Humanities & Social Sciences Communications

ARTICLE

https://doi.org/10.1057/s41599-024-04042-w OPEN

Cybercrime as an industry: examining the organisational structure of Chinese cybercrime

Qiaoyu Luo[1]✉

In an age of advancing information technology, widespread internet access has facilitated a rise in profit-driven cybercrime. Empirical research has found that cybercrime is now highly industrialised. Cybercrime operations have evolved into an assembly of various malicious acts, some of which do not require advanced technical abilities. While extensive research on cybercrime has been conducted globally, there is a lack of detailed investigation into the cybercrime landscape in China, despite it being a vast economic entity with a significant number of cybercrime incidents. Drawing on interviews and secondary data from China collected between 2020 and 2022, this paper seeks to address this gap by offering a comprehensive examination of Chinese cybercrime. It explores the degree of industrialisation within Chinese cybercrime and discusses its impact on the work performed by Chinese cybercriminals. Echoing findings from previous studies on the industrialisation of cybercrime, the current study reveals an elaborate industry built around cyber fraud, populated by various market players working on diverse tasks to support the successful operation of cyber fraud. The research also uncovers the existence of cybercriminal firms that closely mimic the structural and operational approaches of legitimate companies. Similar to how the Industrial Revolution reshaped traditional manufacturing, the industrialisation of cybercrime has transformed it into an assembly line operation, where each cybercriminal carries out basic, tedious, and repetitive tasks on a daily basis.

[1] Department of Sociology, University of Oxford, Oxford, UK. ✉email: qiaoyu.luo@sociology.ox.ac.uk

Introduction

As information technology continues to advance, internet access has become readily available to the vast majority of the public. As a result of shifts in routine activities, the prevalence of profit-driven cybercrime has surged (Felson, 2016; Leukfeldt and Yar, 2016; Soudijn and Zegers, 2012). Economic damage from cybercrime is projected to reach ~10.5 trillion US dollars by 2025 (Morgan, 2020). Empirical research has found that cybercrime is now highly industrialised (Collier et al., 2021; Lusthaus, 2018). Observable cybercriminal activities are often facilitated by various professional actors who specialise in different fields of crime, such as data stealing, malware making, bullet-proof service hosting, and money laundering. Criminal products and services are traded in marketplaces such as online forums and chat groups (Leukfeldt et al., 2019; Levchenko et al., 2011; Lusthaus, 2019). Moreover, cybercriminal firms have also emerged: many of these illicit activities are conducted by criminal firms that adopt structures that resemble legal businesses (Lusthaus et al., 2022). As such, 'hacking' is a word that no longer serves to generalise the concept of cybercrime. Cybercrime has become an aggregation of a series of malicious behaviours, with some of them not directly involving technical skills.

Adding to this complexity, research has found that cybercrime is not only a global and online phenomenon but also an offline and local one (Chen et al., 2023; Lusthaus, 2020; Lusthaus and Varese, 2021). While attacks on victims are carried out in the digital realm, for some individuals, partnerships with fellow cybercriminals extend into real-world interactions. What is more, the local conditions of different countries play an important role in shaping local cybercrime, as certain countries appear to harbour more cybercrime incidents than others, and prevalent cybercrimes also vary between countries. For instance, Lusthaus (2018) found that while cyber fraud is trending in Nigeria and Romania, technical criminal endeavours such as spamming and malware production are more common in the former Soviet Union and in Western countries. In this sense, cybercrime has become a complex social phenomenon shaped by the intricate interplay of foundational socio-economic elements.

As a result, cybercrime studies should be carried out in different social contexts. While existing studies on cybercrime have mostly focused on Western countries, China has not been studied in detail, despite it being a vast economic entity with an enormous amount of cybercrime incidences. Based on interviews and secondary data collected in China between 2020 and 2022, the paper aims to fill this knowledge gap and provide a comprehensive examination of Chinese cybercrime. It examines to what extent Chinese cybercrime has undergone the process of industrialisation and discusses industrialisation's impact on the work performed by Chinese cybercriminals.

The paper is structured as follows: The literature review section outlines recent studies on the industrialisation of cybercrime around the globe and existing studies on Chinese cybercrime. This is followed by the 'Method' section, which describes the research method and the data collection process. Next, the "Findings" section reports the main findings concerning the current landscape of Chinese cybercrime and its industrialisation. Finally, the 'Conclusion and Discussion' section summarises the findings and discusses their contributions to the academic literature and intervention strategies on cybercrime.

Literature review: the industrialisation of cybercrime

This section pulls together some of the relevant literature on the industrialisation of profit-driven cybercrime and provides a conceptual framework for this study. The first two subsections examine the concepts of market and firms in cybercrime settings, and the third subsection reviews existing studies in Chinese cybercrime and argues that there is a general lack of knowledge on the industrialisation of cybercrime in China.

Division of labour, criminal markets and the concept of cybercrime. The very preliminary form of cybercrime is commonly referred to as hacking. At first, most hacking behaviours were often not executed with malicious purposes but rather with curious, recreational and intellectual means. The evidence of this can be seen from the various versions of 'hacking ethic', such as 'the access to the computer should be unlimited and total', 'information should be free', and 'authority should be mistrusted' (Levy, 1984). Hackers who used their hacking skills to commit crime were viewed as being in the minority, and were referred to as the 'underground hackers' (Coleman and Golub, 2008). The public image of these criminal hackers was that they were 'lone wolves' who acted individually (Collier et al., 2021; Lusthaus, 2018). Few online communities existed and were mostly platforms for skilled hackers to share knowledge and tools.

The landscape of hacking activities has changed significantly since the start of the millennium, as computer systems have become increasingly sophisticated and networked. The significant increase in the number of computer users worldwide has expanded the opportunities for cybercrime. Criminal markets and the division of labour naturally emerge when cybercriminals recognise the benefits of specialising in particular tasks (Lusthaus, 2018). Consequently, new types of cybercrime have emerged to support hacking activities, and various online marketplaces have been built to allow cybercriminals to trade their tools and services. At this point, cybercriminals started benefiting from the services and products that other criminals provided, and could focus on their own specialised activity (Lusthaus, 2018). Cybercriminals may also concurrently cooperate with multiple partners online across the globe (Leukfeldt et al., 2017a, 2017b; Soudijn and Zegers, 2012). For example, in analysing a spam-based advertising operation, Levchenko et al. (2011) identified a broad range of offenders specialising in different areas. These offenders include individuals who specialise in sending spam emails, registering and selling domain names, and facilitating payment services. Moreover, actors in the cybercrime markets are not all IT specialists. A study on online travel fraud discovered that the actors involved in the chain of criminal activities include a wide range of specialists, such as ticket providers, professional hackers, and money mules. These specialists conducted only a portion of the whole criminal operation and traded their loot online (Hutchings, 2018). In line with this finding, a former cybercriminal from Eastern Europe stated that even in a malware ecosystem alone, there are more than fifteen roles that cybercriminals can play, involving both technical and non-technical actors who are operating online and offline (Lusthaus, 2018, p. 67).

