations. Thus, the well-functioning reputation mechanism in online marketplaces lowers the entrance hurdle of

cybercrime. It allows non-professional cybercriminals with no pre-established social relationship with other criminals to participate in the trade. The flourishing of online marketplaces may explain why the cybercrime economy has scaled up.

Second, although the hostage was found to be a mechanism that provides governance in the offline world, it did not appear to function in the online domain. One explanation is that there is no suitable object to be taken as hostage in a purely online setting. Moreover, Schelling (1990) and Gambetta's (2009) concept of information hostage also has limited effect in a purely online setting, as the information given can easily be fake, and its validity is difficult to verify. In an anonymous context, there is also the problem of enforcement: even if the hosted information, such as criminal history, is accurate, there is little the other party, or even the police, can do when it is linked to an online identity. Thus, hostage-taking makes more sense and has a more substantial deterring effect when criminals meet offline. As the empirical data also show, when an online identity is linked to a real person, information becomes threatening, and actions can be taken against the wrongdoer.

Third, while there was a lack of discussion about the middleman services in the offline dimension of cybercrime in the literature, this study finds that they are common in China. Professional middleman services, commonly provided by experienced cybercriminals, take place in traditional organised crime to act as third-party governors. However, violent punishment is rare. Instead of violence, being able to provoke social sanction in both online and offline dimensions is their weapon. Acting as an information disseminator, the presence of a middleman partially solves the information transmission problem and facilitates the operating of the reputation mechanism. What middlemen need to signal to their customers is, therefore, not their capability of violence but their reputation and large social networks. As a consequence, the offline dimension of cybercrime governance appears to be less violent. On the other hand, this also implies that violence is not always

necessary for a third-party enforcer. The power of information can be just as strong as violence in certain settings.

5. Conclusion

When cybercriminals cannot rely on the government to enforce contracts and maintain order, they must seek governance elsewhere. This chapter examines how governance is established by Chinese cybercriminals to ensure cooperation.

The chapter found strong support for existing studies on cybercrime and governance. However, there are several novel findings that merit emphasis. First, the cybercrime market in China appears to place a stronger emphasis on local IM-based chat groups over formal forums, in contrast to foreign markets. There also seems to be a stronger level of connectivity among these chat groups and forums. Second, the online market structure, which features connectivity among marketplaces, enables better functioning of the reputation mechanism. Third, professional intermediaries are present to provide third-party governance offline. By maintaining an extensive social network, these intermediaries can enforce contracts by disseminating information about wrongdoers, leading to offline communal punishment. In this context, contract enforcement offline doesn't necessarily have to involve violence.

In conclusion, a successful Chinese cybercriminal would utilise the governance systems of both online and offline markets. They would steer clear of random encounters, whether online or offline. When conducting business online, they would exercise caution in selecting collaborators, choosing to work either with reputable criminals and/or making use of the available third-party governance in online marketplaces. They would also strive to build their reputation by maintaining the quality of their products or services, adhering to business norms, establishing their criminal IP, and forging connections in different

marketplaces, be they chat groups or forums. By doing so, they would have a higher chance of gaining access to various closed chat groups and enjoying a more favourable business environment. When conducting business offline, they would primarily work with those with whom they have a pre-established social relationship, whether this relationship was established online or offline. If none of these social relationships exist, they would approach a professional middleman to safeguard their business transactions. Ironically, much like legitimate businessmen, it appears that cybercriminals also require a substantial amount of social skills and integrity to be successful in the criminal market.

Chapter 6. The Firms

The previous chapter explored the dynamics of the Chinese cybercrime industry, focusing on how criminals engage in the trade of goods and services within the criminal market and the pivotal role governance plays in enhancing their cooperation. Some cybercriminals, however, choose to take their collaborations a step further and adopt a more structured form of cooperation.

This chapter concentrates on the cybercriminal firms within the Chinese cybercrime industry, offering an understanding of how these criminal firms are governed. The first section explores the reasons behind the existence of cybercriminal firms. The second section investigates the extent to which these firms operate online and the rationale behind their choices. The third section delves into the analysis of the organisational structures of various cybercriminal firms. The fourth section examines how internal governance is realised within these firms, while the fifth and final section investigates how cybercriminal firms manage relationships with external actors and discusses whether their governance extends beyond their organisational boundaries.

1. Causes of Emergence

In line with existing global research about criminal organisations, the economically driven nature of the cybercrime industry and its hostile market environment provide good reasons for firms to emerge in China (Reuter, 1983; Von Lampe, 2015; Catino, 2019). First, as Coase (1937) and Williamson (1996) have argued, firms improve production efficiency. Most criminal activities that require communication and cooperation can benefit from cybercriminals working closely in a criminal firm to optimise their gains. Rubo, a US-based

cyber security practitioner who has dealt with some cybercrime-related issues in China, explained:

> Most of the cybercriminals we encountered worked in teams. This is because criminal operations often involve a lot of technical elements, and it is difficult and time-consuming for one person to do it all. Also, as I mentioned before, the value of the data used in criminal operations may reduce as time goes by. Criminals need to complete their operation when the value is still high to maximise their profit. Group work is therefore beneficial to them. (US-CSP-1)

Second, replacing market transactions with a collaborative production process reduces transaction costs and controls information flow (Coase, 1937; Catino, 2019). It enables cybercriminals to adopt a sophisticated modus operandi, which subsequently increases the safety of their operation. This strategy appears to work particularly well in China: police in less economically developed areas often find it challenging to tackle complicated cybercriminal operations. Hanling, a local policeman from a remote district of Guizhou Province, said:

> My conclusion is that the ability of our branch only allows us to handle simple cybercrime cases. There is hope if the criminals do not use technology platforms or phishing websites, or their modus operandi is simple. Nevertheless, if the operations are complicated, we cannot do anything. Our ability to tackle cybercrime is still at an elementary, unprofessional level. Also, while countering cybercrime, except for a few provinces, most of the provinces in China are like us. (GZ-P-4)

Lastly, the overall market volatility in the cyber fraud market, due to intensive police strikes against cyber fraud and its related operations in China, encourages the establishment of firms. For example, a series of police crackdowns on the unauthorised sale of telecommunication equipment such as SIMBOX and GOIP in 2020 led to a dramatic increase in their price on the criminal market. It subsequently caused the price of related services, such as machine maintenance and SIM card transferring, to skyrocket (GZ-P-4,

GZ-P-10). As Hanling noted: “At the beginning, the price of a SIMBOX was low, it cost only two or three hundred yuan. But today [after the crackdown] it is worth at least seven hundred” (GZ-P-4). Similarly, Rouxun, a police officer in Guizhou Province, observed that the market price of machine maintenance services tripled in 2020 due to their strikes (GZ-P-10). As with legal markets, fluctuating market prices in commodities and services create high uncertainty. It therefore incentivises cybercriminals to reduce their dependency on the market and form partnerships within a firm structure (Coase, 1937, Williamson, 1996).

In essence, firms are created to circumvent challenges present in the market. Cybercriminals within the cybercrime industry, driven by profit motives, are no different. They adapt to their business environment and take whatever steps are necessary to ensure their survival and prosperity.

2. Online or Offline?

Cybercrime research often focuses on either the online or offline dimension of the cybercriminal operation. It creates the impression that there is a dichotomy between cooperating online and cooperating offline: while cybercriminals with advanced IT skills (the DDoS attackers, the botnet operators, and malware authors) usually cooperate online, the less skilful cybercriminals (cyber fraudsters) cooperate offline (Leukfeldt, 2014; Leukfeldt & Roks, 2021; Lusthaus & Varese, 2021; Lusthaus et al., 2022). This impression, however, is not accurate. The empirical data suggest that cybercriminals cooperate both online and offline in China. In line with Lusthaus (2018), offline and online links are not always clearly drawn. Most cybercriminal firms operate in both the online and offline worlds in the Chinese cybercrime industry.

On the one hand, it appears that some degree of offline element is often present for firms operating primarily online. A former hacker, Haoming claimed that there are certainly cybercriminal firms that operate online, such as some firms that specialise in infiltration. However, he doubted that some firms operate "purely online" and consist of anonymous members who only meet each other in that dimension. Haoming noted: "Yes, there are groups that operate online. As long as there is a unanimous interest, and the group members know each other's capabilities. But in most cases, these people will meet each other offline eventually" (SX-H-1). In line with Haoming, Feiyue, another former hacker, held that the public impression about cybercriminals only communicating online, especially hackers, is mostly inaccurate. He said: "Hackers are humans. They have social needs. But hackers can't only hang out with ordinary people, as they don't understand each other. For example, if I tell you that I just made a shell, you will ask me what a shell is" (SX-H-2). Therefore, members of a cybercriminal firm, despite starting with anonymous online cooperation, may gradually come closer and start to develop offline connections. In addition, Haoming noted that misunderstandings, disagreements, and arguments are almost inevitable in any firm, especially for firms on a large scale or firms that perform complicated tasks. These issues will be amplified online as members cannot talk in person, and therefore the problems cannot be solved efficiently (SX-H-1). Thus, some degree of offline interaction among the members is often needed in an online firm, for better cooperation.

On the other hand, it would also be arbitrary to say that offline firms operate purely offline. Many firms may choose to send their organisational units to different locations and coordinate online for the purpose of avoiding detection (HUB-P-3, GZ-P-4, GZ-P-9). For instance, Mandong, an 'anti-fraud expert' in his local police station, detected a 'business department' of a well-structured 'cyber fraud company' that conducted the 'who am I scam' in 2018 (GZ-P-9). Although the overall structure of the 'cyber fraud company' was unclear

to Mandong, he believed that it had at least three 'business departments': one of them was responsible for collecting personal information, and the other two were responsible for chatting with the victim and conducting money laundering respectively. Keeping its headquarters in a small town, the 'company' sent its 'chatting department' to another city, as Mandong explained:

> Since 2018 we have cracked down on several cyber fraud groups that did the 'who am I scam'. One of them was very professional and had a relatively sophisticated organisational structure. All members in that group were from Dianbai, they had 'connections' in our city and sent some members here. When they came here, they asked someone to rent apartments for them. The apartment they lived in was separate from the apartment they worked in. They worked as ordinary salarymen: when it was office hours, they went to the workspace to make phone calls, and at night they left the workspace and walked around the city. The two apartments were very close. The distance between them was about one or two kilometres. When they commuted to work, they walked separately, 30 to 50 metres apart from each other. Also, they had a strict rule: they were not allowed to take their personal phones to the workspace, and they had office phones that could only be used in the apartment for work. This group was, in fact, a part of a larger group located in Dianbai, and it was only responsible for making phone calls. Their living costs, SIM cards and bank cards were provided by the headquarters in Dianbai. These fraudsters only needed to lure the victims into making transfers to the provided bank account by pretending to be their acquaintances. You knew this scam already, right? When they asked the victim to make the transfer, they provided the bank account that was given by headquarters. The headquarters would do the money laundering and pay them the commission. Moreover, the 'material', which was the victim's personal information, was also provided by headquarters through a Bluetooth printer. After it was connected to the phones, the headquarters could send over the personal information, and they could print it out. Every day their work schedule was like this: they woke up in the morning, ate breakfast, and walked to the office. When they entered the apartment for work, they took out their office phones that were hidden in the fridges and the water tanks and called their headquarters. Then they used the printer to print out a list of victims with their personal information and a list of bank accounts. After that, they started to make phone calls until 4 or 6 pm, finished work, and went home. (GZ-P-9)

In some cases, the organisational units of a firm are located in different jurisdictions to maximise its secrecy, and cooperation among the units is mostly conducted online. For example, in the case of *Wu Junyi re Fraud* (Case No. [2017] Yue 04 Xing Chu No.171)[16],

[16] 吴俊仪诈骗一审刑事判决书, (2017)粤 04 刑初 171 号

while the chatting unit of the cyber fraud firm was in Thailand, two money-laundering units were located in mainland China and Taiwan respectively. Most members of different units had never met, and the cooperation was done online.

Two factors appear to influence cybercriminal firms in deciding the proportion of their online and offline operations. The first factor is the nature of the task conducted by the firm. If a firm's mission is relatively sophisticated and requires frequent communication and good coordination among its members, a more considerable degree of offline interaction is likely to be observed. For instance, cyber fraud firms that engage in government impersonation scams often lean towards offline operations. Their operations often involve various criminals posing in diverse roles. Consequently, they need to collaborate seamlessly and react swiftly in response to the victim's attitude. In comparison, cyber fraud firms that specialise in acquaintance scams and hacking firms may operate with a higher online component since their tasks are relatively individual-based and have a lower requirement for coordination among the members. However, a firm may update its modus operandi from time to time, and the proportion of its online and offline operations may change accordingly (GD-CSP-2, GZ-P-12, GD-P-22, HUB-P-1).

The second factor is the strength of police repression. Lusthaus (2018, p.168) found that offline collaboration among cybercriminals is relatively rare in the West, where stronger police repression is present, and more common in East European countries where levels of repression are lower. A similar observation can be seen in the cybercrime industry in China. Before 2015, when large-scale operations to tackle cyber fraud had not been initiated, various types of cybercriminal firms flourished in small villages and towns in China. The situation changed soon after the crackdown operation when an increasing number of offline firms started to move part of their operation online to avoid detection (Wen & Tang, 2018; GD-P-9, SX-P-1).

In sum, the operation of criminal firms in the cybercrime industry can hardly be defined as purely online or offline. It is rather a mixture of both. A good balance between online and offline operations appears to be the key to success for these criminal firms.

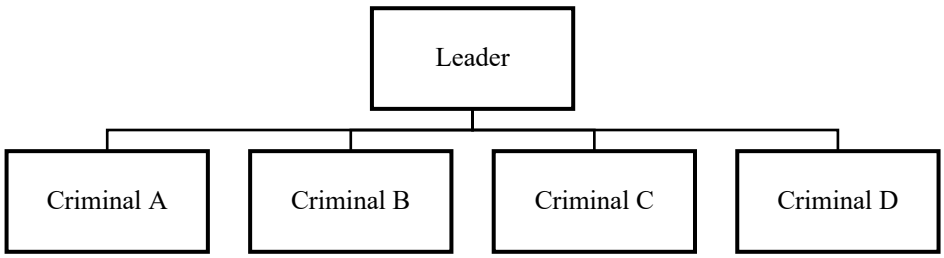
3. Organisational Structure of the Criminal Firms

The previous sections gave an overview of the criminal firms in the cybercrime industry, whereas this section examines the organisational structure they adopt. As Swedberg (2003) noted, no universally applicable organisational structure suits all firms. Firms can take various forms, subject to their situation. Criminal firms are the same. Their organisational structure varies largely on a case-by-case basis (Catino, 2019, p.89). Three distinct organisational structure models of cybercriminal firms have been identified depending on their leadership structure, assigned authority, and division of labour involving the degree to which roles and duties of the employees were designated. I have coined these models the ‘Workshop’ model, the ‘Company’ model, and the ‘Federation’ model.

3.1 The Workshop Model

The empirical data suggest that many cybercriminal firms operate within the cybercrime industry with a structure that resembles the Chinese traditional commercial production unit: the 'workshop'. The workshop model is similar to the ‘horizontal/commission type’ organisational structure adopted by some American street gangs, in which the leadership structure is relatively flat, and the degree of division of labour is rather low (Jankowski, 1991, p.66). Figure 1 below shows the structure of a firm adopting the workshop model.

Figure 1. The Workshop Model



Within the 'workshop model' firms, a leader provides the resources for conducting the crime, including the workspace, crime scripts and tools such as SIM cards and bank accounts, and oversees the criminal operation (HEB-P-1, GZ-P-4). Below the leader, members perform the operations according to the provided blueprint. The degree of division of labour in these firms is low. In most cases, the leader and the members perform similar tasks, and there is no fixed duty for any member. In some circumstances where the members are assigned different roles depending on their expertise, the duties assigned are often interchangeable (GD-P-9). An example of firms that adopt a workshop model can be found in the case of *Sun Hanwei, Sun Hanping & Others re Fraud* (Case No. [2017] Qiong 90003 Xing Chu No.233)[17], which involved a cyber fraud group that conducted the government impersonation scam. The cyber fraud group in this case was formed of six members who lived in a rented apartment provided by the boss. The leader also provided the blueprint of the crime and a set of bank accounts to receive the money transferred from the victims' accounts. In general, the group members carried out the scams independently.

[17] 孙汉位、孙汉平等诈骗罪一审刑事判决书, (2017)琼 9003 刑初 233 号

However, the members assisted each other when necessary, such as when another ‘law enforcement agent’ needed to be present to convince the victims. When other members were involved in a scam, the gain was split equally among the participants. They also helped each other to cash out the profits. The person who cashed out the money took 12% of the sum. Moreover, the members occasionally exchanged favours, including helping each other purchase SIM cards, register SNS accounts, and search for victims.

Cybercriminal firms that adopt the workshop model can also be found in the business sectors of money laundering (GD-R-1, GD-PST-5, GD-P-22) and hacking (SX-H-1, SX-H-5, GZ-P-10). Haoming, a former hacker and a current cybersecurity engineer, explained how cybercriminal firms consisting of hackers specialised in infecting servers and computers might be structured: “An infection team generally consists of three to five members. When there is a task given by the 'exit' [the leader who reaches out for business opportunities], the team members work together to accomplish it” (SX-H-1). Although there are often several stages to an infection process, instead of having a clear division of labour, the members' roles usually overlap when working on a task, and the leader is often involved. Haoming continued: “Most of the time, we start collecting information and attacking the target simultaneously. I may start with a SQL injection, and you may use another method. This is a much more efficient way to perform an attack” (SX-H-1).

