Police Cooperation and the Fight Against Cross-Border Crime along Belt and Road Countries: The Emergence and Proliferation of Telecommunication Fraud in Greater China

Sonny Shiu-Hing Lo 盧兆興教授

Abstract

Instances of telecommunication fraud in the region of Greater China – the Peoples Republic of China (PRC), Hong Kong, Macao and Taiwan – have increased since 2015. Some criminal elements involved in telecommunication fraud have been operating in Belt and Road countries outside either the PRC or Taiwan. The governments of Greater China have been cooperating to combat telecommunication fraud. This paper examines the pattern of telecommunication fraud and addresses the issue of how the governments of China and Taiwan have been tackling it in cooperation with the countries involved in the Belt and Road Initiative (BRI).

Introduction

The BRI has brought about an unprecedented degree of human interaction across national boundaries; nevertheless, a challenge tothe BRI is the spread of cross-border criminal activities. Cross-border crimes can be seen as a result of the liberalisation of border control; they are exacerbated by the greediness of criminal organisations and, to some extent, bureaucratic

corruption in law enforcement (Lo, 2009). This paper will explore how police cooperation in the combat against cross-border crime has been playing a significant role in the development and prospects of countries participating in the BRI. Apart from utilising the BRI as a platform to strengthen economic and diplomatic relations with various countries in the world, the PRC also hopes to consolidate security relations with them (Brown, 2018, p. 215). Traditionally, China has cooperated with many countries along the BRI to fight against various types of crimes, such as smuggling, drug trafficking and terrorism. In recent years, the joint efforts made by China and many other countries to combat telecommunication fraud have become more urgent with the rising popularity of the internet. This digital aspect is becoming a hallmark of cross-border crime control between China and many BRI countries. With the increased cooperation between the Chinese police and their counterparts of various countries, the prospects for the BRI in consolidating multilateral trade and cultural-social as well as economic linkages remain optimistic. Efforts at fighting cross-border telecommunication fraud include intelligence gathering and sharing among law-enforcement agencies, reports from the mass media, and the vigilance of the citizens who are the victims of such crimes. The persistence of these efforts can and will contribute to the success of the BRI.

The Rise of Telecommunication Fraud in Greater China

Telecommunication fraud recently has surged in the region of Greater China. From 2011 to April 2015, police in China and their Taiwanese counterparts actually arrested 7,700 Chinese people from both places, with approximately 4,600 of the 7,700 arrested coming from Taiwan. In May 2015, for instance, 32 Taiwanese criminal suspects who had made calls from a Malaysia-based telecommunication fraud syndicate were arrested by the Malaysian authorities. But the Taiwanese were handed back to the law-enforcement authorities of the PRC rather than to the Republic of China (ROC) on Taiwan. Some Taiwan people argued that the Taiwanese should be sent back to the island republic rather than to the Mainland. However, the PRC police contended that since most of the victims were Mainlanders, and 50 percent of the losses were due to Taiwanese-led syndicates, those detained should face trial in the PRC.

In another case, in November 2015, the PRC police cooperated with their counterparts in Indonesia, Hong Kong and Taiwan to arrange the return of 254 Mainland Chinese criminal suspects involved in a huge cross-border telecommunication fraud syndicate (Mai, 2015). Ninety people in Guangdong province were arrested, including seven Taiwanese. Working from bases in Indonesia and the Philippines, they cheated citizens of Hong Kong and Taiwan by making calls to the Chinese in both places, pretending that they were PRC police officers and claiming that the victims had committed criminal offences, as a pretext for demanding monetary compensation. The money stolen by the Taiwanese syndicate went to Taiwan-based bank accounts. In March 2016, PRC police uncovered another extortion plot in which a 50-year-old man had lost RMB 2.7 billion, through a telephone fraud in which scammers falsely accused him of laundering dirty money for which they held an arrest warrant against him. His funds also found their way to a Taiwanese account.

Efforts at fighting cross-border telecommunication fraud include intelligence gathering and sharing among law-enforcement agencies, reports from the mass media, and the vigilance of the citizens who are the victims of such crimes.

These are typical of the numerous examples of cross-border telecommunication fraud. Several characteristics are prominent. First and foremost, the criminals often operate from

bases outside the PRC and Taiwan so that law-enforcement authorities in both places cannot arrest them easily. Second, when the Taiwanese suspects are arrested, the PRC government often requests that they, along with Mainland Chinese criminal suspects, should be sent back to the PRC for trial because the victims of telecommunication fraud are mainly from the PRC. While most third countries have sent back all the criminal suspects to the PRC, including both Mainland and Taiwan Chinese, the Taiwan authorities naturally hope that Taiwanese suspects should be sent directly to Taiwan.