Probing further into the cybercriminal markets, a series of studies conducted by Leukfeldt and colleagues found a tight intersection between cybercrime and conventional crimes (Leukfeldt, 2014; Leukfeldt et al., 2019; Leukfeldt et al., 2017a; Leukfeldt et al., 2017b; Leukfeldt and Roks, 2021; Leukfeldt and Yar, 2016). In studying a phishing network in the Netherlands, various cybercrime facilitators were identified, including a professional 'caller' who posed as a bank employee, called the victims and acquired login codes; eight bank employees who stole the victims' credentials and made changes to their accounts; and a letter carrier who intercepted the victims' bank letters. The tasks that these offenders performed were very similar to what would have been seen in conventional crime (Leukfeldt, 2014). Similarly, in analysing 18 Dutch police files, a range of low-tech cybercriminals were found, such as offenders who intercepted newly requested debit cards and official posts that contained credentials of the victims and offenders who were responsible for skimming or trading stolen goods. Interestingly, many of them were also involved in conventional crimes such as drug trafficking, smuggling, and burglaries (Leukfeldt et al., 2017b). Furthermore, another study conducted by Leukfeldt and Roks (2021) found that many cybercriminals not only committed other conventional crimes such as theft, burglary, robbery and human trafficking but also feature the contours of street culture. For instance, many cybercriminals would talk in Dutch street vernacular. These studies suggest that as the industrialisation process of cybercrime deepens, the range of actors also increases, and the skills and experiences in cybercrime required for them to participate in the cybercrime market reduce. Consequently, the tasks performed by many cybercriminals are often characterised as simple, repetitive, and boring (Collier et al., 2021).

From the above discussion, it is evident that the concept of cybercrime has expanded significantly. The formation of criminal markets has led to cybercrime encompassing a vast array of goods and services. Whether dealing with highly technical cybercrimes such as hacking or seemingly less technical ones like cyber fraud, the perpetrators may come from diverse backgrounds and perform various roles. These roles span from highly technical to relatively non-technical, yet they are integrated within criminal markets. As a result, it is challenging to delineate a natural boundary where the online trade of illicit goods and services ceases to be classified as cybercrime. Consequently, as Lusthaus (2024) argues, while legal scholar and legislators might find it useful to have an unambiguous definition of cybercrime, it may be better for social scientists to treat cybercrime as the most recent phase of how technology has influenced crime and adopt an inclusive definition of cybercrime. In this article, I use Lusthaus's (2024, p 8.13) definition that *cybercrime is a crime that makes use of digital technology in a significant way*, and I define cybercriminals as *individuals who directly commit or assist such a crime*.

The emergence of cybercriminal firms. According to economics theory in industrial organisation, the emergence of firms signifies the birth of an industry (Coase, 1937; Williamson, 1996). 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). Transaction costs have been one of the most important determinants in explaining the emergence of firms. According to Coase (1937), transaction costs encompass the expenses related to identifying trading partners, negotiating and enforcing agreements, and managing uncertainties and information imbalances in the market. When the market scale increases, transaction costs are also likely to rise. Moreover, socioeconomic factors such as the stability of the market environment, level of trust, and degree of protection of property rights have a strong impact on these costs. When the market environment becomes unstable (e.g., frequent changes in regulatory policies), there is poor enforcement of contracts and property rights, and a low level of trust in the market, and so it becomes more attractive for transactions to be internalised within firms where they can be more effectively controlled. Consequently, firms will emerge as a form of mitigation. What is more, firms have a tendency to expand. Firms expand when internal transaction costs are lower than market transaction costs, and when they can achieve economies of scale. However, since the primary purpose of establishing firms is to minimise transaction costs, firms stop expanding when the marginal cost of internalising transactions exceeds the marginal revenue (Coase, 1937; Williamson, 1996).

The theory of firms is also applied by scholars to understand criminal groupings. Studies have found that criminals frequently encounter high transaction costs. Criminal markets are perpetually under threat from law enforcement, leading to an unstable market environment. These markets typically experience low levels of trust, significant information imbalances, and weak enforcement of contracts and property rights. Consequently, it is unsurprising that criminals are incentivised to internalise their transactions and establish firms (Catino, 2019; Lusthaus et al., 2022; Morselli et al., 2007; Reuter, 1983; Schelling, 1967; Von Lampe, 2015). Nevertheless, since criminal firms 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 (Morselli et al., 2007; Reuter, 1983). For the same reason, criminal firms also tend to have a smaller size and a shorter lifespan (Reuter, 1983). As a result, academic discussion on criminal firms often suggests that when a criminal group consists of entrepreneurs, managers, employees, and temporary workers, it can be classified as a criminal firm (Lusthaus et al., 2022).

Following the concept, cybercriminal firms have also been witnessed and documented in recent studies. For instance, Lusthaus and Varese (2021) found that a range of highly structured offline cybercriminal firms existed in Râmnicu Vâlcea. Within these firms, many members maintained personal connections. They frequently convened in person, establishing a sense of community. Cybercriminal firms may also exist solely in the online dimension. For example, Lusthaus et al. (2022) identified that the criminal crew that developed and maintained Gozi (banking malware) consisted of around six individuals. There is little evidence suggesting that the members were tidily connected offline, and most of their cooperation appeared to take place online. Yet, the crew members had a clear hierarchy, ranging from entrepreneurs down to employees. They also operated together with a clear profit motivation. Thus, while the crew was certainly not legally incorporated, it shared a lot in common with the conception of firms.

Due to the emergence of firms, academics argue that the business of cybercrime has evolved into a mature industry that bears a strong resemblance to the legal economy. As a consequence, fundamental economic principles and patterns can also be applied to understand cybercrime (Collier et al., 2021; Lusthaus, 2018; Lusthaus et al., 2022). What is more, since the existence of firms enables cybercriminals to work as 'employees' or 'temporary workers', and there is often a further division of labour within a firm, the requirement of technical skills and experience for most illicit tasks is additionally reduced (Lusthaus and Varese, 2021).

Cybercrime in China. Chinese cybercrime was tied closely to patriotism in its early stages around the turn of the millennium. Many scholars associate the hacking activities in that period with the rise of nationalism derived from long-term national humiliation and government restrictions on public demonstrations (Hang, 2014; Henderson, 2007; Kshetri, 2013; Webber and Yip, 2018). In a recent study conducted by Webber and Yip (2018), it was found that the pattern of member growth in the hacker communities was coincident with political incidents related to China. However, the general passion for patriotism among Chinese hackers deteriorated over time, and the cybercrime landscape has changed significantly during the past two decades following the disbanding of various patriotist hacking communities, including the biggest two at the time, the HUC and the China Eagle Union (Wang, 2018; Yip, 2010). The surge in the population of Chinese Internet users and a general lack of awareness of cybersecurity in China provided these former patriotic hackers with the opportunity to monetise their skills. As a consequence, profit-driven cybercrime began to come into vogue (Wang, 2018; Yip, 2010). Over the past decades, the cybercrime landscape has continued to evolve. Different forms of cybercrime have taken turns of prominence in China, including the spreading of worms and trojans, DDoS attacks, game account stealing, and IP theft (Yip, 2010; Kshetri, 2013; Lusthaus, 2018). In recent years, cyber fraud has become the mainstream form of cybercrime in China (Franceschini et al., 2023; Zhuang and Ma, 2021). Cyber fraud in China was found to have first emerged in Taiwan in the 1990s in the form of phone-based scams. When these scams were imported into mainland China, their operational scale grew rapidly and soon spread across the country. In recent years, the operational scale has expanded even more significantly and has started to extend to Southeast Asian countries, including Vietnam, Myanmar, Cambodia, and the Philippines (Franceschini et al., 2023; Nguyen and Luong, 2021).