As the examples showed, the Workshop model is widely adopted by Chinese cybercriminal firms, including hacking, fraud, and money laundering firms. This model seems to be particularly appealing to cybercriminal firms that are small, consisting of members who are close friends or relatives, and with a business nature that requires a lower level of coordination (SX-H-1). First, cybercriminal firms adopting the Workshop model are relatively small and commonly comprise around ten members (SX-H-1, SX-H-4, GD-P-20). Because of the size of these cybercriminal firms, a more structured and sophisticated

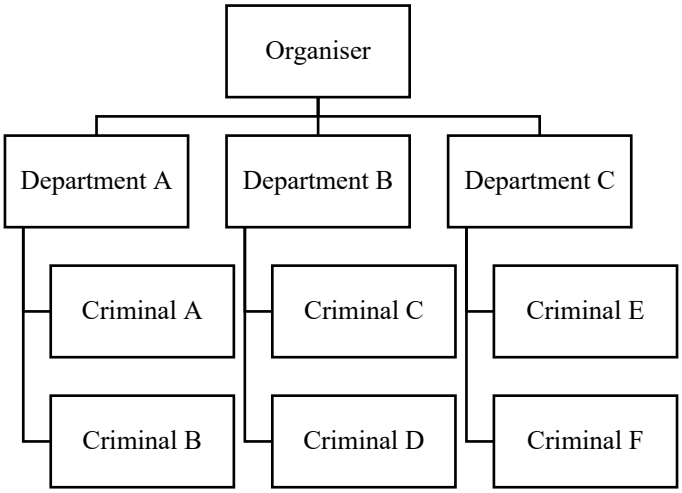
leadership form is simply not needed. Second, since pre-existing bounds exist among the members, a relatively horizontal structure allows the leader to be more friendly with other members. It may therefore avoid conflict between members as the bosses sometimes belong to a younger generation (SX-P-1, GD-P-13). Lastly, as the need for division of labour is relatively low, not assigning specific roles to the members provides more freedom and flexibility.

3.2 The Company Model

In contrast to firms following the Workshop model, some criminal firms adopt organisational structures that closely mirror those of legitimate companies. These 'Company model' firms echo the ‘vertical/hierarchical model’ embraced by American street gangs, where leadership is stratified into several layers and a high degree of division of labour is present (Jankowski, 1991, p.64).

Cybercriminal firms that employ the Company model are often formed by an organiser or a few partners who provide resources for conducting the crime and overseeing the operation. Unlike the Workshop model, in the Company model the organiser or partners do not directly participate in the criminal operation. Instead, they are often responsible for hiring members, repairing necessary resources, and managing the flow of money. Below the organiser and the partners there are several departments. The departments are led by managers appointed by the organiser or the partners. Members in each department are assigned specific duties connected to the operation (SX-R-1, GZ-P-6, GZ-P-2, GD-P-3, GD-P-8, GD-P-11, GD-P-17). Figure 2 demonstrates the structure of a firm adopting the Company model.

Figure 2. The Company Model



According to Liu (2021), the Beijing police cracked down on a 'company' that provided traffic referral services (also known as draining services) to cyber fraudsters in 2021. In essence, they sent out phishing content provided by the cyber fraudsters and attached the fraudsters' contact information. The company was located in an office building, had over 40 members and was registered as a dot-com company that ran an online streaming and marketing business. There were five business departments, namely the media department, the marketing department, the gaming department, the streaming department and the production department, suggesting a high level of division of labour within the firm.

Likewise, Yueyi, the head of an anti-fraud centre at a county-level police station, described a cyber fraud group he had dealt with that used the Company model (GD-P-3). The group specialised in conducting the 'tea leaves scam', Yueyi said:

> In 2018, we uncovered a group of cyber fraudsters who operated in the form of a company in Fujian Province. Inside the company, there was a promotion department, an IT department, and a sales department. The promotion department pretended to be attractive sales representatives, adding clients to WeChat and befriending them. Each of the company members controlled over 25 phones. These people would not take any money from you as this was the company's regulation. They wouldn't even accept your "pocket money" [*Hongbao*] during festivals, so you would think you were talking to an honest person. Eventually, she would reveal this was her business WeChat account and invite you to add her personal account. By doing this, you were handed over to the sales

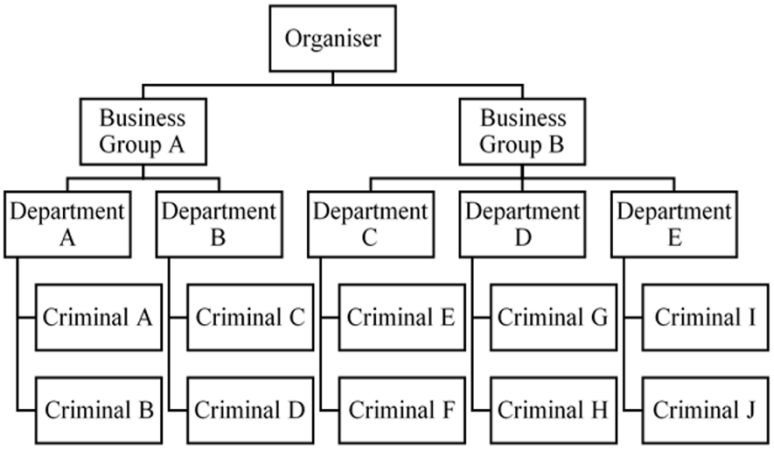
> department. People who worked in the sales department were the "real fraudsters". They would tell you something like: “My grandfather is selling tea leaves, and I am helping him. The tea we sell is all naturally grown”, etc. In the end, they would sell you tea leaves for 800 yuan [approximately $125], and there was a product department that would really send you the tea leaves, but they were worth only 20 yuan [approximately $30]. Lastly, the IT department was responsible for handling the WeChat accounts. Sometimes their accounts were blocked by Tencent [the company that runs WeChat] for their suspicious behaviour, and the IT department tried to resolve the problem. They also maintained the electronic equipment used in cyber fraud, such as phones and computers. (GD-P-3)

Because of the vertical power structure and the clear division of labour, the Company model provides more control and efficiency. Therefore, it appeals to cybercriminal firms that have in a more coordinated format. For example, cyber fraud firms that use a relatively complex modus operandi often adopt this organisational structure.

3.3 The Federation Model

Firms that adopt the Federation model usually consist of an organiser and several mutually independent business groups. Each of the business groups is like a separate firm that operates under the same brand but with its own organisational structure. The independency of the business groups is the biggest difference between this model and the Company model. Like the ‘families’ of a mafia organisation, all the business groups get from the organiser are the necessary resources for the crime. They have to make their own money and periodically give the boss a portion of their gains (Gambetta, 1996; Catino, 2019). As a result, the leader of the business groups enjoys a significant degree of autonomy. They not only have a right to recruit their group members but are also in charge of the operations within their groups. The division of labour in each business group is highly variable among the different cybercriminal firms (GD-R-1, GX-P-1, GZ-P-6, GD-P-10, GD-CSP-2, GD-CSP-3, LECID-1, LECID-2). Figure 3 shows the common structure of a firm that adopts the Federation model.

Figure 3. The Federation Model



A typical example can be found in a confidential case report provided by a subject (LECID-2) about a cyber fraud firm that conducted the 'pig-killing scam'. The cyber fraud firm was founded by a boss who provided resources necessary for a crime operation, such as the crime script, the workspace, and the equipment. The boss appointed an accountant who oversaw the firm and who answered the group members' needs. Below the boss and the accountant, four groups carried out the scam independently. According to their testimony, the group leaders had full control of their groups and acted as partners of the firm. They covered half of the operational costs and took half of the spoils created by their groups at the same time:

> Anyone who was able to recruit 10 members to form a group could apply to become a group leader, and the members he recruited would automatically join his group. The group leader had to cover half of the daily cost of the group members, the cost of the office space and the office supplies, and the other half was paid by the boss. At the same time, the money earned by the group was split equally between the boss and the group leader. However, the group leader also had to pay for the basic salary of the group members. (LECID-2)

On a case-by-case basis, there might be a division of labour within the business groups. For instance, in the case of *Wu Junyi re Fraud* (Case No. [2017] Yue 04 Xing Chu No.171)[18], the cyber fraud firm specialised in the 'government impersonation scam'. The business group members of the firm were divided into three 'lines': the first line impersonated the police who made the first phone call to the victim, the second line imitated other police who were directly in charge of the fraudulent investigation, and the third line posed as a police chief who lured the victim into transferring money to the provided 'secured account'.

The Federation model was found in cyber fraud firms, but not in other cybercrime firms. The business nature of cyber fraud operations may explain this observation. First, as Qiang, a police officer, said, the population in China is large, meaning that cyber fraud firms have many potential victims, not to mention that some victims may be scammed more than once (GD-P-22). Also, as many interviewees noted, by using translation software, cyber fraudsters can extend their tentacles abroad to target foreigners (GZ-P-4, HEB-P-1, GD-CSP-2). This makes the population of cyber fraud victims potentially huge. Thus, each business group of cyber fraud firms can make a profit relatively easily. The boss can earn more profit by having more business groups. In comparison, having more business groups does not necessarily benefit cybercriminal firms that profit by providing illegal services to other criminals. Second, the boss of a cyber fraud firm is more capable of controlling the autonomic business groups. Cyber fraud operations require many resources, including SIM cards, social media accounts, personal information, and bank accounts. Much of these are expendable and need to be replenished periodically. The boss can therefore ensure the business groups hand over their gains by simply controlling these resources. In contrast, although hacking firms also have huge numbers of potential victims, the boss has no

[18] 吴俊仪诈骗一审刑事判决书, (2017)粤 04 刑初 171 号

expenditure resources to offer to his business groups. Thus, these are more difficult for him to control.

Overall, the empirical data suggest that the organisational structures adopted by Chinese cybercriminal firms in the cybercrime industry are not innovative, and are very similar to various organisational structures employed by conventional criminal groups worldwide. This observation should not be unexpected if one recalls the finding that Chinese cybercriminal firms operate in both the online and offline worlds. This finding also echoes existing cybercrime literature that finds profit-driven cybercrime shares much in common with conventional criminal groups (Broadhurst et al., 2013; Lusthaus, 2018; Lusthaus et al., 2022).

4. Internal Governance

Like all criminal organisations, cybercriminal firms cannot rely on legal institutions to maintain their internal order. They must establish alternative governance strategies to control their members. Otherwise, these firms will cease to exist as organisational units. This section examines how cybercriminal firms achieve internal governance.

4.1 Recruitment

Cybercriminal firms operate in conditions of uncertainty, where there is a constant risk of arrest. Therefore, recruiting loyal members is crucial to avoid legal consequences. At the same time, recruiting people who conform to the standards of cybercriminal firms can solve control problems to a large extent (Catino, 2019). Mandong, a police officer, described how an act of betrayal by a member became a breakthrough for law enforcement in tackling a cybercriminal firm: “In order to ensure security, phones must be regularly thrown away to

avoid detection. However, this guy was reluctant to do so. He kept the phones and planned to resell them for money. So we tracked him down, and the group was subsequently taken down" (GZ-P-9).

Kinship and local ties have always played essential roles in the recruitment process for conventional criminal organisations (Hamill, 2010; Gambetta, 1996; Varese, 2001; Catino, 2019). Similar practices have also been found in cybercriminal organisations in the Netherlands, Nigeria and Romania (Leukfeldt & Roks, 2021; Leukfeldt, 2014; Lusthaus, 2018). In line with this cybercrime research, the empirical data suggest that firms in the Chinese cybercrime industry frequently recruit their family members and local friends. The interviewees often refer to this as the *chuanbangdai (传帮带)* practice, which literally means "passing, helping and guiding" (GD-P-2, SX-P-1, GD-CSP-2, GD-CSP-3).

According to Kaile, a young police officer, most cybercriminal firms in China base their recruitment on kinship. He wrote: "When you see a cyber fraudster, it is very possible that his father, his wife, and his brothers and sisters are all involved in cyber fraud. If the fraudster has children, his children may also conduct cyber fraud when they grow up" (SX-P-1). Kaile's statement is supported by several case reports. For instance, in the case of *Shangguan Yingwei, Cai Zheng & Others re Fraud* (Case No. [2018] Yu 238 Xing Chu No.101)[19] , the cyber fraud group comprised six individuals. Among them, two were brothers and another two were father and son. Likewise, in the case of *Zhankangren, Zhanjiayou & Others re Fraud* [20], family relationships within the group were evident – among the seven group members, two were cousins, and another two were a married couple. By only cooperating with relatives, loyalty should not constitute a problem, as there is a strong trust among the members.

[19] 上官英伟才正等诈骗罪一审刑事判决书 （2018）渝 0238 刑初 101 号
[20] 詹康仁、詹家友等诈骗罪一审刑事判决书（2016）浙 0103 刑初 723 号

In addition to recruiting family members, local recruitment can achieve a similar effect, as it largely reduces information asymmetry (Catino, 2019; Pizzini-Gambetta & Hamill, 2011). In the words of police officer Shengjing, locals always "know the leaves and roots" of each other. He further wrote:

> If you are a local, when I ask around, I can easily find out where you live, what you do, and where your family lives. But if you are an outsider, I won't be able to do so. If you are from the Northeast [an area in China]. How do I know your background? How can I ensure that you are not an undercover agent? (GD-P-13)

Because the history and quality of the candidates can be accessed relatively easily, trustworthiness is easier to assess, and the risk of recruitment errors is lessened (Pizzini-Gambetta & Hamill, 2011). At the same time, as Shengjing pointed out, since the novice is recruited locally, both the person and their family members are easy to locate if there is a betrayal (GD-P-13). In other words, both the member and his family are hostages of the criminal firm (Campana & Varese, 2013, p.281).

Not all cybercriminal firms follow the *chuanbangdai* practice in recruitment. Depending on the business nature of the firms, sometimes recruiting strangers is inevitable, especially when the recruitment is based on skills and capabilities. In this case, a more careful examination of the potential candidate must be made. While recruiting, mafia organisations and prison gangs often take a long observation period to assess the candidate's criminal credentials and trustworthiness (Catino, 2019, Skarbek, 2014). This is also the case for most cybercriminal firms in China. In particular, appearance, reflected in personality and manner, such as the way of talking, and performance, represented by skills and achievements (Lusthaus, 2018, p.115), appear to be commonly assessed (SX-H-2, SX-H-5, GZ-P-9, GD-P-20). Feiyue, a former hacker, revealed how a recruitment process might take place:

> The boss often meets hackers through conferences, summits, and competitions such as "Capture-the-Flag". After a certain period of observation, he may find some hackers whom he regularly meets are “willing to talk about anything and capable of doing anything”. Then he will send an invitation to these hackers, saying things like “I have a project, do you wish to help me?” (SX-H-2)

The observation can also take place in a more casual setting and through daily interaction with the candidates. Both Mandong and Yanse, two law enforcement agents, claimed that cyber fraud firms might recruit members from migrant workers who come from other cities. The recruiters often intentionally make friends with migrant workers and assess their criminal credentials and trustworthiness during a period of daily interaction. Once satisfied, the identity of the recruiter is revealed, and an invitation is sent (GZ-P-9, GD-P-20).

In addition, recruitment may happen following a long business relationship, as a certain degree of observation, especially on performance, has already been accomplished during this extended interaction. According to Youlv, a former hacker, after a series of successful business contracts, the boss may treat the desired subject to dinner. This assessment process may repeat several times until the boss concludes the candidate is trustworthy and initiates the recruitment process (SX-H-5).

4.2 Bonds

Binding processes form an essential part of the internal governance provided by cybercriminal firms in the Chinese cybercrime industry. A binding process forms bonds among the firm members, which subsequently discourages opportunistic behaviour and strengthens the social order inside the firms (Catino, 2019; Jankowski, 1991). Catino (2019) pointed out that the more successful a binding process within a criminal organisation, the less necessary it is for the organisation to control its members. Similar to American street

gangs, many cybercriminal firms establish a set of collective values and beliefs as a part of their socialisation process to solidify the group (Jankowski, 1991). Some fraud firms portray their criminal behaviour as a way of surviving in modern society and advocate that ordinary people will never make enough money by doing a regular job. The members also believe that strictly complying with the law and being honest is stupid and useless (GD-P-17). Moreover, they perceive their efforts in fraud to be working hard to make a living and fighting for a better future (GD-P-20, SC-H-1). According to an article published in *The Paper*, a large number of slogans and mission statements were discovered in the office place of a cyber fraud group that was discovered by law enforcement officials, such as, 'Struggle for a better future', 'Are you being lazy at work? Think about your dream, your rent, your parents and your beloved', and, 'You look beautiful when you are fighting for yourself' (Antifraud2, 2019). Similarly, in a confidential case report, a mission statement was also found in a cyber fraud group that was cracked down in Myanmar, which stated: "We are a wolf pack, we work hard, and we are self-disciplined. Helping each other is our spirit. Fighting for ourselves, our family, our brothers, and our future is our goal" (LECID-1).