In August 2016, five Taiwanese criminal suspects were declared by a Kenya court not guilty of telecommunication fraud, but surprisingly they were later sent back to Mainland China, leading to a complaint from the Taiwan foreign ministry (*Apple Daily*, 2016: A19). The Taiwan government also asked its PRC counterpart to report on the personal safety of the five Taiwanese in accordance with the 2009 agreement between the PRC and ROC governing the custody of cross-border criminal suspects. Yet, in response to Taiwan's concern, PRC authorities dismissed the request, contending that the new Taiwan government under the presidency of Tsai Ing-wen should do more to resume the communication channels between the two sides.

Responses from Taiwan and the PRC

Despite the sour relations reflecting renewed tensions between the PRC and the Taiwan governments on how to handle Taiwanese people being arrested by a third country, both governments have recently taken strong measures to deal with cross-border criminal activities. In November 2016, the Taiwan Legislative Yuan revised Article 5 of the Criminal Law (*Criminal Code of the Republic of China*, 2018), adding more legal penalties for Taiwanese citizens who commit crime through their participation in cross-border telecommunication fraud. Those people convicted of serious offenses under this law can be imprisoned for 20 years maximum. The term "cross-border criminal fraud" was also added to Article 5, authorising the judicial authorities not only to impose stiffer penalties but also to take jurisdiction over the management of these criminal suspects. Nevertheless, empowering the judicial authorities to have such jurisdiction is one thing; whether the PRC authorities and the third countries will allow the Taiwan government to exercise that jurisdiction appears to be another matter.

Meanwhile, the PRC authorities have also increased the penalties for telecommunication fraud. On December 20, 2016, a legal document issued by the Supreme People's Court, the Supreme People's Procuratorate and the Ministry of Public Security proposed that offenders convicted of telecommunication fraud amounting to or exceeding 3,000 yuan would be imprisoned for a minimum of three years, and that those offenders cheating other people for any amount over 500,000 yuan would be imprisoned indefinitely (*China Daily*, 2016: 5). Obviously, internet crime has become so serious in the PRC that the criminal courts and police authorities have to adopt stringent measures to curb its growth.

Nevertheless, since Taiwan has diplomatic relations with relatively few countries in the world, extradition of criminal suspects involved in telecommunication fraud directly from the country concerned to Taiwan remains difficult. Many Taiwanese criminal suspects try to exploit the loophole resulting from Taiwan's lacking extradition agreements with many countries in the world. However, some Taiwanese criminal suspects involved in telecommunication fraud have received imprisonment sentences from the countries where they started the fraud operation. For example, in February 2018, four Taiwanese who were arrested in Thailand for engaging in telecommunication fraud and money laundering were imprisoned for 16 years and six months in Thailand – a heavy penalty that could act as a deterrent to Taiwan criminal suspects (*Ta Kung Pao*, 2018a: A19).

For countries that do not have diplomatic relations with Taipei, in cases where Taiwanese criminal suspects stand accused of telecommunication frauds involving Mainland Chinese, the PRC requested that the accused be sent directly to the PRC for trial. In December

2017, the PRC government formally requested that the South Korean government should extradite 51 Taiwanese criminal suspects in a telecommunication fraud, which cheated not only Taiwanese but also Mainland Chinese (*Ming Pao*, 2017: A11).

One challenge in the struggle against telecommunication fraud is that many Taiwanese involved in telecommunication fraud are young people, who have taken the risk of getting rich by participating in such activities. In 2016, 71.77 percent of the 21,576 Taiwan residents who committed telecommunication fraud in the island republic was from the age group between 18 and 39 (*Ta Kung Pao*, 2018a).

evasion and related money laundering activities. In Hong Kong, from 2010 to 2018, for example, a rich woman was cheated by her so-called "lover" through the internet, causing her to lose a total of HK$1.4 million via remittances to Malaysia. In October 2018, the police in Hong Kong, Malaysia and Singapore smashed a telecommunication fraud syndicate that recruited 52 people from the three places to disguise themselves as actors, footballers, professionals, military officers and rich people, cheating mostly Chinese women in the Greater China region (*Wen Wei Po*, 2018: A01; *Ta Kung Pao*, 2018b: A04). The 28 Hong Kong people arrested in this ring opened accounts in Hong Kong to facilitate the process of money laundering after the victims sent their money to the syndicate. After securing the trust of their victims, syndicate members got the details of their credit cards and account information, and in the 147 cases stole a total amount of almost HK$110 million.