As the types of cybercrime have evolved, so too has its organisational structure. Like their foreign counterparts, organisational structures have been observed in the modern operation of Chinese cybercrime. Yip's studies (2010, 2011) found that Chinese cybercriminals frequently exchange stolen goods and provide illicit cybercrime services on Tencent QQ and WeChat, two popular instant messaging platforms in China. In addition, local internet forums that host regular content are also frequently exploited by cybercriminals to conduct illicit trade. Baidu Tieba, as identified by Yip (2010), Zhuge et al. (2009) and Lee (2022), was the largest. Organisational structures that are akin to commercial firms have also seemed to emerge in China. Whilst analysing transnational cyber fraud networks in China, Nguyen and Luong (2021) identified two distinct offline cybercriminal groups. The first group consisted of money mules who were responsible for opening bank accounts and receiving the stolen money from Vietnamese victims; there were strong interactions between members of the group. The second group consisted of cybercriminals who were responsible for making fraudulent phone calls. It was found that the group was structured with a strong hierarchy and division of labour that resembles legal companies. Similarly, Zhao et al.'s (2024) study on Chinese cyber fraud groups and their recruitment found that the groups are often hierarchical and can be divided into a core layer and a peripheral layer. Members of the core layer are managers and employees, who enjoy stable employment, whereas many members of the peripheral layer are temporary workers. Chinese cybercrime organisations can take form on a much larger scale in Southeast Asian countries. 'Scam compounds' that consist of dozens of different cybercrime 'companies' have been found in these regions. These cybercrime 'companies' also employ hierarchical structures. Furthermore, within the compounds, the 'companies' often have dormitories and spaces for shops, entertainment, and other amenities (Franceschini et al., 2023; Zhuang and Ma, 2021). In addition, a strong connection between conventional crime and cybercrime was found by Wang et al. (2021) in their study on illicit money lending. Their research showed that traditional organised criminal groups have started attempting to utilise the internet and move their operations to cyberspace.

Overall, existing studies on Chinese cybercrime suggest that it is currently operating on a large economic scale. There are not only established markets but also criminal groups that appear to fit the definition of criminal firms. However, a systematic analysis of Chinese cybercrime is still lacking. When the term 'industry' was used in some studies of Chinese cybercrime, it was not thoroughly examined through economic theories. Moreover, existing studies tend to focus mainly on one type of cybercrime, overlooking other related cybercriminal activities in detail, which consequently fails to provide a comprehensive picture of Chinese cybercrime. As a result, the extent to which Chinese cybercrime has evolved into an industry compared to international counterparts, what this industry looks like, and the consequent effects on the activities of Chinese cybercriminals, remain areas of uncertainty. Building on the existing literature, this paper aims to fill this research gap and enhance the understanding of the global trend of cybercrime industrialisation by offering a comprehensive examination of Chinese cybercrime.

Method

This study utilises a qualitative research methodology. Qualitative research is well suited for this research, as the target of the research is a hidden population, and quantitative data on this area is commonly unavailable. Quantitative data also have limited utility for the purpose of this current research as one of the main targets is to understand the impact of industrialisation on cybercrime operations and cybercriminals. The qualitative research method has also been successfully conducted in the study of criminals, including not only traditional criminals such as the mafia (Gambetta, 1996; Varese, 2001; Wang, 2017), pirates (Shortland, 2019) and street gangs (Jankowski, 1991) but also cybercriminals (Collier et al., 2021; Lusthaus, 2018; Lusthaus and Varese, 2021). Building on the success of previous studies, the same approach was therefore adopted in the current research.

The collected data comprises primarily semi-structured interviews conducted over a 3-year fieldwork period (2020–2022) across various regions of China, with the exception of two interviewees based in the US. Participants were primarily sourced through geographical, purposive, and snowball sampling strategies.

As for geographical sampling, the majority of the 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. This is because there are often more experienced personnel who have dealt with complicated cybercrime cases in these cities. However, to understand Chinese cybercrime from a comparative angle and allow for variation, cities with different political and economic statuses were also covered, including 'first-tier' (most developed) cities in China, such as Shenzhen, some 'second-tier' cities such as Chengdu, and some rural areas such as Lianjiang. 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.

As for purposive sampling, three groups of people were identified before the fieldwork: practitioners in the cybersecurity sector, law enforcement officers, and former cybercriminals now working in the field of cybersecurity. The recruitment was conducted both online and offline. For the purpose of online recruitment, I joined several cybersecurity-related WeChat groups where people who work in the cybersecurity field often 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

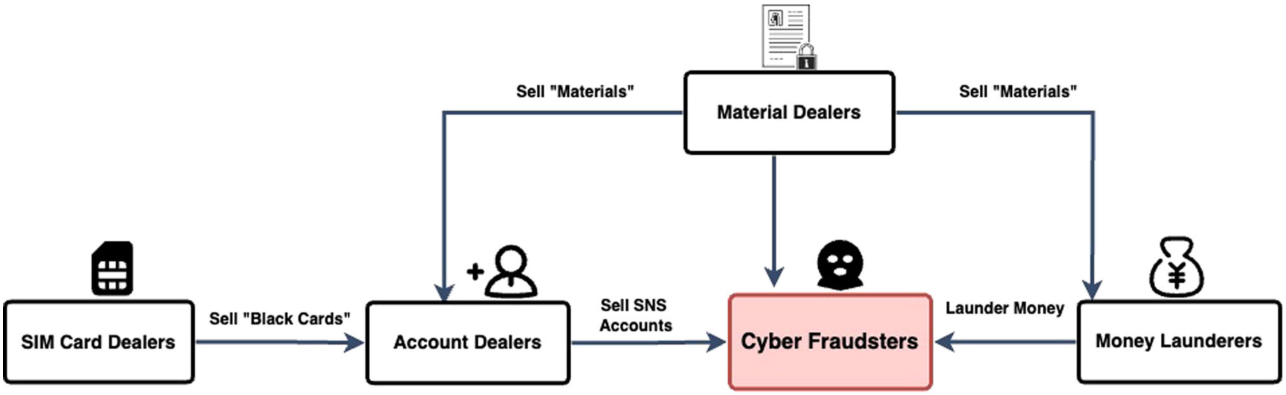

Fig. 1 Principal Facilitators within the Cybercrime Market.

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.

Snowball sampling was also adopted: I always asked my participants if they could refer any other potential candidates to me after their interviews. These attempts acquired fruitful results.

Interviews were mostly conducted face to face ($N = 51$), with online or phone-based interviews reserved for specific situations, such as participants residing in remote areas or scheduling difficulties ($N = 15$). The shortest interview lasted about 15 min, and the longest one lasted about 150 min.

In the end, 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 ($N = 15$). The average interview time was 59 min. The shortest interview lasted about 15 min, and the longest one lasted about 150 min. 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 had 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). Appendix 1 provides a list of interview subjects. Key information about the interviewees is provided. In cases where a participant spans across different groups, I labelled the participants according to their main connection to the topic.