In addition, as Fengshu pointed out: "the organisations are using the same modern company management strategy as those big companies" (GX-P-1). Team-building activities such as dinner parties, karaoke, travelling, and playing pistol are often held in cybercriminal firms to develop informal relationships among the members and to enhance group coherence (SX-R-1, GD-P-21, GX-P-1, LECID-1). Linjiang People's Procuratorate reported a team-building activity hosted by a cybercriminal firm that acted as both "material dealers" and "account dealers" (Linjiang People's Procuratorate, 2021). According to the report, to celebrate the mid-autumn festival, the firm organised a team

trip to an island. When the police arrived at the hotel where the firm members were staying, most members were playing card games while some were still working on their business.

4.3 Compartmentation

Kostelnik and Skarbek (2013) noted that when members are familiar with the organisation and start to control its resources, they have a stronger incentive to defect. This is because defection becomes more rewarding at this point. Consequently, many criminal organisations, including drug-trafficking entities and terrorist groups, adopt the strategy of compartmentation to address this issue (Kenney, 2007; Hofmann & Gallupe, 2015; Catino, 2019).

In essence, compartmentation is "based on the breaking down of information by allocating knowledge, and the activities related to it, to various units, individuals and/or organisations, making it difficult for one subject, whether internal or external, to form an idea of the picture as a whole" (Catino, 2019, p.268). In the ideal situation, information about criminal activities is wholly concealed. The likelihood of betrayal is low if the members are unaware that what they are doing is illegal and unprotected by the law. The second-best situation is when members understand their activities are illegal, and compartmentation reduces the reward gained from betrayal, therefore discouraging such behaviour. The worst situation occurs when members are arrested by the police, and little information can be offered. Thus, successful implementation of a compartmentation strategy can manage the risk of defection and fortify the internal governance of a criminal organisation.

Cybercriminal firms in the Chinese cybercrime industry widely employ compartmentation. Youpu, a police officer in the local anti-cybercrime department of a big

city in Guangdong Province, described how compartmentation works in some Chinese cyber fraud firms (GD-P-19). According to Youpu, a cyber fraud operation is sometimes broken down into various steps and performed by different units of a cyber fraud firm. The criminals within the units have only the limited knowledge necessary to complete the tasks. In agreement, Yinghua, a police officer, wrote: "The cyber fraudsters are generally divided into units of three to five people. Criminals in each unit do not know the existence of other units. Only the leader of each unit knows how to contact the person who is one level above them when they need new equipment or maintenance services" (GD-P-6).

By employing the strategy of compartmentation, cybercriminal firms can ensure secrecy and reduce the consequence of possible arrests if a member becomes an informant. Officer Yanfang held that compartmentation had made tackling cybercrime difficult. It is very difficult for police to detect the top-level criminals of a firm if compartmentation is employed. "At best we can take down two or three layers of these groups, but we cannot find the top-level bosses. So frankly I have no profile of those top-level bosses," said Yanfang (GD-P-2).

Compartmentation also reduces the incentive for betrayal. Since each member has only limited access to resources – including crime-related knowledge, social connection, and capital — little can be gained from betrayal. Zhuyuan, an experienced police officer who has "fought all kinds of crime", discussed a group of smugglers to provide an example of the situation of compartmentation: "Even if the waterman [a criminal who is responsible for smuggling goods across the border] takes the snake gall [the smuggled goods], he has got no place to sell it, as he doesn't know anyone. So why would he do it?" (GD-P-23). The same principle applies to cybercrime. For some cybercriminal firms, information is concealed to the extent that even their members are unaware that the business is illegal. Officer Yueyi found some cases where a lot of members of the cybercriminal firms were

unaware of what they were doing. He provided an example of how compartmentation had successfully taken place in a cyber fraud firm: "the company [cyber fraud firm] looked legit on its surface, it even had connections with some universities, and the universities had even sent students to the company to do internships" (GD-P-3).

In line with Yueyi, a recent university graduate, Yuqing's experience of being recruited to a cyber fraud firm that conducted the 'investment scam' showed how compartmentation worked by concealing information from its members:

> This was a job that I did for ten months, it was recommended to me by a WeChat friend that I was not very familiar with, but he didn't know this was a cyber fraud group either. When I entered the company, my department only had seven people, and it gradually increased to more than 20. Most of us had just graduated from university. The company moved its location once, and the office environment became much better. The company was a start-up technology company that did business in the field of digital currency, and I was in the department of new media operations. My department was next to the human resources department. There was also an IT department, which was responsible for something like developing an app. When I was there, I did some very basic work, and the salary was not very high – just an average salary for this position. The boss [company owner] told us we were the 'facade' of the company. In the beginning, everything was good, I thought I was doing an ordinary job, and at the end of the year, I was already thinking about the year-end bonus and the year-end party, until one day, the police broke into our office – I thought they went to the wrong door at first. Our company has a branch in Hubei Province. The boss always went there for business. The police seemed to arrest a lot of people there as well. Our branch appeared to be mainly responsible for building online platforms, and my department worked on operating marketing platforms such as the WeChat official accounts. The IT department was developing an app. We had a project that was related to bitcoin and blockchain. Our boss told us that this field had a good future and we needed to attract some investment. I only found out from the police that we had a lot of fake project certificates and a website about some stock, which was developed by the IT department, and the data was manipulated by the boss. At the time, each of us only did one small part of the whole project. None of us knew what other departments were doing, and neither did we know what the end product looked like. The boss just told us: "don't worry, just do your own part. The rest will be taken care of by the others". His office was also separate from us. The boss, the head of the IT department, the human resources department, and the administrative director came from the same area of Shanxi Province, but the victims were mostly from Zhejiang Province. The head of our IT department worked in Beijing at the beginning but was later convinced by our boss to join his team. Only the boss, the head of the IT department, the human resources department, and the administrative director knew what was really happening, and in the end, we were all released. Only four of them were sentenced to life imprisonment. (SX-R-1)

Compartmentation was also applied to temporary workers. The presence of deep compartmentation within the organisation could cause some internal actors to appear quite external. The police often also find it difficult to distinguish internal members of a group from external criminals in many cases (GZ-P-9, GD-P-3, GD-P-8). A case provided by Mandong regarding a machine carrier is one example. In this case, a young person was detained by the police for assisting cyber fraudsters in transferring and maintaining a GOIP machine – a SIM bank used by cyber fraudsters to conceal their calling address. Mandong wrote:

> He [the boss of a cyber fraud firm] posted advertisements online, saying that his company was recruiting casual workers and provided good daily wages. In the advertisement, he didn't say he was committing fraud but made up some random stories. Then there was this kid [young person], who saw the advertisement and went to the interview. During the interview, the boss asked him if he knew how to drive and checked that he was smart enough. Then he told the kid that his job was hotel testing, and he needed to drive another guy to go to a hotel selected by the boss every day and just sleep there. The other guy would take care of the rest. This kid did what he was told. The next day, the boss instructed him to pick up someone, who was also a kid [young person], carrying a suitcase. They went to a hotel and got a room. The kid picked up and opened the suitcase, and switched on a machine hidden in the suitcase, then they just rested. The following day, they went to another hotel and repeated what they had done. After a few days, this kid found the job was somehow strange, as it didn't seem like a hotel testing job but rather something illegal. So, he went on to the Internet and searched for what the machine was. When he found out the truth, he quit the job. (GZ-P-9)

Some cybercriminal firms adopt a crowdsourcing model to recruit a vast number of temporary workers at the same time (SC-H-1, GZ-P-8, GD-P-22, GD-P-20, GD-PST-5, CSCR-3). The most notable examples are various 'point-running platforms' developed by money-laundering firms. In essence, point-running platforms allow users ('point runners') to upload their bank account numbers and the QR codes of their mobile-payment platforms, such as Alipay. The money-laundering firms then provide these bank account numbers and QR codes to cyber fraud firms to receive the money transferred from the victims and use them as a part of the money-laundering process. The point runners earn a commission based

on the amount involved in each transaction. Before the transaction, they are required to pay a deposit equal to the money they will receive. Money laundering firms often portray the platforms as part-time earning platforms in their advertising. As such, many ordinary individuals are unaware that they are assisting money laundering schemes (SC-H-1, GZ-P-8, CSCR-3; Fang, 2021). The crowdsourcing model adopted by the money-laundering firms also exists in several different forms, such as P2P (peer-to-peer) currency exchange platforms (GD-P-22) and digital currency exchange platforms (GD-PST-5) with the same idea. Similarly, the crowdsourcing model is also adopted by some SMS verification firms and CAPTCHA-solving firms to recruit temporary workers (CSCR-5).

4.4 Rules and Punishments

Criminal organisations engage in illegal activities. They therefore cannot resort to the same governing institutions that ordinary people rely on to settle disputes. As an alternative, they create and enforce their own rules to achieve internal governance (Skarbek, 2014; Hamill, 2010; Leeson, 2014a; Catino, 2019; Gambetta, 1996; Varese, 2001; Lusthaus, 2018). Cybercriminal firms in the Chinese cybercrime industry are no exception. They establish implicit and explicit regulations that govern the members' behaviour. Punishments are followed if violations happen (LECID-1, LECID-2, GX-P-1, GZ-P-6, SX-R-1, GZ-P-9).

As noted by Fengshu and Mandong, in many cybercriminal firms, members work as "ordinary employees" (GX-P-1, GZ-P-9). Rules that resemble company regulations of legitimate firms are widely adopted. These rules include office hours, performance indicators, and work discipline. A group leader of a cyber fraud firm wrote:

> Our group members worked between 12:30–17:30 and 18:30–23:30. I checked the attendance every day, recorded who was absent, and oversaw their daily workload. On

> weekdays the members were not allowed to gamble in the casinos, they would face a 2000 yuan (approximately $310) fine each time they got caught […] Work phones and personal phones could not be mixed. During office hours, personal cell phones had to be stored in a bag and hung on a wall. (LECID-2)

Another member from the same firm claimed: "There was a written regulation which stated that we had to add at least five friends on social media. If we didn't hit the target, we had to work overtime for an hour and a half" (LECID-2).

Some firms have a regulation regarding the minimum serving period for new members (GD-CSP-3, LECID-1, GD-P-19). For example, a recruiter of a cyber fraud firm located in Myanmar (one of the countries where a lot of Chinese cyber fraudsters reside; more details about Chinese cybercriminals aboard will be discussed in Chapter 7) testified: "When a newbie is recruited, the treasurer will cover the fees for flights and smuggling. He then must work for us for at least three months to cover these fees" (LECID-1). To enforce such regulation, the recruiter might withhold the members' passports or IDs until the serving period is over (LECID-1, GD-CSP-3, GD-CSP-4).

In addition, members may face violent punishments for serious violations of the regulations. (SC-R-1, LECID-1, LECID-2, GD-P-21, GD-PST-4, GZ-P-4). For instance, Yian, a businessman who stayed in Myanmar for about a year and claimed himself to be "almost involved" in the cyber fraud business, recalled a case when a member was "beaten until his leg was broken" as a result of stealing from the firm (SC-R-1). In some extreme cases, quitting the firm without permission is deemed an act of defection, and violent punishments will follow. Chen, a member of a cyber fraud group, testified in an investigation document: "People from the group told me if I didn't chat with the victims, they would lock me in a cage and throw the cage in water. I have seen people who tried to run and who were brought back and beaten" (LECID-1). Chen's statement was supported by Ling, a police officer who noted that there were cases when the members were forced

to stay in the firm and continue with the crime, as he had encountered a case when a member of a cyber fraud group asked him for help. Ling said:

> I remember a case where we used the victim's phone to chat with the scammer [to try to track him down]. Suddenly, the scammer asked us for help. He said he was detained in Myanmar, and his travel documents were taken. The scam organisation forced him to make phone calls and conduct the scam. We reported the case to headquarters, but I don't know what happened after that. (GD-P-21)

While it's certainly possible that criminals may falsify their degree of involvement, the prevalence of such claims indicates that violent punishment is likely to exist. However, all of the violent incidents reported in the empirical data occurred within cyber fraud firms located abroad. But not all cyber fraud firms located abroad use violence. For example, in the case of *Wu Junyi re Fraud* (Case No. [2017] Yue 04 Xing Chu No.171)[21], one offender worked with a cyber fraud firm based in Thailand for two months before deciding to leave. He faced no violent retribution, merely forfeiting the wages he would have earned during his two-month tenure. This evidence indicates that the use of violence may not be a universal practice and could be relatively rare among all firms.

5. External Governance

Firms do not operate on their own. They form business relationships with other market actors in the cybercrime industry. As Kostelnik and Skarbek (2013, p.97) claimed: "For criminal organisations to provide governance, they must solve the organisational and strategic problems of internal and external cooperation". Conventional criminal organisations commonly use threats of violence to establish order while interacting with

[21] 吴俊仪诈骗一审刑事判决书, (2017)粤 04 刑初 171 号

other actors in the community (Hamill, 2010; Skarbek, 2014; Gambetta, 1996; Varese, 2001). This observation is also evidenced in certain cybercrime cases where defectors faced violent retaliation (Lusthaus, 2018; Lusthaus & Varese, 2021).

The empirical data found some incidents when cybercriminal firms try to regulate some aspects of their external relationships. According to Haoming, a former hacker, because cybercriminal firms have broader social connections, more members, and are often wealthy, they could therefore utilise both the threat of violence and "soft violence" to ensure the continued cooperation of their partners (SX-H-1). Haoming said:

> Many firms in the cybercrime industry are akin to traditional criminal groups. Violence against the cheater is possible if there are enough members who can fight or if they are willing to pay money to the local gangs. However, nowadays, people are much more civilised. Breaking your arms and legs is less likely. Instead, they may use soft violence, such as putting excrement on your door. (SX-H-1)

Echoing Haoming's statement, the testimony of Yang, a 'driver' (money mule), reveals his fear of retaliation. Yang was recruited by a water house (money-laundering firm) and ultimately arrested by police. During the interrogation, Yang mentioned that he never dared to take more money than he could gain from these services. He said: "Shuige [the nickname of the boss] can find out the detailed information about my family and me. If I take his money, I know he will take action to retaliate" (LECID-3).

Studies of traditional criminal firms found that they had a tendency to become predatory and start extracting resources from market actors. Such a tendency, however, can be constrained by the feature, goal, and internal motivation of the groups (Skarbek, 2012; Lessing, 2021). The predation tendency was not observed in the case of cybercriminal firms in China. Cybercriminal firms seem to have no intention of governing market actors that have no business connections with them. Conflicts between firms and individual criminals who are not in business relations are rare, and the relationship between these actors is

generally friendly. The firms may even help each other and share crime experiences (SC-R-1, GD-P-17, SX-P-1). Three essential elements that differentiate cybercriminal firms from other traditional criminal firms may be the possible explanation. First, cybercriminal firms are not specialised in violence. Although they may apply violence to threaten their members and market actors in order to prevent defection, their power is often not sufficient for them to act predatorily. Second, the income of cybercrime firms does not come from taxation. Taking over other firms or internalising individual market actors does not directly increase their income. Adversely, as discussed above, most cybercrime firms tend to keep to a relatively small size to balance the profits and the degree of concealment. Lastly, cybercrime can be done across territorial boundaries. Cybercriminal firms can easily purchase products online and seek victims across the country. As a result, it is unnecessary for cybercriminal firms to fight for resources, and firms can interact peacefully.

6. Conclusion

This chapter provided insight into the cybercriminal firms within the Chinese cybercrime industry, offering an understanding of why these firms are formed, how they are structured, how they are governed, and how they interact with external actors. Overall, cybercriminal firms have emerged to increase operational efficiency, counteract market volatility, and navigate other external challenges. They adopt different organisational structures and balance the online and offline proportions to adapt to their task environment and business need. Beyond the infrequent use of violence, the strategies cybercriminal firms employ to achieve internal governance are not markedly different from those adopted by legitimate firms. When compared to traditional criminal organisations, they also show minimal predatory tendencies, as they rarely express interest in governing market actors outside

their immediate business connections. Overall, cybercriminals firms appear to share many similarities with legitimate firms. This finding supports the application of economic theories to understand the behaviour of cybercriminal firms.

Chapter 7. The Protectors

The previous two chapters examined how governance is achieved within the structure of markets and firms to define property rights, enforce agreements, resolve disputes, and create order. They identified forum administrators and professional middlemen as protectors who provide some level of third-party governance service to cybercriminals. They also found that cybercrime firms, despite dedicating themselves to the creation of a strong sense of internalised control, have little intention of taking broad control of the industry. So far, the focus has been on cybercriminals; this chapter turns to the traditional protectors and examines whether they have a role to play in governing the cybercrime industry.

Research into criminal governance in conventional criminal industries has found that capable protectors can not only define and enforce property rights and adjudicate disputes but can mitigate the harms of externalities, including predatory behaviours from rivals and threats of state repression (Gambetta, 1996; Catino, 2019; Wang, 2017; Shortland, 2019; Kaplan & Dubro, 1986; Varese, 2001; Lessing, 2021, Skarbek, 2011). Taking kidnapping as an example, Shortland (2019, p.27) listed what a capable protector could help with the terms of a criminal industry's operation:

> A capable protector can offer a safe location to hold the hostage and from which to communicate without being apprehended. Police or military commanders need to weigh the human and financial cost of forcibly entering informally controlled territory against the benefits of an attempted rescue… Opportunities, police and rivals would not dare to enter the protector's territory to intercept the payment, but the messenger with the ransom will be protected from harassment.