> If the PRC is keen to promote its model of good governance to other countries along the BRI, then there are grounds for optimism in the struggle against cross-border telecommunication fraud, which is in the common interest of all countries along the BRI, and in the world.

The PRC government recognises the severity of telecommunication fraud and has taken immediate measures to address it. On 18 and 19 April 2018, State Councillor and Minister of Public Security Zhao Kezhi chaired a nationwide conference in Shenzhen on combatting crime, including telecommunication fraud. Many public security chiefs attended as he emphasised the need for the utilisation of artificial intelligence and big data to fight crime (*Sing Tao Daily*, 2018: A24). President Xi Jinping also held a meeting on 20 and 21 April to follow up on the conference, emphasising the importance of internet security, the need for education of the netizens, and the importance of self-discipline among internet webmasters and professionals in cooperation with the government to fight internet crime.

Investment fraud and tax evasion are also commonplace in the operation of telecommunication fraud syndicates. In August 2018, the PRC authorities cracked down on tax evasion by celebrities, including Fan Bingbing, who opened studios and empty shell companies in Korgas in Xinjiang. Many of these studios and companies were suspected of being involved in large-scale money laundering, even though the film industry was trying to expand into the west through the BRI.

A New Pattern

Recently, a new pattern of telecommunication fraud has emerged in the Greater China region, including (1) manufactured love affairs, (2) investment fraud, and (3) tax

Implications for BRI Development

The rapid growth of telecommunication fraud within the Greater China region has become the most prominent challenge in combatting cross-border crime. It necessitates

frequent cooperation among the police in Greater China (Lo, 2018). Whether stronger penalties can stem the tide of telecommunication fraud remains unclear, but it is certain that education of all the citizens in the regions of Greater China has begun so that the number of victims can and will be minimised. While education of ordinary citizens is easier in both Hong Kong and Macao, the same measures may not be effective in the relatively vast and diverse geographical areas of China and, to some extent, Taiwan. As such, the PRC relies on technological advancement, such as the mobilisation of Big Data, to assist its police force in cracking down on telecommunication fraud syndicates.

Of course, education alone cannot curb telecommunication fraud in the era of globalisation and regionalisation culminating in the development of the BRI. Fortunately, cross-border police cooperation between the PRC and Hong Kong on the one hand and other foreign states on the other hand has succeeded in mitigating the spread of telecommunication fraud in the era of the BRI. The high tide of telecommunication fraud took place in 2016 and its crackdown began in 2017 until the present. As of early 2019, the incidence of telecommunication fraud appears to have declined. Very few reports on telecommunication fraud have been seen, recently, in the local press. The most probable reason is that, as 2019 represents the seventieth anniversary of the PRC, Beijing hopes to honour the year as an historical symbol of the Chinese Communist Party's success. As such, domestic crime and cross-border crime have to be put under tight control, along with a very aggressive united front campaign targeted at winning the hearts and minds of the people of Hong Kong (Lo, Hung and Loo, 2019). Still, it remains to be seen whether telecommunication fraud will resurge again after 2019.

In the context of security in Greater China, the police in Hong Kong appear to be the most effective in curbing telecommunication fraud, followed by Macao, mainland China and Taiwan. The small physical size of the cities of Hong Kong and Macao means that the police forces can control telecommunication fraud relatively easily. The Macao police have been cooperating with their Zhuhai counterparts to crack down on computer-based schemes to cheat local citizens by imitating the techniques of telecommunication fraud syndicates. The police forces in mainland China are more complex, necessitating cross-provincial and cross-cities agreements to share intelligence and work together. Taiwan has realised the severity of telecommunication fraud syndicates that also involve their own citizens. In fact, the Taiwan government and police have also made tremendous efforts at fighting telecommunication fraud within Taiwan, while cooperating with foreign countries and also the PRC to extradite Taiwan criminal suspects. After all, cross-border telecommunication fraud syndicates that involve a large number of Taiwanese have already tarnished the good image of Taiwan. Therefore, it is in the common interest of the four governments in the Greater China region to exert effective control on the emergence and operation of telecommunication fraud syndicates.