In addition to the interview data, two types of secondary data were also collected. The first type is the law enforcement confidential investigation documents. They are in the forms of files, reports and hand-made diagrams. I labelled these 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 labelled as CSCR. These documents were provided during interviews by the participants. Appendix 2 summarises the secondary data that were coded and cited in this study.

Findings

This section of the paper presents the key results of the study. The initial subsections of the analysis focus on the high degree of industrialisation within China's cybercrime sector, paralleling, if not exceeding, developments in other countries. This industrialisation is evidenced by a highly differentiated market and the advent of cybercriminal firms. The subsequent subsection discusses the recent expansion of the Chinese cybercrime industry and argues that the Chinese cybercrime industry remains largely a local manifestation of the global cybercrime industry. The final subsection explores the ramifications of industrialisation, noting that jobs have become more simplistic, repetitive, and at times, monotonous.

The prevalence of cyber fraud and the rise the criminal market.

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 China Judicial Big Data Research Institute, 282,000 cybercrime cases were adjudicated in the first instance by courts in China between 2017 and 2021. Of these cybercrime cases, almost 40% of the cybercrime cases were sentenced under the charge of cyber fraud. At the same time, 23.76% of the cybercrime cases were under the charge of assisting cybercrime, indicating the existence of a large group of cybercrime facilitators (The China Judicial Big Data Research Institute, 2022). The empirical evidence corroborates the findings presented in this judicial report, demonstrating the existence of a vast cybercrime market in China, centred on cyber fraud. Similar to most cybercrime operations, the data reveals that the effective execution of cyber fraud is contingent upon the collaborative efforts of diverse facilitators (Hutchings, 2018; Levchenko et al., 2011).

The empirical evidence delineates four pivotal groups of facilitators within the cybercrime market, as depicted in Fig. 1 below. The first group of facilitators are the SIM card dealers. 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. However, 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). These SIM cards were collected by the SIM card dealers and sold in bulk to the second group of facilitators: the account dealers for further illegal operations.

Account dealers are the second group of facilitators. Under the same real-name registration system, all online accounts must be bound to citizen ID. 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 (GD-P-20, GZ-P-9, GD-P-19). However, the

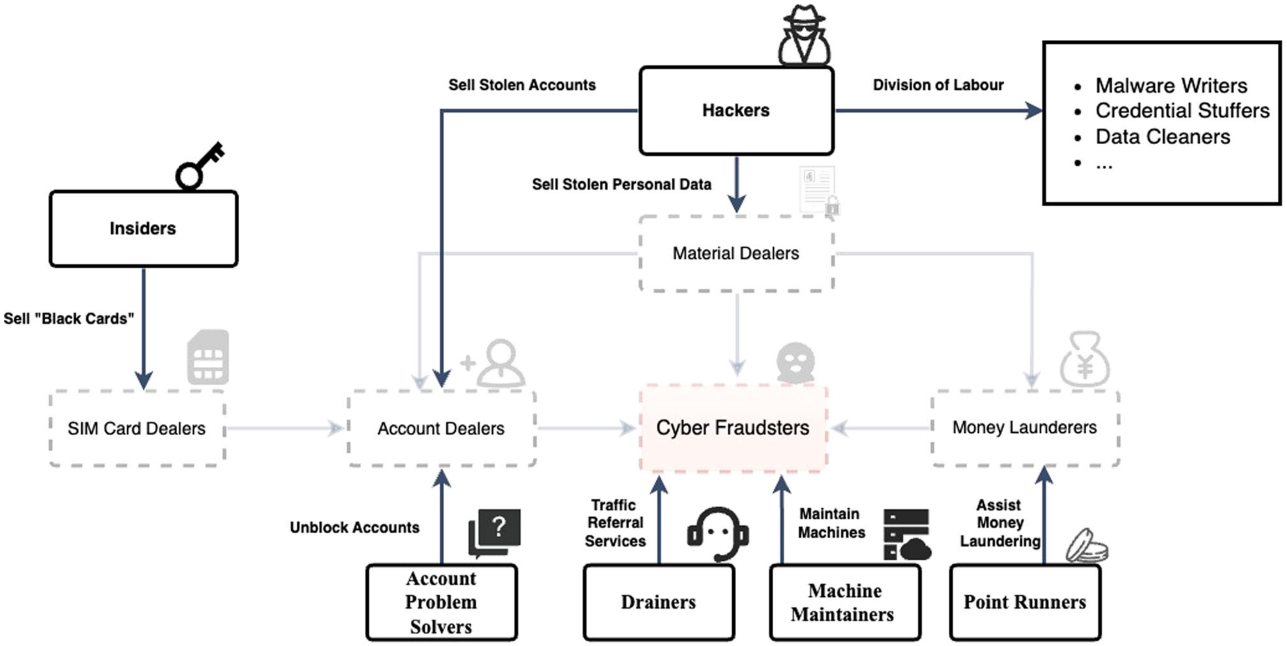

Fig. 2 Additional Market Actors.

account dealers circumvent China's strict real-name system by registering large numbers of social media accounts using the SIM cards purchased from the SIM card dealers and building genuine images for these accounts (known as 'account farming') to avoid detection by social media platforms' security systems (GD-CSP-2, GZ-P-9, GX-P-1).

The third group of facilitators are material dealers. Material dealers are criminals who collect a variety of 'materials' that could be used to conduct cybercrime, including citizen IDs, bank accounts, bank cards with security devices, business licences, and other personal data (SX-H-1, SX-H-5, GZ-P-8, GZ-P-11, GD-PST-4). There are three main customers of the material dealers, all of whom need different materials: account dealers, cyber fraudsters, and 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 enable them to conduct scams more effectively, and this acquisition is also essential for certain types of scam (GD-CSP-3, SX-H-5); for money launderers, entities such as bank cards, USB security keys and business licences are all necessary tools for money laundering (GZ-P-8).

The final group of facilitators consists of money launderers, who have been prominently featured in numerous cybercrime studies. In a multitude of cybercrime operations, there are typically individuals known as money mules engaged to aid the cash-out process for cybercriminals (Hutchings, 2018; Leukfeldt, 2014; Lusthaus and Varese, 2021). However, the situation in China reveals that these individuals are often not merely 'money mules' at the behest of cybercriminals, but professional business entities holding a critical role in the market, which is commonly referred to as a 'water house' by law enforcement (GD-CSP-3, GD-P-20, GX-P-1, GX-P-3, GD-P-22, GZ-P-8, GZ-P-10). A typical process within cybercrime money laundering involves acquiring bank cards from material dealers to dismantle the funds. For instance, a hundred dollars might be split into nine transactions of ten dollars each, distributed across ten different bank accounts, with the residual ten dollars further divided into ten one-dollar transactions, and then channelled into another set of ten separate 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 (GZ-P-8). What's more, on top of the money dissembling, money launderers may add fake digital currency or virtual property transactions at certain stages to conceal it even further (GD-P-22, LECID-5).

The aforementioned four groups of facilitators, however, represent merely a small segment of the market's participants. The cybercrime market is considerably more intricate and divided, as shown in Fig. 2. On the one hand, criminal activities are often delegated to individuals performing more granular tasks for the above-mentioned facilitators. For instance, SIM card leaks may originate from insiders within mobile telecommunications companies: it is conceivable that during the registration of phone numbers, a teller might clandestinely register an additional SIM card using the customer's identification details for subsequent illicit sale (GZ-P-10, GD-P-20). Likewise, hackers frequently supply account dealers and material dealers with stolen accounts and personal data. The value of these compromised accounts extends beyond the time savings afforded by bypassing the need for account farming; they also provide a crucial instrument for perpetrating scams that include the impersonation of a victim's contacts (SX-H-1). Furthermore, there is a division of labour among hackers, such as those who are responsible for creating malware and those who are responsible for cleansing stolen data (US-CSP-2).