Organised crime, corrupt government agents, and local armed groups have also been identified in these studies as common protectors. Deepening this stream of research, the following three sections inspect the role of these traditional protectors and assess their

degree of involvement in protecting cybercriminals. The first section investigates the role of traditional organised crime groups in cybercrime, and posits that their role as protectors in China's cybercrime industry is minimal. The second section assesses the role of corrupt state agents in China and argues that they have contributed substantially to the success of the Chinese cybercrime industry in the past decade. The third section looks into oversea protectors and maintains that they hold a significant position in the recent movements of Chinese cybercriminals. The fourth and final section highlights the findings and critically discusses them in light of existing studies on crime and governance theory.

1. The Role of Organised Crime Groups

Organised crime groups have been found active in providing protection services in various criminal industries, such as prostitution, gambling, and drug distribution (Wang, 2017; Catino, 2019; Gambetta & Reuter, 1995; Gambetta, 1996; Varese, 2001; Chu, 2002; Kaplan & Dubro, 1986). However, a recent study suggests there is little involvement of organised crime groups in the cybercriminal industry (Lusthaus, 2018).

In agreement with Lusthaus's finding (2018), the empirical data provide little evidence to show that organised crime groups provide any form of protection to cybercriminals. Most interviewees argued that organised crime groups and cybercriminals have little interaction according to their professional experiences. For instance, Kangjian, a police officer, outlined: “Cybercriminals generally do not talk to traditional criminals. Paying protection fees to mafia does not happen” (HEB-P-1). Similarly, Xingan, another police officer, provided: “Cybercrime is now very civilised. Cybercriminals generally do not pay protection fees to the Mafia. Many cybercriminals know each other well, and they often share information and experience of success with each other” (GD-P-16). Only one

interviewee, Haoming, a former hacker, mentioned the potential existence of violent enforcement services provided by the Mafia: "In my city, if you have money and are willing to spend it liberally, such as spending 100,000 yuan as if it were only 10 yuan, you can get the Mafia to take actions against those who have betrayed you" (SX-H-1). However, he himself didn't know exactly where to locate these mafia groups. He also had neither used the mafia enforcement services nor heard of any disputes between cybercriminals where mafia members were involved. Therefore, his statement is rather speculative. This shows that the overall degree of mafia involvement in cybercrime, if there is any, is low.

The empirical data find three possible explanations for this observation. The first explanation is associated with the distinct character of the cybercrime market. Studies on organised crime and private protection have found that some markets are more easily penetrable than others. These markets often feature unskilled labour, a high level of competition, a low level of technological development, and replaceable goods and services (Catino, 2019; Gambetta & Reuter, 1995; Varese, 2001). The drug distribution, prostitution, and gambling industries are a few examples that conform to the above features (Wang, 2017; Gambetta, 1996; Chin, 2009; Varese, 2001; Chu, 2002; Kaplan & Dubro, 1986). For Gambetta and Reuter (1995, p.128), when "the barriers to entry are low, and to avoid competition, mafia organisations are invited by entrepreneurs to keep out new entrants and enforce the agreement among cartel members". However, the cybercrime industry does not have many of the above elements. The empirical data suggest that there is a lack of competition within the industry. Speaking of cyber fraud, Xingan said: "One reason [for a lack of organised crime involvement] is that the market in China is way too big. There are 1.4 billion potential victims in China. There is little competition" (GD-P-16). This may explain Lusthaus's (2018) finding that cyber fraudsters are "somewhat friendly with each other". There is also little competition for businesses that support cyber fraud. On the one

hand, goods that facilitate cyber fraud, such as SIM cards and compromised credit cards, are consumables. Cyber fraudsters need to frequently change them to avoid police detection. The demand is therefore huge (SX-H-1, GZ-P-9, GZ-P-8). On the other hand, many goods and services can also be used in other legal and illegal business scenes. For instance, stolen personal data are widely used in private-detective and telemarketing services (SX-H-2, GZ-P-10, GZ-P-6). Compromised credit cards are also needed for various criminal activities, such as online gambling (GX-P-3). What's more, cybercrime requires skills and expertise. To sufficiently handle disputes, one must have a good understanding of the market. In this aspect, traditional organised crime groups cannot compete with professional middlemen who used to be elite cybercriminals. As a result, the cybercrime industry is difficult for organised crime groups to infiltrate.

The second explanation relates to the concealment of cybercriminals. The operation of organised crime groups relies heavily on territorial control (Skarbek, 2012; Varese, 2011). For many traditional crimes, criminals reside in a fixed place and carry out their illicit activities locally. Their activities are also readily observable by mafia members with good local information networks. But the activities of cybercrime are more hidden. The existence of online marketplaces also enables goods and services to be provided across spatial boundaries. Therefore, cybercriminal firms may pose as legitimate companies and operate in office buildings. Cybercriminals may also sit in random apartments and conduct their business remotely. Therefore, it is difficult for the Mafia to locate them, as Kangjian said: "They [the cybercriminals] simply do not let anyone know what they do" (HEB-P-1). In agreement with Kangjian, Xiangan wrote: "Cybercriminal groups often work in office buildings and pose as legitimate companies. The Mafia has no idea what they are doing" (GD-P-16).

The last potential explanation is connected to China's anti-crime and anti-corruption campaigns in recent years. As discussed in Chapter 3, during the past few decades, China has reinforced its efforts to fight traditional street crime. By using cutting-edge technology and increasing the number of CCTV cameras, the police have imposed a significant threat to traditional criminals who commit crimes on the street. These measures have subsequently reduced the operational scale of organised crime (GD-P-22, GX-P-3, GZ-P-4). The recent campaigns targeting organised crime in China have further weakened the power of organised crime groups. In 2018, China launched the 'Special Criminal Syndicate Combat' to crack down on organised crime (Notice on Launching the Special Criminal Syndicate Combat, 2018). According to the the State Council of the People's Republic of China, the Chinese police have busted 15,319 mafia and mafia-style groups, with aorund 237,000 criminals involved between 2018 and 2021 (Ren & Liu, 2021). China also started an anti-corruption campaign in 2012 that aimed to crack down on corrupt government officials – the 'protective umbrellas' that protect local gangsters. Although the campaign has attracted much criticism, there has been the successful destruction of a number of politico-criminal nexuses, including Zhou and Wen Qiang's group (Wang, 2017). Consequently, the scale of organised crime has generally decreased in China, and organised crime is now incapable of providing large-scale protection services.

That said, organised crime groups can get involved in cybercrime in ways other than providing protection. Lusthaus (2018) has identified three main ways for organised crime groups to engage in the cybercrime business other than providing protection: being an investor, being a service provider, and getting directly involved. While there is overall little direct evidence pointing to the engagement of traditional organised crime in the cybercrime industry, the interview data offer some speculations that seemingly support Lusthaus's findings. First, the participants were often unsure of the identity of the leaders of many

large-scale cyber fraud firms located abroad. Many of them seemingly knew of or shared the names of the owners of some casinos (GD-CSP-2, GD-CSP-3, SC-R-1, GZ-P-6). Considering that investing in the gambling industry has been a common practice for many traditional organised crime groups (Chu, 2002; Catino, 2019), it is possible that these large-scale cyber fraud firms are also owned by organised crime. Moreover, some members of cyber fraud firms located abroad were illegal immigrants (GD-CSP-4, LECID-1, LECID-2). In a confidential investigation document, a cyber fraudster described her journey to a cyber fraud firm during the interrogation. She said:

> At that time, I flew with several strangers from Xiamen to Longdongbao in Guizhou, then took a connecting flight to Xishuangbanna [the border between China and Myanmar]. Upon arrival, there was a car to pick us up, taking us to the foot of a mountain. Then we took motorcycles to [smuggle us to] our destination. (LECID-1)

While it is not clear whether the smuggling process was arranged by the cyber fraud firms, there might be organised crime groups specialised in human smuggling that provide this service. Finally, Qiubai, a police officer who works for the department of counter-organised crime, described to me a so-called 'trap loan' operation:

> A typical form of mafia-cybercriminal nexus is called the "trap loan". This is done when cybercriminals develop online lending apps, promote them online, and attract victims to sign lending contracts with them. After the victim signs the contracts, the cybercriminals use technical means to stop victims from paying back the money in due time. The excessive penalty interest occurs, and the Mafia later shows up and forces the victims to repay the loan. (GD-P-15)

Although it is arguable whether the 'trap loan' operation can be grouped into the category of cyber fraud and subsequently fall under the scope of cybercrime, this example demonstrates that there are at least some attempts by traditional organised crime groups to engage in internet-related activities.

2. The Role of Corrupt State Agents in China

In addition to services provided by organised crime groups, criminals commonly need to seek protection from state agents to mitigate the risk of apprehension. Even organised crime groups – the protectors – are no exception (Wang, 2017; Varese, 2001). Wang (2017) described the broad existence of corrupt state agents – the 'red mafia' − who act as a 'protective umbrella' to safeguard the criminal operation of various street criminals, including organised crime groups. In line with Wang, the empirical data found traces of protection provided by corrupt state agents to cybercriminals in China in the past decade.

In 2015, the Ministry of Public Security listed 18 cyber fraud hotspots in China, with almost all being the site of a representative scam (Wen & Tang, 2018). These areas included both cities and counties/regions, as summarised in Table 1:

Table 1: Cyber Fraud Hotspots and Representative Scams

Number	Province	City	County/Region	Representative Scam	Year Announced
1	Hebei	/	Fengning	Mafia Scam	2015
2	Jiangxi	/	Yugan	Child Begging Scam	2015
3	Fujian	Longyan	Xinluo	Online Shopping Scam	2015
4	Anhui	Hefei	/	Auction Scam	2015
5	Guangdong	Maoming	Dianbai	Who am I Scam	2015
6	Liaoning	Anshan	/	Fake Medicine Scam	2015
7	Henan	/	Shangcai	Fake Army Scam	2015
8	Hubei	Xiantao		Government Impersonation Scam	2015
9	Hunan	/	Shuangfeng	Photoshop Scam	2015
10	Guangxi	/	Bingyang	QQ Scam	2015
11	Hainan	Danzhou	/	Fake Ticket Scam	2015
12	Sichuan	Deyang	/	/	2015
13	Fujian	/	Anxi	/	2017
14	Fujian	/	Nanjing	/	2017
15	Hubei	/	Xiaochang	Credit Card Scam	2017
16	Guangdong	/	Raoping	Game Card Scam	2017
17	Guangxi	/	Luchuan	Lottery Scam	2017
18	Hainan	/	Dongfang	Game Currency Scam	2017

These hotspots were also commonly recognised among the law enforcement agents and cybersecurity professionals interviewed. Terms such as ‘high-risk areas’, ‘hard-hit areas’, and ‘capping areas’ were frequently mentioned by the interviewees. An experienced police officer or a cybersecurity professional who worked in fraud could immediately find out the criminals’ location after reading through the case report or hearing about the *modus operandi* (SX-P-1, GD-P-9, GD-P-12, GD-CSP-3). Some could even enumerate six or seven of these hotspots without thinking. For example, Xiangwei, a former police officer and a current cybersecurity professional, provided me with some examples about the cyber fraud hotspots without hesitation:

> For example, in Bingyang, Guangxi Province, criminals do the QQ scam; then in Dongfang, Hainan Province, criminals do scams on online games. They make video game advertisements and tell people they could purchase game cards or in-game currency for a low price. They only make a small amount of money though. Also, in Hunan Province, criminals do the Photoshop scam. They use Photoshop to make fake photos of company leaders having affairs, then send them to the company and threaten them for money. (GD-CSP-3)

The core geographic units of cyber fraud cases were seemingly the villages within these hotspots. In contrast, the centres of these areas were relatively peaceful, with many locals being unaware of the situation until their hometown appeared in the hotspot list (Wen & Tang, 2018). Data collected from the interviews also confirmed the finding. Zhimei wrote:

> Most people conduct the scam in rural areas. People would make phone calls in the mountain and cash out the money in the village […] You can imagine the situation of drug trading, that the whole village is selling drugs. (GD-P-10)

At the peak, there were numerous ‘fraud villages’ in each hotspot, and most people in the villages were involved to a certain degree, as Fengshu described:

> People who lived in these villages were very self-disciplined: every day after dinner, people didn't play Mah-jong [a tile-based game that is popular in China], nor did they drink alcohol or make trouble. They all sat down in front of their computers: typed, scammed the victims, and made money. (GX-P-1)

In some villages, gathering to exchange scam experiences even became a fixed daily activity. A family who missed out on a gathering would be seen by the other families as not being rich enough (GD-P-13). In addition to the activity of fraud, cybercrime businesses that facilitate cyber fraud, such as SIM card dealing and CAPTCHA solving, also flourished in these villages (GX-P-1, GX-P-2, GZ-P-6, GZ-P-10, GZ-P-12). Zhenqiang, a police officer, said:

> Taking Bingyang county as an example. In the beginning, there was a great demand for telephone trojans to control the victim's phone, so some people in our county got involved in hacking. When the QQ scam became popular in the county, some local people started selling bank cards and SIM cards. Later when the requirements on registering SIM cards and bank accounts became strict, people who lent out their SIM cards showed up…There were also people who began to provide draining and marketing services for cyber fraudsters. (GX-P-2)

The prevalence of cybercrime in these villages was strongly associated with the protection offered by the local government agents, including government officers, police officers, prosecutors, and judges. These government agents not only turned a blind eye to the criminals, but also actively hindered operations taken by police from the outside. Under the acquiescence of the local government agents, villagers formed self-protection units. When police from the outside went to these villages to arrest suspects, villagers would try as much as they could to resist by destroying evidence or hiding the targets (SX-P-1, GD-CSP-3). On the other hand, the local government agents informed the criminals about the forthcoming operations from the outside (GD-CSP-2, GD-P-9). As a result, police from the outside often struggled when they had to arrest people from these villages. For instance,

Xiangwei, a cyber security practitioner who works closely with the police to fight cybercrime, explained:

> If you go to those places [the cyber fraud hotspots], it is highly possible that you can't arrest anyone. Even if you get him, you wouldn't be able to get out of the village. The government and the police are all involved. We have been to some villages to arrest someone before; right after we took him, a bunch of villagers surrounded us. They just took away the person we caught and ran away. (GD-CSP-3)

Kaile gave the same statement:

> In those areas [the cyber fraud hotspots], the local governments were really uncooperative [...] They brought us a lot of problems […] To give you a simple example: when you entered these villages and wanted to arrest someone, many people would show up and try to hinder you. They would give you fake evidence or even destroy it. (SX-P-1)

As the empirical data showed, the scale of local protection appears to be prominent in these hotspots. The formation of large-scale local protection in these villages can be attributed to three main factors. The first is the prevalence of *guanxi* practices in these villages. *Guanxi*, as mentioned in Chapter 2, is a unique reciprocal relationship between individuals in China. A *guanxi* practice is a practice of reciprocity and favouritism that surpasses formal institutions (Wang, 2017; Jacobs, 1979; Fei, 1992; Fan, 2002). To establish a *guanxi* relationship, individuals need to acquire a proper *guanxi* base through kinship and family ties, common social identities, common third parties, and anticipatory bases. In addition, activities such as bribes that facilitate the further development of the *guanxi* relationship are also necessary on some occasions, especially when the *guanxi* base is not solid enough (Fan, 2002). In the case of cyber fraud hotspots, the geographical feature of Chinese villages enable criminals to easily identify *guanxi* bases with government agents, as many government agents are socially connected to them. Some may be close or distant

relatives, and others may attend the same schools or share friends (GD-P-13, GD-P-5, GD-CSP-3, SX-P-1). In some cases, a solid *guanxi* base between criminals and government agents is sufficient to establish a *guanxi* relationship and trigger *guanxi* practice. For example, Kaile held: "Simply because of the existence of kinships and close friendships, many agents are reluctant to take action against them" (SX-P-1). Agreeing with Kaile, Daihui added: "[Within the *guanxi* base] there is a common ideology of 'this is our people', and the state agents feel obligated to protect them" (GD-P-5). In other cases, further transactional activities or interpersonal interactions are needed to establish a proper *guanxi* relationship (Wang, 2017, p.161; Fan, 2002). Paying a monetary bribe is one of the most common strategies. Zhimei said: "Have you realised that the villages are all located in remote areas? They are poor and famous for being lawless […] The government agents just openly accept money from people and do them a favour" (GD-P-10). Under the *guanxi* practice, a state agent has a strong sense of moral obligation to act in favour of the criminals with whom he has established a *guanxi* relationship. This moral obligation often subverts their official duties and formal institutions.