From the perspective of the security challenges in and for the BRI, telecommunication fraud constitutes a menace to not only the domestic security of the PRC but also its image in the world. As such, the PRC has taken swift and tough action against criminal elements involved in the telecommunication fraudulent syndicates, especially the Taiwanese. In the minds of PRC leaders, such syndicates are like the new *heidao* (triads) that threaten the regime security of the Chinese Communist Party. They have undermined the good image of the PRC at a time when President Xi Jinping's BRI is in full swing. They have also been taking advantage of the political tensions between Beijing and Taipei. In short, telecommunication fraud syndicates are seen as the enemies of the PRC government, which can no longer tolerate their existence and operations.

From the perspective of foreign countries where criminal elements from the PRC and Taiwan operate their telecommunication fraud schemes, there is willingness to cooperate with the police forces in the Greater China region to fight these criminal activities. However, such illicit activities

might make some foreign countries cast doubts on whether the BRI championed by the PRC can and will be as smooth as it is presented in the official rhetoric. To calm the anxieties of foreign countries, the PRC has already made strenuous efforts at combatting cross-boundary crime, while emphasising the need for good governance, for example, in anti-corruption work. If the PRC is keen to promote its model of good governance to other countries along the BRI, then there are grounds for optimism in the struggle against cross-border telecommunication fraud, which is in the common interest of all countries along the BRI, and in the world.

Finally, from the broader perspective of fighting transnational organised crime, telecommunication fraud syndicates have displayed unique features. Unlike the traditionally hierarchical and tightly organised nature of crime syndicates like the Italian and American mafia (Cressey, 1997), the syndicates that involve Mainland Chinese and Taiwanese in countries outside Greater China appear to be organised quite loosely and are based on personal networks. As the Chinese attach great importance to the concept of *guanxi* (personal connections), it plays a crucial role in recruiting members to join and operate these criminal syndicates. Yet, since the telecommunication fraud syndicates in Belt and Road countries often involve a mixture of both mainland Chinese and Taiwanese, their composition is relatively loose and their *guanxi* is based on the common objective of making quick profits. Furthermore, these syndicates often target their own ethnic group, the Chinese in their hometowns. While their ethnic target is narrow and focused, the support networks extend to non-Chinese accomplices providing logistical support and bases rather than the key leaders in their organisations. Indeed, these telecommunication fraud syndicates cheat their victims through the internet by utilising personal data stolen in the regions of Greater China. Identity theft is commonplace in the regions of Greater China, where many individuals are relatively insensitive to this problem, and where private-sector organisations and companies acquire personal data easily without much by way of safeguards to protect their privacy.

As such, the roots of telecommunication fraud syndicates are deep in the regions of Greater China. Their complete elimination may be a bridge too far, but the education of ordinary citizens and private-sector organisations on how to protect the personal data of individuals can be a first step toward the prevention of such crime, followed by multiple measures, notably the sharing of criminal intelligence among police forces in Greater China and the persistent cooperation between them and their overseas counterparts.

Sonny Shiu-Hing Lo, HKU Space

References

Apple Daily (2016, August 9), A19.

Brown, K. (2018). The Belt and Road: Security Dimensions. *Asia Europe Journal*, 16 (3), 213-222.

China Daily (2016, December 21), 5.

Cressey, D. R. (1997), The Functions and Structure of Criminal Syndicates. In Patrick Ryan, George E. Rush (Eds.), *Understanding Organized Crime in Global Perspective: A Reader*. London: Sage Publications.

Criminal Code of the Republic of China (2018, June 13). Retrieved from https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=C0000001

Lo, S. S. (2018). *The Politics of Policing in Greater China*. London: Palgrave.

Lo, S. S. (2016). *The Politics of Controlling Organized Crime in Greater China*. London: Routledge.

Lo, S. S. (2009). *The Politics of Cross-Border Crime in Greater China*, New York: M. E. Sharpe.

Lo, S. S., Hung, S. C., Loo, J. H. (2019). *China's New United Front Work in Hong Kong: Penetrative politics and its implications*. London: Palgrave Macmillan.

Ming Pao, (2017, December 23), A11.

Mai, J. (2015, November 10). "Hundreds arrested as police crack phone-scam gangs based overseas targeting Hong Kong, mainland China." *South China Morning Post*. Retrieved from https://www.scmp.com

Oriental Daily News, April 21, 2019, A24.

Sing Tao Daily (2018, April 21), A24.

Ta Kung Pao (2018a, February 23), A19.

Ta Kung Pao (2018b, October 27), A4.

Wen Wei Po (2018, October 28), A1.