On the other hand, as the country's efforts to prevent crime grow, so does the number of people helping with cybercrimes. For example, when it became clear that many online accounts were set up for fraud, social media companies started using new technology to spot and block these fake accounts, which led to many accounts being closed. In response to this, 'account problem solvers' have emerged as novel commercial ventures, offering services to liaise with SNS platforms and manage the account reinstatement process through online channels (GZ-P-9). Similarly, numerous cyber fraudsters have recently begun to exploit telecommunications equipment equipped with Voice over Internet Protocol (VoIP) protocols, enabling them to make phone calls remotely via a computer to reduce the risk of detection (GZ-P-4, GZ-P-9). They may also hire machine maintainers to swap out the SIM cards in the machines, service the machines, and frequently relocate them to evade police detection, thereby further enhancing their safety (GZ-P-9, GZ-P-10).

Another recently emerged facilitator is known as a 'drainer'. These individuals offer traffic-referral services to cyber fraudsters. Their operation entails drawing in potential victims and enticing them to connect with the social media profiles controlled by cyber fraudsters (GD-PST-2, GX-P-2, GZ-P-6). Strategies adopted by the drainers 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). Finally, to increase the level of concealment and the efficiency of the money laundering process, some money launderers 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 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 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).

Yet even the actors introduced above are not exhaustive; many more cybercriminals are working in each business sector to support the functioning of the cybercrime market. The cybercrime market is also 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).

In sum, presented in this subsection is a highly specialised, dynamic cybercrime market that evolves continually under the influence of national policies in China. This finding aligns with previous research on international cybercrime, which suggests that modern cybercrime activities are rarely executed by solitary actors but rather through the collaborative efforts of various market participants (Hutchings, 2018; Lusthaus, 2018; Leukfeldt et al., 2017a; Soudijn and Zegers, 2012). Moreover, insufficient regulation in the areas of personal data protection, telecommunications, and mobile payment sectors, as the above empirical evidence presents, has contributed to the development of cybercriminal market in China. The easy access to products such as personal data, SIM cards, and telecommunications equipment, along with the widespread use of mobile payment services without a comprehensive regulatory system, leads cybercriminals to recognise the potential profits of focusing on specific tasks that facilitate cyber fraud. At the same time, crackdowns on these facilitating activities, without sufficient effort to improve regulations in these sectors, appear to be counterproductive and have contributed to the further development of the market. The rise of the market provides the soil for industrialisation.

The present of cybercriminal firms. Beyond the market, the empirical evidence also found a diversity of cybercriminal firms in China. These firms, engaged in hacking, cyber fraud, draining, and money laundering, have been identified within the broader spectrum of cybercriminal operations.

Haoming, a former hacker and a current cybersecurity engineer, explained how a cybercriminal group specialising in infecting servers and computers is commonly 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 and the members have different specialities, the members' roles sometimes overlap when working on a task, and the leader is often involved. The structure of such hacking groups seems to resemble most small-scale cybercriminal groups with a significant degree of online component, such as the Gozi group (Lusthaus et al., 2022) and some high-tech cybercriminal groups in the Netherlands (Leukfeldt et al., 2017a). Although these groups have relatively flat hierarchical structures and lack clearly defined roles among their members, the distinction between leaders and employees remains evident. As Lusthaus et al. (2022) put it, they are 'situated on the defining boundary,' which, overall, aligns with the concept of criminal firms. There are good reasons for firms like this to rise among the high-tech cybercriminals. The most significant factor is that cybercriminals conduct business in an unstable environment, facing constant threats from law enforcement and the risk of defection by their collaborators (SX-H-1). It is, therefore, preferable for them to form stable partnerships and internalise market transactions to avoid the trouble of identifying reliable partners for each venture. Haoming wrote: "If I want to do something, or I want to get something, I often need people, and I surely want to find someone I know, right? I can't just go onto the internet and say: 'Hi, who wants to hack with me?'" (SX-H-1). Moreover, time and efficiency are crucial in many situations. For instance, in the sale of vulnerabilities and data, early sellers typically command higher prices. Consequently, forming a stable team can minimise communication delays and other transaction costs, thereby enhancing efficiency and enabling members to achieve greater profits (SX-H-1, US-CSP-1).

Cybercriminal firms that employ a more hierarchical structure and align more closely with the theory of firms in legitimate world were also found. For example, Yueyi, the head of an anti-fraud centre at a county-level police station, described a cyber fraud group he had dealt with:

> 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)

Yueyi's statement clearly demonstrates the group's three-tiered hierarchical structure. Below the leader, there are various departments responsible for different duties. Beneath these departments are the employees who carry out the tasks. The distinctions among entrepreneurs, managers, and employees are pronounced.

As illustrated by the example above, this type of cybercriminal firm typically internalises many components of the market, such as machine purchasing and maintenance, traffic referring, and account problem solving. This approach not only enhances production efficiency, reduces communication costs, and mitigates transaction risks, but also effectively manages market price fluctuations caused by police repression (Coase, 1937). 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).

Franchise-like operations have also been observed within some firms as part of their expansion strategy (GD-R-1, GX-P-1, GZ-P-6, GD-P-10, GD-CSP-2, GD-CSP-3, LECID-1, LECID-2). A confidential investigation report provides an example of how a cyber fraud group that conducted the notorious pig-butchering scam used this strategy to expand their business (LECID-2). A team leader of the group testified in the report:

> Anyone who was able to recruit 10 members to form a group [team] could apply to become a group [team] leader, and the members he recruited would automatically join his group [team]. The group [team] leader had to cover half of the daily cost of the group [team] 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 [team] was split equally between the boss and the group [team] leader. However, the group [team] leader also had to pay for the basic salary of the group [team] members. (LECID-2)

The testimony clearly demonstrates that cybercriminal firms not only mirror legitimate firms in their structure but also engage in similar economic activities as those conducted by businesses in the legitimate world.

In addition, it is worth noting that all cybercriminal firms found in this study had an offline component. Some degree of offline element appears necessary for coordination. Haoming, a former hacker, doubted that some firms operate 'purely online' and consist of anonymous members who only meet each other in that dimension. He noted that misunderstandings, disagreements, and arguments are almost inevitable in any group, especially for groups on a large scale or groups 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). Furthermore, offline interaction seems to be inevitable to satisfy criminals' social needs. 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 group, despite starting with anonymous online cooperation, will gradually come closer and start to develop offline connections.

This section demonstrates the existence of various cybercriminal firms in China. Although their structures may differ, they are formed to minimise transaction costs in the open market, consistent with economic theories (Coase, 1937; Williamson, 1996). Beyond their structure, these cybercriminal firms also operate in ways similar to legitimate businesses. Furthermore, the incorporation of an offline element within these firms seems to have blurred the lines between them and conventional criminal firms as established in earlier research (Reuter, 1983; Von Lampe, 2015). Overall, the prevalent existence of cybercriminal firms in China indicates that Chinese cybercrime operates at a highly industrialised level, comparable to that observed in international contexts.