The second factor is political consideration. When the cybercrime industry proliferated in villages, local government agents were concerned that a large number of arrests and convictions would bring a bad reputation to the region, which might subsequently affect the local economy and their own prospects of promotion. Therefore, they were unwilling to work with police from the outside to tackle local crime. The outcome consequently formed a vicious circle. Kaile's statement illustrated this point:

> Speaking about local protection, the local governments do not like the outsiders. They do not cooperate with you when you try to arrest people there. Because in their mind, it is like this: "Okay, you are taking my people and claiming they are guilty of the crime. Putting aside my potential *guanxi* relationship with the people you want to arrest, you are saying that there are a lot of criminals in my area." The potential reputational damage itself can form a motivation for them to be uncooperative. (SX-P-1)

The final factor is the economic factor. As stated by many participants, most hotspots had a poor local economy, leading to other social issues (GX-P-2, GZ-P-10, GD-P-4, GD-P-9, GD-P-10, GD-P-11, SX-P-1). Although the proliferation of cybercrime and the increased number of cybercriminal firms caused damage to the national economy, the victims were not the local people. The flourishing of cybercrime, on the other hand, solved local employment problems, reduced street crime, and increased local taxation income. As a result, there was an incentive for local government agents to shut their eyes to cybercrime, if not act in support of it (GD-P-9, GD-P-10). Jinghuai, a police officer, said: "Why would they [the local governments of the cyber fraud hotspots] want to stop cybercrime? Cybercrime increased the local taxation income and stimulated economic growth. You see, there was the soil for cybercrime to grow in these areas" (GD-P-10).

Local protection by the government seemed to last only until 2015, at which point the Ministry of Public Security decided to initiate a large-scale 'uncap' operation to tackle cyber fraud. The operation involved identifying cyber fraud hotspots and setting deadlines for the local governments and police bureaus of these hotspots to deal with these problems under public supervision. If the issues were not solved by the deadline, restrictions on promotion would be imposed on the local government officials, and some might even be dismissed (GD-P-10, GD-CSP-2). Therefore, according to Zhimei, the local government did a 180-degree turn in terms of their attitude. In some areas, the local government even adopted brutal enforcement measures such as knocking down the houses of repeat offenders (GD-P-10). As a consequence, many cybercriminals left their hometowns and went abroad, soon discovering that the same or an even greater level of protection could be found overseas.

3. The Overseas Protectors

Following the national anti-cyber fraud operation, while many cybercriminals were broken up into parts and moved to different cities around the country, some chose to seek opportunities abroad. The most mentioned country where Chinese cybercriminals reside is Myanmar (GD-CSP-2, GD-CSP-3, SX-R-1, SX-H-1, SX-H-2, SX-CSP-2, GD-P-11, HEB-P-1, GX-P-1, GX-P-3, GD-P-15, GD-PST-3, GD-PST-4). According to the participants, in areas such as Kokang, Shan State, Kachin, and Mengla, the cybercrime industry is so flourishing that the criminals openly operate on a large scale in the fanciest building in town. Xinxue, a police officer, stated:

> I went to Dehong once. It is a Chinese town bordering Myanmar. There is a river about five metres wide, and the cybercriminals are just over the river... We found some local guys to bring us over the border to Myanmar. When we got there, they introduced the subject of the buildings we saw from the other side of the river. These guys were all aware that it was a den of cybercriminals. We landed in front of a casino called Xinhe casino, which was the most famous casino in the town. The casino was like this: the first two floors were a casino, then there were seven floors; from the third floor up, each floor was a den of cyber fraudsters. (GZ-P-6)

Echoing Xinxue, Xiangwei believed the operation of cybercrime in Myanmar, run by Chinese cybercriminals, is as "mature" as it is in China. These are not random individual criminals who escape from China and conduct petty scams, but well-organised criminal firms. Xiangwei wrote:

> The cybercrime industry in Myanmar is as well-developed as in China. I am not talking about a few individuals who hit and run, but a sophisticated industry. There are many firms that do scams and also firms that support scams. Criminals even bring chefs from China just to cook for them. (GD-CSP-3)

Sharing a similar culture and language with China is one reason why Chinese cybercriminals have moved to Myanmar. In the Wa area, for instance, Chinese nationals form a significant proportion of the population, and Chinese is spoken everywhere (GX-P-1, GD-P-15, SX-P-1). Kaile wrote: "There are many Chinese people in the Wa area. Chinese yuan is basically the common currency in Wa. Living there is not much different from living in China" (SX-P-1). This statement is consistent with Chin (2009), who conducted research into the Wa area about the modern drug trade. In his research, he described Bangkang, a town in the Wa area, as follows:

> These days Bangkang looks and feels more like a town in China than like one in Myanmar. Because there are a large number of Chinese in Bangkang, Mandarin is the most popular language; most of the store signs are in Chinese characters and if some are in Chinese and Burmese characters, the Burmese characters are often misspelled and nobody seems to notice or care. (p.30)

The population structure and the ubiquity of the Chinese language provide a solid foundation for cybercriminals to live and operate in Myanmar at the lowest cost.

Another reason for Chinese cybercriminals to gather in Myanmar is its geographical proximity to China. Because it borders China, the cost for Chinese cybercriminals to travel to Myanmar is low. According to Xiangwei, in off-peak seasons, a return flight between Myanmar and China would cost less than 1000 yuan (GD-CSP-3). Moreover, as mentioned above, many Chinese cybercriminals in Myanmar are illegal immigrants. Smuggling into Myanmar from China is also an easy option. Ningxin, a cybersecurity practitioner who cooperates with the police to conduct foreign cybercrime crackdowns, wrote:

> Smuggling to Myanmar from China is so easy. We went to Yunan Province to inspect the geographical feature. The border line is very long between Myanmar and China. It is even hard to say there is a border in certain towns: the farmland of a Chinese family could be right next to the farmland of a Burmese family. People can easily cross the border by riding a bicycle. (GD-CSP-2)

In agreement with Ningxin, Xueman, a prosecutor, added that smuggling is a more popular way to access Myanmar:

> In almost all cases I encountered, the criminals were smuggled across the border; none of them went there the formal way, perhaps for economic consideration. The cost of human smuggling is relatively cheap. They first take buses to the border cities, then change to motorcycles, and finally walk over the mountains to get there. (GD-PST-4)

Its accessibility enables Chinese cybercriminals to move in and out of Myanmar easily. Many of them stay there for crime and come back home for a family gathering during festivals. Thus, many participants likened the movement of cybercriminals to the movement of labour (GD-CSP-2, GZ-P-12, GD-CSP-4). There is also a concept called 'striking the backflow' among the police, which refers to arresting these cybercriminals when they return to China (GZ-P-6, GZ-P-10).

Nevertheless, the most crucial reason Chinese cybercriminals choose Myanmar is that they obtain a high level of protection from the local armed groups. Across all the interviews, the most common image evoked to describe Myanmar's local politics is that of complexity. According to the interviewees, the local political environment is highly complicated. There is not only the government that oversees the areas but also independent local armed groups who have equal or even more significant power in their local areas. The local government or military groups often protect the cybercriminals in return for protection fees (GD-CSP-2, GD-CSP-3, GD-P-15, GD-P-16). Ningxin wrote: "The local armed groups make money by protecting the cybercriminals. Just like what they did to the drug farmers and drug traders. Upon receiving the protection money, they promise the criminals that they won't be arrested by the Chinese police" (GD-CSP-2). Because of the protection, arresting criminals in Myanmar is not easy for the Chinese police. Negotiations involving benefit

exchanges and monetary bribes are often needed. Speaking of the concept of 'striking the backflow', Xinxue, a police officer, elaborated:

> Why do we strike the "backflow"? Because if the criminals are abroad, especially in Myanmar, you cannot simply go and arrest people. In Myanmar, the criminals often reside in areas controlled by the local armed groups. They do not listen to the government. In Shan State, for example, if we want to arrest criminals from there, we have to use various methods to "negotiate" with the boss of the local armed groups. When the deal is made, we tell them to bring the criminals to the border and we take them from there. (GZ-P-6)

Concurring with Zhimei, Xueman, a prosecutor, described an unpleasant crackdown operation conducted by the Chinese police in Myanmar:

> The cybercriminals were protected by the local armed groups. Before the police got there, the local armed groups informed the criminals, and the criminals ran away. So the police could only arrest people who were part of the deal. Even if the police knew that other cybercriminals were operating in the neighbouring block, they couldn't get them. (GD-PST-4)

What's more, some participants also reported that there are local armed groups who directly participate in cybercrime by investing in it (GD-CSP-2, SC-R-1, GD-P-14). For instance, Ningxin held:

> In some cases, there are inextricable links between local armed groups and cybercriminals. The last time when we tried to arrest criminals in Myanmar, the cybercriminals swaggered in front of us and walked straight into the local armed group boss's house. Only later, we find out that the cybercrime group was, in fact, bankrolled by the boss's wife. (GD-CSP-2)

Two political and economic factors may be the most relevant to explain why local armed groups protect cybercriminals or even directly participate in cybercrime. The first factor relates to local development. Fengshu, a police officer who works in a Chinese city neighbouring Myanmar, believed the political environment in Myanmar to be a key driver

of cybercrime proliferation (GX-P-1). According to Fengshu, the political conflict between different armed groups and the local government in Myanmar create a strong demand for the local armed groups to acquire money to maintain their military power. Protecting and taxing cybercriminals is one of the fastest and easiest ways to achieve this goal. In line with Fengshu, Siwen, another police officer from the same city, added that part of the 'tax income' from protecting cybercrime is also used to build public facilities in these regions, such as roads, schools, and hospitals. Local development can therefore benefit from protecting cybercriminals (GX-P-3). Furthermore, Yian claimed that the proliferation of cybercrime could assist the development of the local economy. There is a great demand for recreational facilities such as restaurants, spas, and casinos because of the gathering of Chinese cybercriminals in these areas. It therefore creates business opportunities for the local people, and increases the local employment rate. In addition, bringing money obtained from cybercrime into China can be risky. Thus, cybercriminals spend a significant amount of money locally on houses, cars, and luxury products. This creates a positive effect on the local economy. The growth of the local economy not only increases the support rate of the local armed groups but also helps to achieve the local armed groups' political goals (SC-R-1).

The second factor is associated with the nature of the cybercrime industry. The proliferation of many traditional crimes can have a strong negative impact on the local people. Because the local people can also be victimised by traditional crime, there is severe political pressure on the local governor to control it. However, in the case of the cybercrime industry, since both the criminals and the victims are Chinese, the negative impact on the local people is trivial (SX-P-1). Moreover, cybercrime is 'invisible' to the local public compared to traditional street crime. Fengshu said: "Unlike traditional crime, such as drug trafficking, there is always violence and a smell of blood. Cybercrime is almost invisible

to the public. Local people cannot see or feel it when it targets foreign citizens" (GX-P-1). As a result, the political pressure from local people is slight when the local governor chooses to protect cybercrime. As Yian inspected, some local people may even support the protection of cybercrime due to its substantial economic benefits (SC-R-1).

The empirical data suggested that Myanmar is one of many countries where Chinese cybercriminals reside. Protection is also available to Chinese cybercriminals in many other states for political and economic reasons. Cybercrime activities in regions such as Europe, northern Africa, Southeast Asia, and the Middle East were also reported (SX-P-1, GD-CSP-2, GD-CSP-3, GD-P-1, GD-P-19, GD-P-11, GD-P-12, SX-R-1, LECID-10).

A state that uses a different language, has a different judicial process, and has no cooperation agreements with China can make a crackdown operation from China difficult, as Ningxin complained: "On many occasions, you know there are criminals, you know who they are, but you can't do anything to them" (GD-CSP-2). This, combined with the protection from the governors, forms a 'perfect storm' in which Chinese cybercriminals can reside. As a result, a reputation of corruption in a foreign state transmits a strong signal to Chinese cybercriminals and attracts them to move there (GD-P-10). For Xinxue, Chinese cybercriminals are "flyers that follow the stinky smell of corruption". If there is any possibility that protection may be granted, they will move (GZ-P-6). Supporting Xinxue, Xiuping, a prosecutor, pointed out: "Chinese cybercriminals always move to places where the level of legal development is low. For example, many cybercriminals move to small towns in Southeast Asian countries because the local government officials don't care about the law there" (GD-PST-5). Xiangwei also emphasised: "A common feature for states where a lot of Chinese cybercriminals reside is that the corruption level is high. The criminals can buy protection from them" (GD-CSP-3). In addition to Myanmar, Cambodia was reported to be another state where a lot of Chinese cybercriminals domicile due to the

availability of protection provided by corrupt government officials (GZ-P-6, GD-P-10). Zhimei said:

> Arresting criminals in Cambodia is unrealistic for us now. Because the criminals are protected. If you really want to arrest them, you need to pay. I am not sure about the price in Myanmar, but the market price in Cambodia is 30 to 50 thousand yuan for each criminal, 10 thousand yuan for each car, and 10 to 20 thousand yuan for each computer. The cost is enormous for the Chinese government. (GD-P-10)

In sum, the empirical data found that Chinese cybercriminals now move to countries where protection is available. The protection given to Chinese cybercriminals by the local armed groups, combined with the culture and geographical proximity, makes Myanmar one of the perfect places for Chinese cybercriminals to reside. By protecting Chinese cybercriminals, political and economic benefits arise for local armed groups and the local public, and give birth to an interesting symbiotic relationship between the three parties. Nevertheless, Myanmar is not the only state with the soil to propagate cybercrime. For various reasons, a similar level of protection also exists in other countries. Once Chinese cybercriminals detect potential protection in a state, they take action quickly. The movement of Chinese cybercriminals is unlikely to stop any time soon, as Fengshu concluded: "Don't underestimate the intelligence of cybercriminals […] After the strike in China, these people are constantly looking for new safe harbours. They are now testing various countries like Fiji and Laos and repeatedly trying to fight with the Chinese government" (GX-P-1).

4. Discussion: Protectors' Choice and Cybercrime Displacement

In line with the body of research in criminal governance and protection theory, the study found that protection is important to criminal operations (Wang, 2017; Shortland, 2019;

Varese, 2001; Lessing, 2021). In addition to solving commercial disputes and shaping economic order within the industry, cybercriminals in China also need protection from the local authority to safeguard their operation and avoid state repression. When strong protection is available, the industry flourishes. After all, cybercriminals are criminals. They have little power to fight state repression. Their governance system is embedded into the larger governance system controlled by the local authority, whether it is the state, the organised crime groups, the clans, or the insurgent groups who take actual control of the territory (Shortland, 2019; Lessing, 2021). As a result, as presented in the empirical data, depending on the political situation of the territory, cybercriminals seek help from various protectors in different locations. In China, while traditional organised crime groups play little role in safeguarding criminal operations, cybercriminals went to the local governments; in Myanmar, the cybercriminals rely on the protection given by armed groups; in other countries, the cybercriminals head to corrupt officials.

Next, in line with previous studies, the study found that corruption plays a role in protection (Wang, 2017). In the case of China, the long-existing social practice of *guanxi* generates corruption, which further leads to the phenomenon of protection. However, the phenomenon of protection cannot be explained by corruption alone, especially when the scale of protection is large. Political and economic reasons can form a forceful incentive for the local authority to provide protection to cybercriminals in addition to corruption. The underlying political and economic factors must also be considered. The cybercrime industry resembles two other infamous criminal industries: the piracy industry in Somalia (Shortland, 2019) and the drug industry in Myanmar (Chin, 2009), where the protectors' choice to protect criminals is motivated by economic and political goals. In the case of Somalia, alongside the personal economic benefits, the political elites in Somalia also chose to protect piracy out of area-development and political considerations. The piracy-

prone regions were remote areas where the transportation of goods was costly and complex. There was simply no comparable alternative income stream, and the political elites needed money to pursue their political agendas, such as to win elections or defend their territories (Shortland, 2019). A quote from the then-president of Himan-and-Heeb clearly illustrates this: "I'd take these guys on, but I can't right now because I don't have the resources…Besides, you can't just wipe out a whole line of work for thousands of young men. If you take something away, you must replace it with something else. Otherwise, more problems" (Shortland, 2019, p.54). In the case of Myanmar, a similar discovery was made where the armed group leaders who control different territories protected and taxed drug entrepreneurs to achieve their economic and political goals: they needed a myriad of funds to support their armies and build public facilities such as roads, power plants, and bridges to enhance the infrastructure of their societies and thus solidify their governance. In addition, some leaders also directly entered the business to secure even more significant funds for personal wealth and state-building (Chin, 2009). As a result, Chin (2009, p.234) summarised that "drug trade is almost always tied to politics…more often than not, drug enforcement operations are shaped by the local political climate or international political alliances". The same story seems to repeat in the case of cybercrime. The interviews quoted in this study clearly suggest that economic and political considerations are essential in deciding whether to protect cybercrime.

Moreover, the study interestingly found that the cybercrime hotspots in Myanmar − Kokang, Shan State, Kachin, and Mengla − overlap with the hotspots of the drug industry in Chin's research (2009). A possible explanation, stemming from the interviews, is that the protectors in Myanmar might find that protecting cybercriminals is a perfect substitution for protecting drug entrepreneurs under the global political pressure of fighting the drug trade. While earning the same amount of money from protecting criminals, the

economic and political costs are significantly lower in the case of protecting cybercriminals. Cybercrime is shadowy, and protecting Chinese cybercriminals who do not target Burmese citizens seems to impose little harm on the region, at least on the surface. This finding may indicate a possibility that cybercrime will proliferate in countries with political conflicts and underdeveloped economies in the future. In these countries, protecting foreign cybercriminals can be an attractive option for the political elites to accumulate economic and political capital.

Finally, the study also observed the phenomenon of crime displacement in the case of Chinese cybercrime (Barr & Pease, 1990; Johnson & Guerette, 2012; Short & Brantingham, 2010). In particular, spatial displacement was found, as after the intensive crackdown events in China, the cybercriminals moved to other countries where the same level of protection was available. Moreover, the displacement seems to be 'malign', meaning that after the displacement, the seriousness and the scale of operation did not reduce (Barr & Pease, 1990). While little research has been done on cybercrime displacement, the study suggests that the nature of cybercrime is the key to explaining the 'malign' displacement of Chinese cybercrime. In traditional crime, local knowledge and resources are essential for criminal operations. Criminals must be familiar with demand and supply within the local market and must be able to handle relationships with local competitors, protectors, and the authorities for their business to run smoothly. A lack of knowledge and resources is often one of the biggest hurdles for criminals when transplanting to a new territory (Varese, 2011). In the case of cybercrime, localisation is not a problem; it can be done remotely. As the empirical data indicated, cybercriminals can easily reside in one country and target victims in another. By keeping a similar mode of operation, cooperating with other Chinese cybercriminals online, and targeting only Chinese victims, Chinese cybercriminals face fewer challenges when moving abroad and maintaining their

operational scale. As a result, compared to traditional crime, there can be more ‘malign’ crime displacement in the case of international-level cybercrime.

5. Conclusion

In sum, this chapter examined various protectors within the cybercrime industry in China. It found that protection is essential for the Chinese cybercrime industry to function. Whilst traditional organised crime groups do not have a significant role in offering protection in China, cybercriminals rely heavily on corrupt state officials. When the state agents stopped offering protection, cybercriminals moved abroad to seek protection overseas. Under the protection of various protectors, cybercriminals can effectively minimise the detrimental impact caused by state repression. Political and economic considerations can drive these protectors into protecting cybercriminals.

Compared to traditional criminals, cybercriminals have a wide choice of protectors. They are able to travel to other countries where protectors are present and continue to commit cybercrime in their home country. Since the harm is not done to the victims who reside in the protectors' country, protection is more likely to be offered by foreign protectors when there are political and economic benefits. Moreover, because cybercrime can be done remotely, criminals rely less on local resources. When moving abroad, cybercriminals can maintain their operational scale relatively easily. Thus, when governmental crackdowns intensify in a certain country, cybercriminals may opt to relocate overseas. As nations increasingly enforce stringent policies against cybercrime, we might observe an upswing in the international migration of cybercriminals in the near future.

Chapter 8. Conclusion

Criminals need governance institutions to conduct business activities and facilitate cooperation. Previous research shows that without the assistance of state governance, cybercriminals create extra-legal governance as an alternative, to serve the same purpose. This dissertation followed these studies and extended the scope of research to the cybercrime industry in China. Using a rich amount of empirical data, this study offered insight into how the cybercrime industry is structured in China. It explored who the main actors are within the industry, how governance institutions are created by the cybercriminals to ensure cooperation in the forms of market and firms, and examined the roles of traditional protectors identified in previous research on extra-legal governance.

1. Summary of Empirical Findings

Following the theory chapter and the method chapter, Chapters 3 and 4 were dedicated to addressing the primary sub-research question: *How is the landscape of cybercrime in China characterised?* Each chapter had a different focus, however. Chapter 3 provided background information about the Chinese cybercrime industry. In essence, the chapter posited that the realm of cybercrime is primarily built around cyber fraud. After introducing six types of mainstream scam, the chapter argued that the prevailing social framework hasn't adequately adapted to the swift socio-economic advancements of recent times, culminating in a surge of cyber fraud and associated cybercrime activities, such as scam promoting, communication transmission support, and money laundering. At the same time, the country's internet infrastructure is not as restrictive as theoretically suggested. Cybercriminals can bypass its surveillance system at an additional cost, such as by

purchasing or renting SIM cards, credit cards, and national identity cards from others. Furthermore, several practical challenges, such as a lack of human resources, have hindered the state's effectiveness in combatting cybercrime. As a result, though the internet infrastructure might force cybercriminals to expend more resources to circumvent surveillance, cybercrime operations in China are not fundamentally different from those in other countries.

Chapter 4 continued the focus on the characteristics of the cybercrime industry in China, examining the actors within the industry. Contrary to the common image of cybercriminals, most of the actors are situated in the lower class of Chinese society. They often live in small cities, have a low education level, and do not have stable employment. Yet regardless of their IT skills, most are professional cybercriminals who are specialised in their specific domains. Finally, mirroring traditional criminal sectors, the chapter reveals that these cybercriminals collaborate through market and firm structures.

Chapter 5 and 6 then explored the structure of the market and the firm within the cybercrime industry. It also examined the functioning of governance systems in the two different structures. Focusing on the markets, Chapter 5 discovered that trade happens on both the market’s online and offline dimension: on the Internet, most of the cooperation is conducted on marketplaces, while offline there are no marketplaces, and trade is conducted in random locations. In some cases, the offline business encounter is also random. Criminals may meet their partners through advertisements on a wire pole, regular online chatting groups, or even pubs. Governance systems encompassing both self-governance and third-party governance are developed in both the online and offline domains. Self-governance in the online market is achieved based on the reputation mechanism and communal punishments. The general lack of trust within the online criminal market, the availability of information transmission on the Internet, and the system of invitation into

closed groups are believed to be essential in supporting the functioning of the self-governance system. In the offline market, however, the reputation mechanism functions well only when pre-established social relations are present because criminals cannot assess their potential partner's reputation ex-ante and have nowhere to report dishonest behaviour to cause reputation damage to the cheater without a shared community. However, the nature of offline trades gives birth to the possibility of hostage-taking and violence. Like in traditional crime, these two mechanisms are adopted to achieve self-governance by the cybercriminals subject to their ability to use violence and handle hostages. On the other hand, third-party governance online is achieved in two ways. One way is by having administrators who create, manage, and enforce forum rules. The robustness of third-party governance, however, varies among marketplaces. Another way of achieving third-party governance is by having middlemen guarantee the trade between two parties. Both administrators of marketplaces and reputable criminals can provide such services. In the offline market, middleman services are the primary form of third-party governance. In fact, middleman services are widely used by cybercriminals while conducting business offline. This could be due to the unavailability of self-governance in the offline market for many criminals.

Chapter 6 examined various types of cybercriminal firms in the cybercrime industry. This chapter argued that there are three possible reasons for firms to have emerged in the Chinese cybercrime industry: first, the economically driven nature of the cybercrime industry encouraged a more coordinated form of cooperation among the cybercriminals to increase operation efficiency and profits; second, employing the structure of firms enabled sophisticated modus operandi and therefore enhanced their safety; lastly, the frequent police repression against the cybercrime industry caused market volatility, which led to an increase in transaction costs for the cybercriminals. These cybercriminal firms have both

online and offline dimensions. Balancing the online and offline proportions is mainly influenced by the nature of the firms and the degree of police repression. Cybercriminal firms may adjust their online and offline activities due to the development of their modus operandi and fluctuations in the task environment. The chapter also provided insight into the structure of these firms and how governance is achieved within them. Cybercriminal firms may take the form of the Workshop model, the Company model, or the Federation model. The complexity in the organisational structure of the three models is ranked in ascending order. The nature of their businesses influences the structure a firm chooses to adopt. Regardless of the structure, setting up a selective recruitment scheme, developing a bonding process, employing compartmentation, and creating rules are the four common strategies that the firms use to achieve internal governance. As for external market actors, predatory activities are not common. Unlike traditional criminal groups, cybercriminal firms have a general lack of intention to govern market actors that have no business connections with them. A weaker power in the use of violence, not relying on tax income, and a low degree of territorial reliance could be the potential explanation. Ultimately, in the world of cybercrime, it seems unnecessary for cybercriminal firms to fight for resources, and firms can interact with each other peacefully.

The final empirical chapter, Chapter 7, turned to the protectors who often played a significant role in traditional criminal industries. A capable protector can facilitate criminal operations by creating a stable and orderly social and commercial environment that promotes the criminal economy. The data suggested that traditional organised crime groups do not have a significant role in offering protection in China. Instead, cybercriminals rely heavily on corrupt state officials. Some also move abroad and seek protection from local armed groups. Economic and political considerations influence the decision-making of state agents and local armed groups, in addition to the direct personal benefits they derive

from corruption. Due to the nature of cybercrime, cybercriminals can travel to other countries where protectors are present and continue to commit cybercrime in their home country. At the same time, because the harm is not directed towards the residents of the protectors' country, protection is more likely to be offered by foreign protectors when the political and economic benefits overcome the costs. As a result, this chapter predicted that there would shortly be more cybercriminal movements across the globe.

2. Reflection on Theories

While the contribution of this dissertation is largely empirical, the new context offers some points of interest in relation to the application of the governance theory. Overall, this study is a theory-confirming case: it showed that effective governance systems can encourage people to act collectively and refrain from acting against others and abusing common pool resources (Skarbek, 2014; Ostrom, 1990). In such a way, human predatory inclinations are constrained, and economic exchanges flourish (Hobbes, 2014; Barzel, 2002). These private governance systems can be developed among criminals to facilitate their business interactions without the support of states (Gambetta, 1996; Varese, 2001; Wang, 2017; Skarbek, 2014). Despite being extra-legal, they are sometimes just as effective as state governance (Leeson, 2014a). The same principles apply to cybercriminals. The study of the cybercrime industry in China found that cybercriminals rely on both self-governance and third-party governance to regulate their business orders, just like traditional criminals (Lusthaus, 2018). Traditional wisdom, such as making use of the reputation mechanism, hostage-taking, seeking middlemen services, and developing norms and rules, were largely adopted by cybercriminals to achieve governance in the market (Lusthaus, 2018; Leukfeldt, Kleemans & Stol, 2017; Leeson, 2014a; Stringham, 2015; Catino, 2019; Landa, 1981;

Skarbek, 2008, 2012). Cybercriminals also rely on a selective recruitment process, a socialisation process, compartmentation, rules, and violence to achieve internal governance within criminal firms (Pizzini-Gambetta & Hamill, 2011; Wang, 2017; Skarbek, 2014; Kostelnik & Skarbek, 2013; Jankowski, 1991; Catino, 2019). Furthermore, the study also supports the view that better functioning of the criminal governance systems requires a degree of protection that safeguards their criminal operation (Wang, 2017; Shortland, 2019; Lessing, 2021). Without such protection, the governance system is under constant threat of state intervention. Cybercriminals are no exception.

On the other hand, some new perspectives that can be added to the understanding of private governance and extra-legal governance also emerged in the study of the Chinese cybercrime industry. First, the study discovered that self-governance functions better in the online domain. As Chapter 5 discussed, cybercriminals can efficiently make use of the reputation mechanism to achieve self-governance on online marketplaces. In contrast, in the offline world, the effectiveness of self-governance is restricted. The efficiency of information transmission online is the most crucial reason for this observation. The availability of information in online marketplaces makes reputation easy and costless to assess. It therefore becomes the essential property of cybercriminals, and directly influences their trustworthiness (Lusthaus, 2018). Having no reputation, or even a bad reputation, is detrimental to cybercriminals' business. As a result, communal punishment that affects a cybercriminal's reputation becomes effective in supporting the functioning of self-governance. In the offline domain, however, the community size decides the efficiency of information transmission. This impedes the effectiveness of communal punishment and reduces the strength of the reputation mechanism (Leeson, 2014a; Stringham, 2015; Landa, 1981; Skarbek, 2012; Ostrom, 1990). As a result, cybercriminals are forced to take extra actions such as hostage-taking and violence to enforce agreements. Since most

cybercriminals are not experienced in handling hostages and using violence, relying on a third party becomes a better option.

Second, while most studies associate third-party governors with the professional use of violence (Wang, 2017; Shortland, 2019; Lessing, 2021; Gambetta, 1996; Varese, 2001; Barzel, 2002; Skarbek, 2014), this study found that violence is not always necessary in third-party governance. Reputation damage can also be seriously detrimental to cybercriminals. Middlemen who are familiar with the business and have social connections with other cybercriminals can be equally capable as third-party governors. Instead of violence, these middlemen act as information disseminators and use social sanctions as a weapon. They enforce agreements by bridging the gaps in information transmission on both online and offline dimensions and facilitate the functioning of self-governance. In the world of cybercriminals, they seem to be more popular than traditional organised crime groups.

Third, studies have pointed out that organised crime groups are often predatory. They will expand their territory and extract more resources when opportunities present (Skarbek, 2012, 2014; Lessing, 2021). Conflicts between organised crime groups are therefore common. Nevertheless, this study observed that when organised crime groups move their operations online, such predatory nature seems to reduce. They may maintain a degree of external governance, but most cybercriminal firms have little intention of expanding their governance to market actors who have no business relationship with them. This is likely because the demand for territorial resources reduces when operating online. Thus, when more criminal groups start to shift their operations online, such as drug distribution groups and gambling groups, we may witness fewer violent conflicts in the future.

Finally, this research found that the traditional organised groups that rely on providing governing services face challenges in the cybercrime industry. Because there is less competition in the cybercrime industry, there is also less demand for judicial services.

While cybercrime's need to safeguard its criminal operations still remains, traditional organised crime groups need to achieve a greater penetration of state systems to be able to protect cybercriminals from apprehension, should they want to seek business opportunities in the world of cybercrime.

3. Policy Implications

Moving away from the theories, the findings of this study may also shed some light on policies that aim to tackle cybercrime. During the past few decades, various countermeasures have been developed to tackle cyber fraud in China. A significant amount of resource has been spent on two aspects: policing and education. The former concerns improving policing strategies with the assistance of technologies and private sectors. The latter is linked to publicising popular scams and advocating the severe legal consequences of participating in cybercrime. These two measures face several challenges.

As for policing, one of the greatest challenges is perhaps the lack of resources to fight cybercrime. In addition to the issue of understaffing, as discussed in Chapter 3, there is also a shortage of funds. When a complicated cyber fraud operation involves suspects around the country, exactly when to send whom to investigate these places becomes an issue for many local police stations (GZ-P-4, GZ-P-9). This problem is more severe in cities with a lower level of economic development, where police resources are scarce. They are therefore unable to deal with complicated cybercrime cases. Corruption and protection form the second difficulty that undermines the effect of policing. As discussed in Chapter 7, the availability of government officials who provide protection services to cybercriminals has created huge difficulties in policing. Although the recent anti-corruption campaigns have successfully tackled the problem, it is unclear to what extent

the issue still remains in China, especially in small cities or towns located in remote areas. Thirdly, transnational crime is another issue that affects the policing of cyber fraud. Residing aboard and perhaps even receiving protection from the local politicians or armed groups render apprehension extremely costly. Fourthly, the underdevelopment of regulation also hinders policing. Without clear and comprehensive regulations, the police either do not know what action to take, or take actions that consequently harm legitimate businesses, as shown in Chapter 3. Finally, technologies that allow police to identify and intercept calls that are potentially associated with fraudulent activities have been used to prevent cyber fraud (GD-P-2, GD-CSP-2). Nevertheless, there is a tension between privacy protection and cyber fraud prevention. The issue of privacy invasion, caused by the application of these technologies, remains controversial. Where the line should be drawn is worth further consideration.

As for education around cybercrime, the current policy focuses on two main aspects: publicising popular scams and advocating the severe legal consequences of participating in cyber fraud. However, this approach is not very effective in stopping cyber fraud. On the one hand, the *modus operandi* of cyber fraud and the types of scam are constantly updating. Individuals may be aware of one type of scam but fall into another. On the other hand, there are many lower-class individuals participating in the cybercrime industry. Tian and Lin's (2020) study on lower-class individuals in Sanhe (三和: an area in Shenzhen where a lot of lower-class individuals gather) discuss how these individuals make their living: temporary employment, selling their citizen ID cards, SIM cards, bank accounts, WeChat accounts, and acting as the legal person for someone else's company (so that they will face legal consequences if the company commits a crime). In their observations of and interviews with ‘Glasses’, one of the individuals, they described:

> In the past, he always told others not to apply for SIM cards and sell them to others. Finally, on an occasion when he was desperately craving food to safe himself from hunger, he gave up his bottom line for money. He applied for five SIM cards, kept one for himself, and sold all of the rest. (p.184)

As the example showed, 'Glasses' knew exactly what he did was illegal, and there may be legal consequences awaiting him, but he felt that he had no choice. His experience may be indicative of many lower-class individuals in China. Education does not seem to work well for these individuals.

Efforts to overcome the challenges in both policing and education should be made in the future. Regarding policing, these efforts may include investing more resources in fewer economic development cities or developing a more efficient management scheme that reduces the imbalance of resources. At the same time, the government should be persistent in nationwide anti-corruption policies. These will hopefully further undermine the business opportunities for cyber fraud in China. Increasing international cooperation, especially with countries that border China and countries with a large number of Chinese immigrants, should also be implemented as a long-term strategy. Although barriers exist, international cooperation is not impossible to achieve (Lusthaus, 2018). The intensified cooperation between China and those countries will likely force Chinese cybercriminals to move to countries where they face higher operational costs. This may reduce the overall scale of cyber fraud operations. Future legislation should focus more on rudimentary institutions. Some of them may not be directly linked to cybercrime. These institutions include banking, company registration, digital currencies, telecommunication and data protection. However, regulations may come at a price. For instance, strict regulations on transferring between bank accounts may burden regular business transactions. There is a fine balance to tread. An alternative institution may also be created to release the load. Similarly, a balance should also be found in applying interception technologies: with applying technologies to

combat crime, the impact on individuals' privacy should be acknowledged. Ultimately, the police can only accomplish so much. The increased strength in policing will likely escalate the degree of fragmentation in the cybercrime industry. By evading police investigation, more technologies may be employed by cybercriminals, bringing in more parties involved in the industry. This seems like an endless battle. Thus, other measures should be taken alongside policing to better combat cyber fraud.