The global expansion of the industry. In line with newspaper coverage and previous studies, the empirical evidence also found traces of Chinese cybercriminals operating aboard, especially in East and Southeast Asian countries (Franceschini et al., 2023; Nguyen and Luong, 2021; Zhuang and Ma, 2021). For instance, some market actors of the Chinese cybercrime industry seemly operate in foreign countries. A police officer from Guangdong Province, Youpu, arrested some Chinese hackers from Cambodia in 2020. According to him, these hackers not only conducted hacking themselves but also sometimes subcontracted specific technical tasks to domestic hackers and distributed commissions based on the specific tasks (GD-P-19). Similarly, money launderers have also moved their operation to foreign countries such as the Philippines, Australia, and Middle East countries (GZ-P-8, SC-R-1).

Moreover, many cyber fraud firms have established themselves in foreign lands such as Myanmar. According to the participants, in areas such as Kokang, Shan State, Kachin, and Mengla, the cybercrime business is so flourishing that the criminals almost openly operate on a large scale in the fanciest building in town (GZ-P-6, GD-CSP-2, SX-H-4). 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)

Yet, while the firms are established in foreign countries, many of their members are recruited from mainland China and were smuggled to Myanmar. In a confidential investigation report, a recruiter of a cyber fraud firm located in Myanmar testified: 'When a newbie is recruited [from China], the treasurer will cover the fees for flights and smuggling. He then must work for us for at least 3 months to cover these fees' (LECID-1).

The empirical evidence seems to suggest that the Chinese cybercrime industry has reached a scale that extends beyond local manufacturing. In this regard, the development of the Chinese cybercrime industry appears to surpass cybercrime industries found in other countries, which are mostly domestically established (Lusthaus, 2018). However, the evidence also reveals that the participants in the Chinese cybercrime industry are almost exclusively Chinese, with limited involvement from foreign criminals. Additionally, there is not enough evidence to suggest that the Chinese cybercrime industry intersects or integrates with cybercrime industries in other countries. Therefore, the Chinese cybercrime industry remains largely a local manifestation of the global cybercrime industry.

Cybercriminals in the age of industrialisation. While the preceding subsections have focused on assessing the extent of industrialisation present, this subsection delves deeper to explore the influence of the industrialisation process on the routine operations of cybercriminals.

The first observable outcome of the industrialisation process is the development of an extensive value chain. This is characterised by a multitude of market actors, each specialising in distinct tasks, many of which require a relatively low level of technical expertise (GD-CSP-2, GD-CSP-3, SX-H-4, SX-H-5, SX-CSP-2, US-CSP-1, US-CSP-2). For instance, Fengshu, a police officer, described the daily tasks conducted by the account dealers:

> These people[account dealers]'s task is to register and purchase social media accounts to resell them. They steal pictures and use Photoshop to edit them, creating personas that appear wealthy and attractive. To make these profiles look real, they also update the accounts with new posts every few days, building a genuine image. (GX-P-1)

The daily tasks of account dealers are repetitive and straightforward, with the 'technical' aspect of their work perhaps being limited to the image editing process in Photoshop. Similarly, regarding the tasks of material dealers, another police officer, Zhimei, posits that although some may possess hacking skills and access databases to steal personal data, most data is obtained through offline means:

> A lot of personal data is sold offline. You put down your information at the [company] 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. (GD-P-10)

Reflecting on the same point, cybersecurity practitioner Chengzi claimed that 'social resources' are more important than technical skills for cybercriminals nowadays. He explained:

> As long as you understand the theory [how cybercrime works] and possess your own 'social resources', there's no need for technical skills to enter this field. For instance, if you are a telephone operator or know how to find one, you can start a SIM card business. We call this a 'professional entry point'. (SX-CSP-2)

Even in business sectors where technical skills are essential, the level of expertise required is considerably reduced due to the process of industrialisation. For instance, in the context of hacking for data theft, cybersecurity engineer Ming observed that criminals need to acquire only a very specific set of skills to engage in this business, as they are responsible for just a small part of the overall process. Ming wrote:

> Even in hacking, there's a division of labour. Some are solely tasked with identifying vulnerabilities, while others exploit these weaknesses to steal data or user accounts. Then, there are those who compile this data, cleanse it, and structure it. All these activities are carried out as services, and the end products are sold to others. (US-CSP-2)

Addressing the same point, Youlv, a former hacker, even believes that anyone who acquires basic knowledge of computing or cybersecurity is capable of becoming a hacker (SX-H-5).

This characteristic of cybercrime tasks is even more pronounced for criminals who are employees of criminal firms, as there is typically an additional division of labour within these firms. As observed by Fengshu and Mandong, two police officers, members within many cybercriminal firms often operate as 'ordinary employees' (GX-P-1, GZ-P-9). Rules that resemble the company regulations of legitimate firms found in a case report can best support their claim. A group leader of a cyber fraud firm testified in the case report:

> 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. (LECID-2)

Another member from the same firm wrote: '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).

From the accounts given by these cybercriminals, it is striking to observe that typical corporate concepts such as office hours, performance indicators, work discipline, and overtime prevalent in legitimate businesses are equally applicable to the cybercrime industry. This finding strongly supports Collier et al.'s (2021) argument that as cybercrime becomes industrialised, this illicit economy begins to replicate the division of labour, cultural tensions, and alienation found in the mainstream economy, rendering the activities of cybercriminals into a profound and tangible experience of intense boredom.

Building on the aforementioned discovery, the second consequence of industrialisation on the activities of cybercriminals is that it obscures the boundary between cybercrime and traditional crime. As observed in numerous operations, whether by independent criminals or the 'employees', their tasks bear a close resemblance to those traditionally associated with street crime, such as the illicit trade of bank accounts and identity cards. Furthermore, there appears to be a minimal barrier for traditional criminals transitioning into cybercrime. This could account for the close associations between street criminals and cybercriminals observed in the Netherlands (Leukfeldt, 2014; Leukfeldt et al., 2019; Leukfeldt et al., 2017a; Leukfeldt et al., 2017b; Leukfeldt and Roks, 2021; Leukfeldt and Yar, 2016).

In addition, as has seldom been discussed in previous studies, as a result of cybercrime industrialisation, many tasks performed by cybercriminals, when viewed in isolation, may not be even readily classified as illicit. For example, the tasks of machine maintainers consist merely of swapping out SIM cards, maintaining the machines, and regularly relocating them. Likewise, the role of drainers is simply to encourage individuals to add certain SNS accounts to their friend lists. The activities in themselves do not constitute anything illegal. This has significantly increased the difficulties for law enforcement in tackling these cybercrime facilitators, as Yi, a police officer, complained: 'If you consider these behaviours in isolation, they cannot be even deemed criminal. It's only when you link everything together that you can categorise them as cybercrime' (GD-P-8).