With respect to education, frequent updates on new scam operations, and ensuring these updates reach enough audiences, may reduce the number of potential victims. Analysing and summarising the common features of scams may also be helpful in educating the public to increase their awareness. Adding enterprises to the object of education, raising their general alertness of cyber security, and informing service providers about the potential misuse of their services may reduce the chance of data leaks and prevent criminals from exploiting various tools to commit fraud. Moreover, the underlying social issues that undermine the effect of education should also be addressed, even if they do not seem directly connected to cybercrime.

Unemployment and underemployment were found to be two central issues in the cybercrime industry (Lusthaus, 2018). Lusthaus (2018) found that when technical talents cannot secure suitable jobs, they are forced to seek alternative professions that give full play to their skills. This is especially prominent in Eastern Europe. The empirical data of this thesis supported Lusthaus' view and found the same phenomenon in China. However, those unemployed were not only hackers but individuals who did not have technical skills. As Chapter 4 discussed, not all cybercriminals need to acquire IT skills. Many are in fact victims of the economic transaction process in China. They also form a majority in the cybercrime industry and support its functioning. At the same time, as also shown in Chapter 4, although most cybercriminals arrested had no criminal history, those with criminal

records were all traditional criminals. This suggests that criminals who acquire technical skills may find it easier to land suitable jobs than those who do not after release from prison. The fact that many ex-hackers now work in private security companies may also support this view. As a result, solving the broader social issue of employment, not only for the general public but also for individuals with criminal records, may also help to reduce the scale of cybercrime.

4. Limitations and Future Research

Although substantial fieldwork was conducted in China, the findings of this study should be considered suggestive. The intrinsic nature of case studies challenges the external validity of the findings. The findings may only reflect the case of China and the field of study, and cannot be generalised to the rest of the world. Albeit there are universal strategies shared by cybercriminals worldwide, differences still exist among countries, depending on the socio-economic environment of the specific countries and the nature of the cybercrime industry. For instance, factors like the isolated online environment, the language barrier, and the specific products in demand within the Chinese cybercrime industry mean that Chinese cybercriminals predominantly collaborate with their local counterparts. They also primarily communicate through chat groups on Chinese instant messaging platforms. This relatively close-knit communication fosters a more connected market, which in turn offers a conducive environment for self-governance. Compared with the Chinese cybercrime market, in countries with a higher level of English prevalence and lower level of restriction on internet access, such as those in Western Europe, cybercrime forums appear to be more popular, and cybercriminals rely more on the third-party governance provided by the forum administrators.

A similar concern regarding validity is that there are missing data from numerous provinces in China due to the influence of the COVID-19 pandemic. There is also the lack of the offender's perspective, as most of my interviewees are law enforcement and cybersecurity practitioners. Efforts to compensate for this issue have been made by including more secondary data in the analysis, such as court judgments, but the risk remains. It is possible that not all perspectives in China can be represented here. Future studies on Chinese cybercrime should examine the findings with primary data from provinces that are not included in this research. These will include Beijing, Shanghai, and provinces with relatively low levels of economic development, such as Xingjiang, Qinghai, and Tibet. The perspectives of offenders should also be included on a broader scale. Moreover, internal validity may also be affected by the accuracy of the interview data. Many interviews have a retrospective nature, meaning that they consist of recollections of the interviewees' past experiences. A partial reconstruction of recollections may occur during the interview process, challenging the accuracy of the interview data. Triangulating interview data with secondary data has been intensively used to reduce this uncertainty.

Subject to various limitations, this empirical study is, however, the first attempt at systematically studying the cybercrime industry in China. Building on the findings of this research, further research in the same field can be developed with better data and research designs.

5. Epilogue

Cybercrime is not a mystery. Cybercrime in China is a lot like a regular business: the industry is well developed, with a high level of division of labour. There are clear career paths for criminals in different areas of expertise. Criminals may choose to work as

freelancers in the market or join an established firm until they can afford to invest in one of their own. The private governance systems within the industry, too, closely resemble those established in legal business regimes. The methods of dispute resolution in the cybercrime industry are often not too much different from how disputes are resolved between law-abiding individuals outside of court – and perhaps individuals do not frequently rely on courts to settle disputes anyway.

Cybercriminals are not shrouded in mystery either. They are flesh-and-blood individuals. For many, committing cybercrime is simply a means to accumulate wealth and improve their quality of life. Treating the business of cybercrime as a type of economic behaviour, and treating cybercriminals as economic actors, is perhaps the best approach to understanding them. One of my interviewees, a police officer, once recorded a conversation between a cybercriminal living abroad and his wife during a phone interception. According to the police, their conversations were very mundane. There was neither drama nor sensationalism, with solely a series exchange of plain statements: how much the husband had made that month, how much the family still owed on their loan, when the husband would return home.

Bibliography

Ames, W. L. (1981). *Police and community in Japan*. Univ of California Press.

Antifraud2. (2019, May 30). Dianxin zhapian fan: Ni dui wo de 'nuli' yiwusuozhi [Cyber fraudsters: You have no idea how hard I work]. *The Paper*. https://www.thepaper.cn/newsDetail_forward_3567318

Aravind, T. N., Mukundh, A., & Vijayakumar, R. (2023). Tracing Ip Addresses Behind Vpn/Proxy Servers. *2023 International Conference on Networking and Communications (ICNWC)*, 1–10.

Axelrod, R. (1990). *The Evolution of Co-Operation*. Penguin Books Ltd.

Bancroft, A., & Reid, P. S. (2016). Concepts of illicit drug quality among darknet market users: Purity, embodied experience, craft and chemical knowledge. *International Journal of Drug Policy*, *35*, 42–49.

Barr, R., & Pease, K. (1990). Crime placement, displacement, and deflection. *Crime and Justice*, *12*, 277–318.

Barzel, Y. (2002). *A theory of the state: Economic rights, legal rights, and the scope of the state*. Cambridge University Press.

Bhaskar, V., Linacre, R., & Machin, S. (2019). The economic functioning of online drugs markets. *Journal of Economic Behavior & Organization*, *159*, 426–441.`

Bidgoli, M., & Grossklags, J. (2017). "Hello. This is the IRS calling.": A case study on scams, extortion, impersonation, and phone spoofing. *2017 APWG Symposium on Electronic Crime Research (eCrime)*, 57–69.

Blundell, R., Dixit, A. K., Sherrerd, J. J., & others. (2004). *Lawlessness and economics: Alternative modes of governance* (Vol. 1). Princeton University Press.

Broadhead, S. (2018). The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments. *Computer Law & Security Review*, *34*(6), 1180–1196.

Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., & Chon, S. (2014). An analysis of the nature of groups engaged in cyber crime. *An Analysis of the Nature of Groups Engaged in Cyber Crime, International Journal of Cyber Criminology*, *8*(1), 1–20.

Button, M., & Cross, C. (2017). *Cyber frauds, scams and their victims*. Taylor & Francis.

Cai, T., Du, L., Xin, Y., & Chang, L. Y. (2018). Characteristics of cybercrimes: Evidence from Chinese judgment documents. *Police Practice and Research*, *19*(6), 582–595.

Campana, P., & Varese, F. (2013). Cooperation in criminal organizations: Kinship and violence as credible commitments. *Rationality and Society*, *25*(3), 263–289.

Catino, M. (2019). *Mafia organizations*. Cambridge University Press.

CCTV. (2021, November 17). *Gonganbu 'jingwang2021' shida anjian gongbu, dadiao tuanhuo 180 yu ge [The Ministry of Public Security announces the top ten cases from 'Net Cleaning 2021,' dismantling over 180 criminal groups.]*. https://news.cctv.com/2021/11/17/ARTI64k4b5NcZP4jsIGHItnk211117.shtml

Central People's Government of the People's Republic of China. (2021, December 31). *Daji dianzha zhe yi nian: Pohuo anjian 37wan yu qi, fa'anshu chixu xiajiang [Cracking Down on Telecom Fraud This Year: Over 370,000 Cases Solved, and the Number of Reported Incidents Continues to Decline]*. https://www.gov.cn/xinwen/2021-12/31/content_5665884.htm

Chan, A., & Siu, K. (2012). Chinese migrant workers: Factors constraining the emergence of class consciousness. *China's Peasants and Workers: Changing Class Identities*, 79–101.

Chan, K. W., & Zhang, L. (1999). The hukou system and rural-urban migration in China: Processes and changes. *The China Quarterly*, *160*, 818–855.

Chang, K. (2011). A path to understanding guanxi in China's transitional economy: Variations on network behavior. *Sociological Theory*, *29*(4), 315–339.

Chawki, M., Darwish, A., Khan, M. A., Tyagi, S., Chawki, M., Darwish, A., Khan, M. A., & Tyagi, S. (2015). 419 scam: An evaluation of cybercrime and criminal code in Nigeria. *Cybercrime, Digital Forensics and Jurisdiction*, 129–144.

Chen, J., & Palaoag, T. D. (2022). Regional Differences of Internet Technology Diffusion in China: A Case Study of Shaanxi and Tibet. *2022 International Conference on Computer Science, Information Engineering and Digital Economy (CSIEDE 2022)*, 105–113.

Cheng, T., & Selden, M. (1994). The origins and social consequences of China's hukou system. *The China Quarterly*, *139*, 644–668.

Chin, K.-L. (2009). *The Golden Triangle: Inside Southeast Asia's Drug Trade*. Cornell University Press.

China Union Pay. (2022, January 25). *China UnionPay Released 2021 Mobile Payment Security Survey Research Report*. https://cn.unionpay.com/upowhtml/cn/templates/newInfo-nosub/7885004da382485e8bde5a0ba000fdd3/20220125112643.html

Chu, B., Holt, T. J., & Ahn, G. J. (2010). Examining the creation, distribution, and function of malware on-line. *Department of Justice Abstract*, 1–183.

Chu, Y. (2002). *The Triads As Business*. Routledge.

Coase, R. H. (2012). *The Firm, the Market, and the Law*. University of Chicago Press.

Coase Ronald, H. (1937). The Nature of the Firm. *Economics*, *4*, 386–405.

Cohen, L. E., & Land, K. C. (1987). Age structure and crime: Symmetry versus asymmetry and the projection of crime rates through the 1990s. *American Sociological Review*, 170–183.

Collier, B., Clayton, R., Hutchings, A., & Thomas, D. (2021). Cybercrime is (often) boring: Infrastructure and alienation in a deviant subculture. *The British Journal of Criminology*, *61*(5), 1407–1423. https://doi.org/10.1093/bjc/azab026

Dickson-Swift, V. (2008). *Undertaking sensitive research in the health and social sciences*. Cambridge University Press.

Dixit, A. K. (2004). *Lawlessness and economics: Alternative modes of governance* (Vol. 5). Princeton University Press.

Dupont, B. (2013). Skills and trust: A tour inside the hard drives of computer hackers. In *Crime and networks* (pp. 195–217). Routledge.

Dupont, B., Côté, A.-M., Savine, C., & Décary-Hétu, D. (2016). The ecology of trust among hackers. *Global Crime*, *17*(2), 129–151.

Dupont, B., & Lusthaus, J. (2022). Countering distrust in illicit online networks: The dispute resolution strategies of cybercriminals. *Social Science Computer Review*, *40*(4), 892–913.

Elster, J. (2015). *Explaining social behavior: More nuts and bolts for the social sciences*. Cambridge University Press.

Espinosa, R. (2019). Scamming and the reputation of drug dealers on Darknet Markets. *International Journal of Industrial Organization*, *67*, 102523.

Fan, Y. (2002). Questioning guanxi: Definition, classification and implications. *International Business Review*, *11*(5), 543–561.

Fang. (2021, February 23). 'Paofenpingtai', xunihuobi jing cheng kuajing xiqian xin tongdao ["Point-running Platform" and Digital Currency Has Become the New Channel for Cross-border Money Laundering]. *Xinhua News*. http://www.xinhuanet.com/2021-02/23/c_1127126734.htm

Fei, X., Hamilton, G. G., & Zheng, W. (1992). *From the soil: The foundations of Chinese society*. Univ of California Press.

Felson, M. (2016). The routine activity approach. In *Environmental criminology and crime analysis* (pp. 106–116). Routledge.

Feng, T., & Lin, K. (2020). *Qi bu huaigui: Sanhe qingnian diaocha [Yearning for Return: An Investigation into Sanhe Youth]*. Dolphin Press.

Ferguson, H. (2017). Building online academic community: Reputation work on Twitter. *M/C Journal*, *20*(2).

Gambetta, D. (1996). *The Sicilian Mafia: The business of private protection*. Harvard University Press.

Gambetta, D. (2009). *Codes of the underworld: How criminals communicate*. Princeton University Press.

Gambetta, D., & Reuter, P. (1995). Conspiracy among the many: The mafia in legitimate industries. In *The economic dimensions of crime* (pp. 99–120). Springer.

Geller, A. (2020). How Comprehensive Is Chinese Data Protection Law? A Systematisation of Chinese Data Protection Law from a European Perspective. *GRUR International*, *69*(12), 1191–1203.

Government of the People's Republic of China. (2018, April 4). *78 min Taiwan dianxin wangluo zhapian fanzui xianyiren cong Feilvbin bei jieya huiguo [78 Taiwanese Cyber Fradusters Were Arrested in the Philippines]*. https://www.gov.cn/xinwen/2018-04/04/content_5279836.htm

Granovetter, M. (1985). Economic action and social structure: The problem of embeddedness. *American Journal of Sociology*, *91*(3), 481–510.

Graue, C. (2015). Qualitative data analysis. *International Journal of Sales, Retailing & Marketing*, *4*(9), 5–14.

Guzman, A. T. (2008). *How international law works: A rational choice theory*. Oxford University Press.

Haas, B. (2017, December 22). Man in China sentenced to five years' jail for running VPN. *The Guardian*. https://www.theguardian.com/world/2017/dec/22/man-in-china-sentenced-to-five-years-jail-for-running-vpn

Hamill, H. (2010). *The Hoods*. Princeton University Press.

Han, J. (2016, May 2). *Taiwan dianxin zhapianfan: Zao zhi bei qianfan dalu shoushen jiu bugan gan le [Taiwanese cyber fraudster: Had I known I would be deported to mainland China for trial, I wouldn't have dared to commit the crime]*. Xinhua News. http://www.xinhuanet.com/politics/2016-05/02/c_128949290.htm

Hardin, G. (1968). The tragedy of the commons: The population problem has no technical solution; it requires a fundamental extension in morality. *Science*, *162*(3859), 1243–1248.

Haslebacher, A., Onaolapo, J., & Stringhini, G. (2017). All your cards are belong to us: Understanding online carding forums. *2017 APWG Symposium on Electronic Crime Research (eCrime)*, 41–51.

Hennink, M., Hutter, I., & Bailey, A. (2020). *Qualitative research methods*. Sage.

Hill, P. B. (2003). *The Japanese Mafia: Yakuza, Law, and the State*. Oxford University Press.

Hirschi, T., & Gottfredson, M. (1983). Age and the explanation of crime. *American Journal of Sociology*, *89*(3), 552–584.

Hobbes, T. (2014). *Leviathan*. Wordsworth Editions.

Hofmann, D. C., & Gallupe, O. (2015). Leadership protection in drug-trafficking networks. *Global Crime*, *16*(2), 123–138.

Holmstrom, B. R., & Tirole, J. (1989). The theory of the firm. *Handbook of Industrial Organization*, *1*, 61–133.

Holt, T. J., Smirnova, O., & Hutchings, A. (2016). Examining signals of trust in criminal markets online. *Journal of Cybersecurity*, *2*(2), 137–145.

Hou, G. (2021). Cryptocurrency money laundering and exit scams: Cases, regulatory responses and issues. *Understanding Cryptocurrency Fraud*, 83.

Hu, Y. (2020, August 11). ”Dianxin wangluo zhapian dingshang ruoshi qunti, nongmin, gongren deng cheng muhou ‘bangxiong’ [Cyber fraudesters targeting vulnerable groups, with farmers and workers becoming unwitting accomplices behind the scenes]. *The Paper*. https://www.thepaper.cn/newsDetail_forward_8672280

Hutchings, A. (2014). Crime from the keyboard: Organised cybercrime, co-offending, initiation and knowledge transmission. *Crime, Law and Social Change*, *62*, 1–20.

Isacenkova, J., Thonnard, O., Costin, A., Francillon, A., & Balzarotti, D. (2014). Inside the scam jungle: A closer look at 419 scam email operations. *EURASIP Journal on Information Security*, *2014*, 1–18.

Jacobs, J. B. (1979). A preliminary model of particularistic ties in Chinese political alliances: Kan-ch’ing and Kuan-hsi in a rural Taiwanese township. *The China Quarterly*, *78*, 237–273.

Jankowski, M. S. (1991). *Islands in the street: Gangs and American urban society* (Vol. 159). University of California Press Berkeley.

Jewkes, Y., & Yar, M. (2013). *Handbook of Internet crime*. Routledge.