Discussion and conclusion

In the wake of global cybercrime industrialisation, the past two decades have witnessed the transformation of Chinese cybercrime from patriotic hacking into a sophisticated profit-driven industry. Largely in line with the existing studies on cybercrime industrialisation and Chinese cybercrime, the current study found that a comprehensive industry has been constructed around cyber fraud with a variety of market actors working on mundane and repetitive tasks to support the successful operation of cyber fraud (Hutchings, 2018; Levchenko et al., 2011; Yip, 2010; Zhuang and Ma, 2021). There are also cybercriminal firms in the industry that imitate the structure and operation strategies of legitimate companies (Franceschini et al., 2023; Leukfeldt et al., 2017b; Lusthaus, 2018; Lusthaus and Varese, 2021). With the presence of well-developed market and firms, the study shows that cybercrime in

China has evolved into an economic industry (Coase, 1937; Williamson, 1996). Fundamental economic principles and patterns should, therefore, be able to be applied to understand Chinese cybercrime (Collier et al., 2021; Lusthaus, 2018; Lusthaus et al., 2022).

From the perspective of industrialisation's influence on cybercrime personnel, with the advancement of industrialisation, the cybercriminal market is evolving, with an expanding value chain and an increasing number of specialised roles. This significantly simplifies the formerly complex cybercrime activities. The rise of cybercriminal firms has further simplified the process. Inside these firms, a strict division of labour breaks down what might be a single 'service' or 'product' into numerous, more straightforward tasks. Consequently, much like the Industrial Revolution reshaped traditional manufacturing, the industrialisation of cybercrime has turned it into an assembly line operation, with each participant performing simple, dull, and repetitive work on a daily basis. In this sense, cybercrime has indeed become 'boring' (Collier et al., 2021).

This shift in the nature of cybercriminals' work appears to lower the entry barrier to cybercrime, seemingly challenging the binary distinction between 'traditional crime' and 'cybercrime'. As Leukfeldt and colleagues' research indicates, there are many similarities between cybercriminals and traditional criminals, with many conventional criminals engaging in cybercriminal activities (Leukfeldt, 2014; Leukfeldt et al., 2019; Leukfeldt and Roks, 2021). Wang et al. (2021) also note a trend of traditional criminals transitioning to cybercrime. In this light, under the trend of global cybercrime industrialisation, the boundary between cybercrime and traditional crime has become exceedingly indistinct. Thus, in line with Lusthaus (2024), the paper argues that rather than defining cybercrime as a distinct category, it might be more apt to consider it as an extension and modern evolution of traditional crime. On one hand, academia should attempt to apply traditional criminological, sociological, and economic theories to understand cybercrime. On the other hand, by identifying and interpreting the conflicts, traditional theories can evolve to better align with the characteristics of modern society.

The industrialisation of cybercrime has also impacted the policymaking of combating such activities. On one hand, the number of industries requiring regulation due to their involvement in cybercrime has expanded, such as the telecommunications and online payment sectors. The regulatory gaps in these industries can easily lead to the emergence of cybercrime facilitators, further complicating the cybercrime industry. On the other hand, the simplification of cybercriminal activities has led to the decriminalisation of many behaviours, presenting significant challenges to law enforcement in terms of evidence gathering and subsequent sentencing. Consequently, the focus of cybercrime governance needs to encompass all sectors of modern society, not merely the internet sphere. Additionally, legislators need to pay attention to these decriminalised cybercrime-facilitating activities and actively contemplate how to address the legal difficulties law enforcement encounters in combating cybercrime. What is more, there must be awareness of the global expansion of the cybercrime industry. As the empirical evidence suggested, there has been an increasing number of Chinese cybercriminals moving overseas. Therefore, strengthening cooperation with other countries in combating cybercrime has become a pressing issue. As previously mentioned, both cybercriminals and victims overseas are predominantly Chinese, making it essential to explore ways to enhance the willingness of other countries to collaborate. Additionally, the international expansion of the cybercrime industry may be supported by traditional organised crime, such as human smuggling organisations. Increasing efforts to combat these traditional organised crimes and strengthening border controls may also help reduce the scale of international expansion. Finally, further investigation is needed into the patterns and underlying causes of the expansion of Chinese cybercriminals abroad, in order to develop more targeted crime prevention policies.

The current research has several limitations. There is missing data from numerous provinces in China due to the influence of the COVID-19 pandemic. It is possible that not all perspectives in China can be represented here. There is also a lack of the offender's perspective, as most of the interviewees are law enforcement and cybersecurity practitioners. Efforts to compensate for this issue have been made by including secondary data in the analysis, such as the case reports, but the risk remains. Due to the constraints of the scope and length, this paper also does not provide a comprehensive analysis of the international expansion of China's criminal industry. Subject to the limitations, this empirical study is, however, the first attempt at systematically examining the cybercrime industry in China. Building on the findings of this research, future studies in this field could benefit from enhanced data and improved research designs, allowing for deeper examination of the Chinese cybercrime industry or a broader exploration of the cybercrime industry across different countries to further advance the discussion.

Data availability

Data sharing is not applicable due to the nature of this research. Following the research ethics, the researcher has a responsibility to protect the privacy of the interview participants and the secrecy of the interview content, the interview data therefore cannot be shared. In addition, the secondary data contains sensitive confidential information such as the police investigation process. They also cannot be shared.

Received: 27 March 2024; Accepted: 18 October 2024;
Published online: 15 November 2024

References

Catino M (2019) Mafia organizations. Cambridge University Press

Chen S, Hao M, Ding F, Jiang D, Dong J, Zhang S, Guo Q, Gao C (2023) Exploring the global geography of cybercrime and its driving forces. Humanit Soc Sci Commun 10(1):71. https://doi.org/10.1057/s41599-023-01560-x

Coase RH (1937) The Nature of the Firm. Economics 4:386–405

Coleman EG, Golub A (2008) Hacker practice: Moral genres and the cultural articulation of liberalism. Anthropol Theory 8(3):255–277

Collier B, Clayton R, Hutchings A, Thomas D (2021) Cybercrime is (often) boring: Infrastructure and alienation in a deviant subculture. Br J Criminol 61(5):1407–1423. https://doi.org/10.1093/bjc/azab026

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

Franceschini I, Li L, Bo M (2023) Compound capitalism: a political economy of Southeast Asia's online scam operations. Crit Asian Stud 55(4):575–603. https://doi.org/10.1080/14672715.2023.2268104

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

Hang R (2014) Freedom for authoritarianism: patriotic hackers and Chinese nationalism. Yale Rev Int Stud 5(1):47–64

Henderson, SJ (2007). The dark visitor: inside the world of Chinese hackers. Lulu.com

Hutchings A (2018) Leaving on a jet plane: the trade in fraudulently obtained airline tickets. Crime Law Soc Chang 70(4):461–487

Jankowski MS (1991) Islands in the street: gangs and American urban society, vol. 159. University of California Press Berkeley

Kshetri N (2013) Cybercrime and cyber-security issues associated with China: some economic and institutional considerations. Electron Commer Res 13:41–69

Lee CS (2022) Online fraud victimization in China: a case study of Baidu Tieba. In: The new technology of financial crime. Routledge, pp 62–81

Leukfeldt ER (2014) Cybercrime and social ties: Phishing in Amsterdam. Trends in organized crime. https://doi.org/10.1007/s12117-014-9229-5

Leukfeldt ER, Kleemans ER, Kruisbergen EW, Roks RA (2019) Criminal networks in a digitised world: on the nexus of borderless opportunities and local embeddedness. Trends Organ Crime 22(3):324–345. https://doi.org/10.1007/s12117-019-09366-7

Leukfeldt ER, Kleemans ER, Stol WP (2017a) A typology of cybercriminal networks: from low-tech all-rounders to high-tech specialists. Crime Law Soc Chang 67:21–37

Leukfeldt ER, Lavorgna A, Kleemans ER (2017b) Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime. Eur J Crim Policy Res 23(3): 287–300. https://doi.org/10.1007/s10610-016-9332-z

Leukfeldt ER, Roks RA (2021) Cybercrimes on the streets of the Netherlands? An exploration of the intersection of cybercrimes and street crimes. Deviant Behav 42(11):1458–1469. https://doi.org/10.1080/01639625.2020.1755587

Leukfeldt ER, Yar M (2016) Applying routine activity theory to cybercrime: a theoretical and empirical analysis. Deviant Behav 37(3):263–280. https://doi.org/10.1080/01639625.2015.1012409

Levchenko K, Pitsillidis A, Chachra N, Enright B, Félegyházi M, Grier C, Halvorson T, Kanich C, Kreibich C, Liu H et al. (2011). Click trajectories: end-to-end analysis of the spam value chain. 2011 IEEE symposium on security and privacy. IEEE, pp 431–446

Levy S (1984) Hackers: heroes of the computer revolution (Vol. 14). Anchor Press/Doubleday, Garden City, NY

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). IEEE, pp 474–480

Lusthaus J (2020) Cybercrime in Southeast Asia. Austral Strategic Policy Inst Australia Tech Rep 29:2020

Lusthaus J (2024) Reconsidering Crime and Technology: What Is This Thing We Call Cybercrime? Ann Rev Law Soc Sci 20(1):369–385

Lusthaus J, van Oss J, Amann P (2022) The Gozi group: a criminal firm in cyberspace? Eur J Criminol 147737082210776. https://doi.org/10.1177/14773708221077615

Lusthaus J, Varese F (2021) Offline and local: the hidden face of cybercrime. Polic J Policy Pract 15(1):4–14. https://doi.org/10.1093/police/pax042

Morgan S (2020, November 13). Cybercrime to cost the world $10.5 trillion annually by 2025. Cybercrime Magazine. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Morselli C, Giguère C, Petit K (2007) The efficiency/security trade-off in criminal networks. Soc Netw 29(1):143–153

Nguyen T, Luong HT (2021) The structure of cybercrime networks: Transnational computer fraud in Vietnam. J Crime Justice 44(4):419–440

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

Schelling TC (1967) Economics and criminal enterprise. Public Interest 7:61

Shortland A (2019) Kidnap: inside the ransom business. Oxford University Press

Soudijn MRJ, Zegers BCHT (2012) Cybercrime and virtual offender convergence settings. Trends Organ Crime 15(2–3):111–129. https://doi.org/10.1007/s12117-012-9159-z

The China Judicial Big Data Research Institute. (2022, July). Special Judicial big data report on characteristics and trends of cybercrime. https://file.chinacourt.org/f.php?id=c9b92b185f359c81&class=enclosure

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

Von Lampe K (2015) Organized crime: analyzing illegal activities, criminal structures, and extra-legal governance. Sage Publications

Wang P (2017) The Chinese Mafia: organized crime, corruption, and extra-legal protection. Oxford University Press

Wang P, Su M, Wang J (2021) Organized crime in cyberspace: how traditional organized criminal groups exploit the online peer-to-peer lending market in China. Br J Criminol 61(2):303–324

Wang Y (2018) 'Xiao Shi De Hei Ke' [the disappeared hackers]. Southern people weekly. https://www.nfpeople.com/article/5439

Webber C, Yip M (2018) The rise of Chinese cyber warriors: towards a theoretical model of online hacktivism. Int J Cyber Criminol 12(1):230–254

Williamson OE (1996) The mechanisms of governance. Oxford university press

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

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. In ACM Web Science Conference. Koblenz, Germany. IEEE, pp 1–4

Zhao Y, Gan T, Luo Q (2024) Beidong Juanru Yu Zhudong Xuanze—Qingnian Canyu Dianxinwangluozhapian Fanzui De Guochengxing Jizhi [Passive Involvement and Active Choice: The Mechanisms of Youth Engagement in Cyber Fraud]. Youth Explor 4:55–67. https://doi.org/10.13583/j.cnki.issn1004-3780.2024.04.005

Zhuang H, Ma Z(2021) Dongnanya Diqu Zhongguo Gongmin Kuajing Wangluo Fanzui ji Zhili Yanjiu [Cross-Border Cyber Crime of Chinese Citizens in Southeast Asia and Its Governance]. Nanyang Wenti Yanjiu [Southeast Asian Aff] 4:41–54

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

Acknowledgements

The author is grateful to Federico Varese and Jonathan Lusthaus for their excellent supervision, and to the CrimGov group members: Martina Baradel, Zora Hauser, Elena Racheva, Alae Baha, Emilia Ziosi, Jack Warburton, Fanqi Zeng and Miranda Bruce for their comments on an earlier version of this paper. Special thanks are extended to Professors Ishizuka Shinichi, Masahiro Tsushima, and Koichi Hamai for hosting me at the Corrections and Rehabilitation Center, Ryukoku University, while I was writing this paper. Finally, I would like to express sincere gratitude to the anonymous reviewers for their insightful comments and constructive feedback, which greatly contributed to improving the quality of this paper. The work is supported by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (No. 101020598 – CRIMGOV, PI: Federico Varese).

Author contributions

I am the sole author of the article.

Competing interests

The author declares no competing interests.

Ethical approval

Approval was obtained from the Social Sciences and Humanities Inter-divisional Research Ethics Committee of the University of Oxford (reference no: R66962/RE001) on 13th February 2020. This research complies with the procedures established by the University of Oxford for the ethical approval of all research involving human participants. The ethical approval permits the researcher to conduct interviews and collect and use secondary data. The research was conducted in accordance with the guidelines set forth by the British Society of Criminology's Statement of Ethics for Researchers in the Field of Criminology and the British Sociological Association's Statement of Ethical Practice.

Informed consent

All participants were adults, and no vulnerable individuals were involved. Informed oral consent for participation, use of data, and publication was obtained from all interview participants before the interview started. Oral consent was used for two reasons: (1) the topic is sensitive, making it impractical to obtain written consent from participants, and (2) considering the cultural and political concerns in China, the existence of paper records could pose a risk to both the researcher and the participants. For the same reason, the oral consent itself was not recorded. Before the interview began, I read the information from my oral consent form aloud and asked if participants minded if I recorded the conversation and used the data for research and publication. Then I asked for oral consent verbally, by asking participants to state their name, agree to participate, and indicate whether or not they minded if the interview was recorded. The interview only commenced after oral consent had been given, and the conversation was recorded only if oral consent was provided. No payment or other incentives were offered in this research. Codes and randomly assigned pseudonyms were used to refer to participants to ensure anonymity. Informed consent to use the secondary data for publication in academic journals was also obtained from participants who provided me the data. Participants were fully informed about how their anonymity would be protected, the purpose of the research, how their data would be used, and any potential risks of participation.

Additional information

Supplementary information The online version contains supplementary material available at https://doi.org/10.1057/s41599-024-04042-w.

Correspondence and requests for materials should be addressed to Qiaoyu Luo.

Reprints and permission information is available at http://www.nature.com/reprints