Jiang, Y. (2023, January 21). 31 Shengfen 2022 nian GDP chulu: 16 di paoying quanguo, Fujian, Jiangxi zengsu zuikuai [The 2022 GDP for 31 provinces is released: 16 regions outperform the national average, with Fujian and Jiangxi growing the fastest]. *Chinanews*. https://www.chinanews.com.cn/cj/2023/01-21/9940105.shtml

Jingshi Police. (2020, July 29). Nanzi tongguo VPN ‘fanqiang’ fangwen jingwai seqeing wangzhan, bei xingzheng chufa [A man administratively penalized for using VPN to ‘climb over the wall’ and access foreign pornographic websites]. *Fenghuang*. https://news.ifeng.com/c/7yUhGsebHyS

Johnson, S. D., Guerette, R. T., & Bowers, K. J. (2012). Crime displacement and diffusion of benefits. *The Oxford Handbook of Crime Prevention*, *337*.

Kaplan, D. E., & Dubro, A. (1986). *Yakuza: The explosive account of Japan’s criminal underworld*. Addison-Wesley Reading, MA.

Kenney, M. (2007). *From Pablo to Osama: Trafficking and terrorist networks, government bureaucracies, and competitive adaptation*. Penn State University Press.

Kostelnik, J., & Skarbek, D. (2013). The governance institutions of a drug trafficking organization. *Public Choice*, *156*, 95–103.

Krylova, Y. (2019). The Rise of Darknet Markets in the Digital Age: Building Trust and Reputation. In *Returning to interpersonal dialogue and understanding human communication in the digital age* (pp. 1–24). IGI Global.

Kshetri, N. (2013). Cybercrime and cyber-security issues associated with China: Some economic and institutional considerations. *Electronic Commerce Research*, *13*, 41–69.

Kuzmin, A. (2012). State and trends of Russian cybercrime in 2011. *2012 IV International Congress on Ultra Modern Telecommunications and Control Systems*, 933–939.

Landa, J. T. (1981). A theory of the ethnically homogeneous middleman group: An institutional alternative to contract law. *The Journal of Legal Studies*, *10*(2), 349–362.

Lee, J.-A., & Liu, C.-U. (2012). Forbidden City enclosed by the Great Firewall: The law and power of Internet filtering in China. *Minn. JL Sci. & Tech.*, *13*, 125.

Lee, J.-A., & Liu, C.-Y. (2016). Real-name registration rules and the fading digital anonymity in China. *Wash. Int'l LJ*, *25*, 1.

Leeson, P. T. (2007). An-arrgh-chy: The law and economics of pirate organization. *Journal of Political Economy*, *115*(6), 1049–1094.

Leeson, P. T. (2014a). *Anarchy Unbound: Why Self-Governance Works Better Than You Think*. Cambridge University Press.

Leeson, P. T. (2014b). Pirates, prisoners, and preliterates: Anarchic context and the private enforcement of law. *European Journal of Law and Economics*, *37*, 365–379.

Lessing, B. (2021). Conceptualizing criminal governance. *Perspectives on Politics*, *19*(3), 854–873.

Leukfeldt, E., Kruisbergen, E., Kleemans, E., & Roks, R. (2020). Organized financial cybercrime: Criminal cooperation, logistic bottlenecks, and money flows. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 961–980.

Leukfeldt, E. R. (2014). Cybercrime and social ties: Phishing in Amsterdam. *Trends in Organized Crime*. https://doi.org/10.1007/s12117-014-9229-5

Leukfeldt, E. R., Kleemans, E. R., Kruisbergen, E. W., & Roks, R. A. (2019). Criminal networks in a digitised world: On the nexus of borderless opportunities and local embeddedness. *Trends in Organized Crime*, *22*(3), 324–345. https://doi.org/10.1007/s12117-019-09366-7

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017). Cybercriminal networks, social ties and online forums: Social ties versus digital ties within phishing and malware networks. *The British Journal of Criminology*, *57*(3), 704–722.

Leukfeldt, E. R., Lavorgna, A., & Kleemans, E. R. (2017). Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial

Cybercrime as Organised Crime. *European Journal on Criminal Policy and Research*, *23*(3), 287–300. https://doi.org/10.1007/s10610-016-9332-z

Leukfeldt, E. R., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior*, *37*(3), 263–280. https://doi.org/10.1080/01639625.2015.1012409

Leukfeldt, E., & Roks, R. (2021). Cybercrimes on the streets of the Netherlands? An exploration of the intersection of cybercrimes and street crimes. *Deviant Behavior*, *42*(11), 1458–1469.

Leukfeldt, R., & Kleemans, E. E. (2019). Cybercrime, money mules and situational crime prevention: Recruitment, motives and involvement mechanisms. In *Criminal networks and law enforcement* (pp. 75–89). Routledge.

Levchenko, K., Pitsillidis, A., Chachra, N., Enright, B., Félegyházi, M., Grier, C., Halvorson, T., Kanich, C., Kreibich, C., Liu, H., & others. (2011). Click trajectories: End-to-end analysis of the spam value chain. *2011 Ieee Symposium on Security and Privacy*, 431–446.

Levi, M., Doig, A., Gundur, R., Wall, D., & Williams, M. (2017). Cyberfraud and the implications for effective risk-based responses: Themes from UK research. *Crime, Law and Social Change*, *67*, 77–96.

Li, X. (2015). Regulation of cyber space: An analysis of Chinese law on cyber crime. *International Journal of Cyber Criminology*, *9*(2), 185.

Liang, B., & Lu, H. (2010). Internet development, censorship, and cyber crimes in China. *Journal of Contemporary Criminal Justice*, *26*(1), 103–120.

Liu, M. (2021, April 8). Yi gongsi shexian wei jingwai zhapian jituan feifa yinliu, Beijing jingfang zhuahuo 44 ren [A company suspected of providing draining services for

overseas fraud groups, Beijing police arrested 44 people]. *The Beijing News*. https://www.bjnews.com.cn/detail/161789355415019.html

Luo, Y. (1997). Guanxi: Principles, philosophies, and implications. *Human Systems Management*, *16*, 43–52.

Luo, Y. (2008). The changing Chinese culture and business behavior: The perspective of intertwinement between guanxi and corruption. *International Business Review*, *17*(2), 188–193.

Lusthaus, J. (2018). *Industry of anonymity: Inside the business of cybercrime*. Harvard University Press.

Lusthaus, J. (2019). Beneath the dark web: Excavating the layers of cybercrime's underground economy. *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 474–480.

Lusthaus, J., & Varese, F. (2021). Offline and Local: The Hidden Face of Cybercrime. *Policing: A Journal of Policy and Practice*, *15*(1), 4–14.

Lusthaus, J., Van Oss, J., & Amann, P. (2022). The Gozi group: A criminal firm in cyberspace? *European Journal of Criminology*, 14773708221077615.

Magaloni, B., Franco-Vivanco, E., & Melo, V. (2020). Killing in the slums: Social order, criminal governance, and police violence in Rio de Janeiro. *American Political Science Review*, *114*(2), 552–572.

Marvell, T. B., & Moody, C. E. (1991). Age structure and crime rates: The conflicting evidence. *Journal of Quantitative Criminology*, 7, 237–273.

McCarthy, N. (2018, August 23). *China Now Boasts More Than 800 Million Internet Users And 98% Of Them Are Mobile [Infographic]*. Forbes. https://www.forbes.com/sites/niallmccarthy/2018/08/23/china-now-boasts-more-than-800-million-internet-users-and-98-of-them-are-mobile-infographic/

Miller, S., Curran, K., & Lunney, T. (2018). Multilayer perceptron neural network for detection of encrypted VPN network traffic. *2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, 1–8.

Morselli, C., Giguère, C., & Petit, K. (2007). The efficiency/security trade-off in criminal networks. *Social Networks*, *29*(1), 143–153.

Myerson, R., Hou, Y., Tang, H., Cheng, Y., Wang, Y., & Ye, Z. (2010). Home and away: Chinese migrant workers between two worlds. *The Sociological Review*, *58*(1), 26–44.

Nguyen, T., & Luong, H. T. (2021). The structure of cybercrime networks: Transnational computer fraud in Vietnam. *Journal of Crime and Justice*, *44*(4), 419–440.

Olson, M. (1989). Collective action. In *The invisible hand* (pp. 61–69). Springer.

Ostrom, E. (1990). *Governing the commons: The evolution of institutions for collective action*. Cambridge university press.

Pizzini-Gambetta, V., & Hamill, H. (2011). *Shady Advertising": Recruitment among Rebels and Mobsters*.

Powell, W. W. (1990). Neither Market Nor Hierarchy. *Research in Organizational Behavior*, *12*, 295–336.

Reuter, P. (1983). *Disorganized crime: The economics of the visible hand*. MIT press Cambridge, MA.

Ren, Q., & Liu, Y. (2021, March 30). Saoheichue cong zhuanxaing douzheng zhuanxiang changtaihua kaizhan, weilai zenme zuo? [The transition from a specialised campaign to a normalised approach in cracking down on organised crime: How should it be done in the future?]. *The State Council of the People's Republic of China*. https://www.gov.cn/xinwen/2021-03/30/content_5596864.htm

Rhumorbarbe, D., Staehli, L., Broséus, J., Rossy, Q., & Esseiva, P. (2016). Buying drugs on a Darknet market: A better deal? Studying the online illicit drug market through the

analysis of digital, physical and chemical data. *Forensic Science International*, *267*, 173–182.

Schelling, T. C. (1967). Economics and criminal enterprise. *The Public Interest*, *7*, 61.

Schelling, T. C. (1990). *The Strategy of Conflict* (2nd ed.). Harvard University Press.

Sebagh, L., Lusthaus, J., Gallo, E., Varese, F., & Sirur, S. (2022). Cooperation and distrust in extra-legal networks: A research note on the experimental study of marketplace disruption. *Global Crime*, *23*(3), 259–283.

Sharrock, R. A. W., Anderson, R., & Harper, R. (2013). The Inescapability of Trust. In *The Complexity of Trust in Computing*. Cambridge University Press.

Short, M. B., Brantingham, P. J., Bertozzi, A. L., & Tita, G. E. (2010). Dissipation and displacement of hotspots in reaction-diffusion models of crime. *Proceedings of the National Academy of Sciences*, *107*(9), 3961–3965.

Shortland, A. (2019). *Kidnap: Inside the ransom business*. Oxford University Press.

Skarbek, D. (2011). Governance and prison gangs. *American Political Science Review*, *105*(4), 702–716.

Skarbek, D. (2012). Prison gangs, norms, and organizations. *Journal of Economic Behavior & Organization*, *82*(1), 96–109.

Skarbek, D. (2014). *The social order of the underworld: How prison gangs govern the American penal system*. Oxford University Press.

Song, Y. (2014). What should economists know about the current Chinese hukou system? *China Economic Review*, *29*, 200–212.

Soudijn, M. R., & Zegers, B. C. T. (2012). Cybercrime and virtual offender convergence settings. *Trends in Organized Crime*, *15*(2–3), 111–129.

Steffensmeier, D., Zhong, H., & Lu, Y. (2017). Age and its relation to crime in Taiwan and the United States: Invariant, or does cultural context matter? *Criminology*, *55*(2), 377–404.

Stevenson, C. (2007). Breaching the great firewall: China's internet censorship and the quest for freedom of expression in a connected world. *BC Int'l & Comp. L. Rev.*, *30*, 531.

Stockmann, D., & Luo, T. (2019). Authoritarian deliberation 2.0: Lurking and discussing politics in Chinese social media. *Digital Media and Democratic Futures*, 169–195.

Stringham, E. P. (2015). *Private Governance: Creating Order in Economic and Social Life*. Oxford University Press.

Swedberg, R. (2003). The case for an economic sociology of law. *Theory and Society*, *32*(1), 1–37.

Symkovych, A. (2018). The 'inmate code'in flux: A normative system and extralegal governance in a Ukrainian prison. *Current Sociology*, *66*(7), 1087–1105.

Taneja, H., & Wu, A. X. (2014). Does the Great Firewall really isolate the Chinese? Integrating access blockage with cultural factors to explain Web user behavior. *The Information Society*, *30*(5), 297–309.

The Linjiang People's Procuratorate. (2021, October 13). *Fanzui tuanhuo gongsi zuzhi tuanjian, shuizhi tuanjian bian 'tuanmie' [Criminal Firms Organised Team-building Activity, Leading to Police Crackdown]*. http://www.jllinjiang.jcy.gov.cn/ljxw/202110/t20211013_3395630.shtml

The Supreme People's Court of the People's Republic of China. (2022, August 1). *She xinxi wangluo fanzui tedian he sifa qushi dashuju zhuanti baogao [Special Judicial Big Data Report on Characteristics and Trends of Cybercrime]*. https://www.court.gov.cn/fabu-xiangqing-368121.html

The Supreme People's Procuratorate of the People's Republic of China. (2020, June 1). *Zuigaorenminjianchayuan gongzuo baogao (di 13 jie quanguo renmin daibiao dahui di san ci huiyi zhangjun 2020 nian 5 yue 25 ri) [Work Report of the Supreme People's Procuratorate (Third Session of the 13th National People's Congress, Zhang Jun, May 25, 2020)]*. https://www.spp.gov.cn/spp/gzbg/202006/t20200601_463798.shtml

Tsang, E. W. (1998). Can guanxi be a source of sustained competitive advantage for doing business in China? *Academy of Management Perspectives*, *12*(2), 64–73.

van Waardenberg, A. (2021). *Reputation in AlphaBay: The effect of forum discussions on the business success of cryptomarket sellers.* [B.S. thesis].

Van Wegberg, R., Oerlemans, J.-J., & van Deventer, O. (2018). Bitcoin money laundering: Mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin. *Journal of Financial Crime*.

Varese, F. (2001). *The Russian Mafia: Private protection in a new market economy*. OUP Oxford.

Varese, F. (2011). *Mafias on the move: How organized crime conquers new territories*. Princeton University Press.

Von Lampe, K. (2015). *Organized crime: Analyzing illegal activities, criminal structures, and extra-legal governance*. Sage Publications.

Wall, D. S. (2008). Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime. *International Review of Law, Computers & Technology*, *22*(1–2), 45–63.

Walton, G. (2001). *China's golden shield: Corporations and the development of surveillance technology in the People's Republic of China*. Rights & Democracy.

Wang, P. (2017). *The Chinese Mafia: Organized Crime, Corruption, and Extra-Legal Protection*. Oxford University Press.

Wang, X., Juffermans, K., & Du, C. (2016). Harmony as language policy in China: An Internet perspective. *Language Policy*, *15*, 299–321.

Wehinger, F. (2011). The dark net: Self-regulation dynamics of illegal online markets for identities and related services. *2011 European Intelligence and Security Informatics Conference*, 209–213.

Wen, L., & Tang, S. (2018, August 9). Zhongyang dianming guapai 18 ge dianxinzhapian zhongdian diqu, 5 ge yi zhaipai [The central government has named and listed 18 cyber fraud hotspot—5 of them have been 'uncapped']. *People's Daily*. http://legal.people.com.cn/n1/2018/0809/c42510-30219981.html

Whitty, M. T. (2018). 419-It's just a Game: Pathways to Cyber-Fraud Criminality emanating from West Africa. *International Journal of Cyber Criminology*.

Williams, M. L., Levi, M., Burnap, P., & Gundur, R. V. (2019). Under the corporate radar: Examining insider business cybercrime victimization through an application of routine activities theory. *Deviant Behavior*, *40*(9), 1119–1131.

Williamson, O. E. (1996). *The mechanisms of governance*. Oxford university press.

Williamson, O. E. (1998). The institutions of governance. *The American Economic Review*, *88*(2), 75–79.

Wong, Y.-H., & Chan, R. Y. (1999). Relationship marketing in China: Guanxi, favouritism and adaptation. *Journal of Business Ethics*, *22*, 107–118.

Xin, Y. (2022, June 1). 2022 xin yixian chengshi mingdan guanxuan: Shengyan diechu, Hefei chonggui xin yixian! (Fu zuixin 1-5 xian chengshi wanzheng mingdan) [2022 New First-Tier Cities Announced Officially: Shenyang Drops Out, Hefei Returns to the New First-Tier! (Includes the Complete List of Tier 1-5 Cities)]. *China Business Network*. https://www.datayicai.com/report/detail/286

Xinhua. (2022, January 6). China handles 62,000 cybercrime cases in 2021. *ChinaDaily*. https://www.chinadaily.com.cn/a/202201/06/WS61d64646a310cdd39bc7f668.html

Yip, M. (2010). *An investigation into Chinese cybercrime and the underground economy in comparison with the West* [PhD Thesis]. University of Southampton.

Yip, M. (2011). *An investigation into Chinese cybercrime and the applicability of social network analysis*.

Yip, M., Webber, C., & Shadbolt, N. (2013). Trust among cybercriminals? Carding forums, uncertainty and implications for policing. *Policing and Society*, *23*(4), 516–539.

Zhao, K., Zhang, Y., Xing, C., Li, W., & Chen, H. (2016). Chinese underground market jargon analysis based on unsupervised learning. *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*, 97–102.

Zhuge, J., Holz, T., Song, C., Guo, J., Han, X., & Zou, W. (2009). *Studying malicious websites and the underground economy on the Chinese web*. Springer.