QUESTIONNAIRE

CHINA

Xingan LI

International Institute for Innovation Society

1. Introduction

Please read carefully before answering the questionnaire

The RAYUELA project is aimed at protecting children in their online interactions. For this purpose, the project will develop a "game", which will present the children with realistic scenarios relating to the following cybercrimes/cyber-facilitated crimes:

- ***Online grooming*** (further: OG) is the crime where the perpetrator (usually an adult) uses electronic communication services, including social media, to contact a minor and build rapport with the aim of eventually meeting in person for the purposes of sexual activity. The perpetrator may employ various strategies (deception, romantic/emotional attachment, promise of material or other benefits, blackmail, coercion, etc.) to lower a child's inhibitions, heighten their curiosity about sexual experiences, or otherwise convince them to meet up.
- ***Cyber bullying*** (further: CB) is a broad term that includes all types of bullying behaviour online. This includes cyber stalking and cyber harassment, and any other type of behaviour online aimed at hurting the victim. Cyber bullying may also have a sexual component.
- ***Misinformation and deception*** (further: MD) is a behaviour that may or may not be punishable by law depending on the context. It involves all kinds of information sharing that is fake, or deceptive. For a criminal qualification to apply, typically the behaviour will need to be intentional and there will need to be material consequences to this intention.
- ***Human trafficking with a cyber component*** (further: HT) is the online facilitation of human trafficking by grooming and attracting potential victims for human trafficking.

The purpose of the game is to teach children how to remain safe online, while the obtained insights will be used to provide policy recommendations and educational tools.

The game does not focus solely on the threats of potentially falling victim to one of these four crimes. It also aims to raise awareness about the general threats of using IT, such as the Internet and connected devices, and minors' capacity to make responsible choices in this regard.

A particular point of interest is understanding whether minors are aware of when they, or someone else, is crossing the line in becoming offenders themselves, as this an important aspect of protecting children online. Due to the nature of online communication, inhibitions may be lowered, and certain actions may feel more innocent or less "real" than in real life. In addition, a perception may exist that what happens on the Internet has little or no impact beyond the digital world. This creates situations where minors engage in what they perceive to be relatively innocent behaviour ("everyone does this on the internet"), that may however have serious legal consequences.

One of the goals in RAYUELA is to ensure that minors realize when their behaviour may turn into actions that are punishable by law.

The present study and questionnaire are set up in the context of the RAYUELA project in order to provide an overview of the **legislative framework and relevant policies** in a number of countries, both in the EU and beyond, in relation to:

- How the main crimes of OG, CB, MD and HT are dealt with by the legal system i.e., which behaviours are punishable and under which conditions?
- How cybercrime and cyber-facilitated crime perpetrated by minors is dealt with in the legal system (both in general and specifically in relation to the crimes in focus)?
- What international instruments and cooperation mechanisms are available in dealing with cybercrime perpetrated by minors?

Importantly, we want to know both the legal rules and policies which are implemented in practice, and their effect on the **real enforcement situation**. If you have knowledge about the effects of current policies on crime rates by minors and on the crime rates for OG, CB, MD and HT, this would be of interest.

We are specifically interested in **case law** that illustrates the "why and how" of certain legal rules, principles and policies in practice. Case law will help us illustrate the similarities and differences between jurisdictions and is therefore *essential***.** Please ensure to have a good amount of case law processed in your answers.

In addition, we want input on **international legal instruments and international cooperation** relevant for cybercrime, and in particular for cybercrime perpetrated by minors. What happens when cybercrimes is perpetrated in a cross-border context? What are the legal rules in place for cooperation with authorities from other countries, and how does this work out in practice (issues, problems, etc.)?

Lastly, we are interested in some **statistical information on cybercrime** in your country and cybercrime by minors specifically.

The purpose of this questionnaire is to help you provide this information for your jurisdiction.

2. Questions relating to OG, CB, HT and MD with minors as victims

Question 1: Is online grooming punishable by law in your country?

Answer:

Please explain the applicable rules (all applicable legal qualifications/ articles, conditions for application, prescriptive period, and the range and types of punishment that may be imposed and jurisdictional aspects in cross-border cases) and applicable policy.

Yes. Online grooming is punishable according to the Criminal Law of the People's Republic of China Article 240. Those abducting and trafficking women or children are to be sentenced to 5 to 10 years in prison plus fine. Those falling into one or more of the following cases are to be sentenced to 10 years of more in prison or to be given life sentences, in addition to fines or confiscation of property. Those committing especially serious crimes are to be sentenced to death in addition to confiscation of property.

(1) Primary elements of rings engaging in abducting and trafficking women or children;

(2) those abducting and trafficking more than three women and/or children;

(3) those raping abducted women;

(4) those seducing, tricking, or forcing abducted women into prostitution, or those selling abducted women to others who in turn force them into prostitution;

(5) those kidnapping women or children using force, coercion, or narcotics, for the purpose of selling them;

(6) those stealing or robbing infants or babies for the purpose of selling them;

(7) those causing abducted women or children, or their family members, to serious injuries or death, or causing other grave consequences;

(8) those selling abducted women or children to outside the country.

Abducting and trafficking women or children refers to abducting, kidnapping, buying, selling, transporting, or transshipping women or children.

Article 241. Those buying abducted women or children are to be sentenced to three years or fewer in prison, or put under criminal detention or surveillance.

Those buying abducted women and forcing them to have sex with them are to be convicted and punished according to stipulations of article 236.

Those buying abducted women or children and illegally depriving them of or restricting their physical freedom, or injuring or insulting them, are to be convicted and punished according to relevant stipulations of this law.

Those buying abducted women or children and committing crimes stipulated in paragraphs two and three of this article are to be punished for committing more than one crime.

Those buying and selling abducted women or children are to be convicted and punished according to article 240 of this law.

Those buying abducted women or children but not obstructing bought women from returning to their original residence in accordance with their wishes, or not abusing bought children and not obstructing efforts to rescue them, may not be investigated for their criminal liability.

Article 262: Whoever abducts a minor under the age of fourteen and leaves his family or guardian shall be sentenced to fixed-term imprisonment of not more than five years or criminal detention.

Even though there is no explicit regulation on online grooming, the act is directly included in the broad constituent element of "abducting", which covers the use of deception, inducement or other means to take away minors under the age of fourteen.

Please provide case law to illustrate the application of the rules in practice.

Cases decided by courts of different levels have only weak value of reference by but not binding to other courts.

At about 20:00 on May 21, 2013, the defendant Li Xia found that Zuo So-and-So led his grandson Chen So-and-So (under 2 years old) and his granddaughter to play in Century Square, Xiangfu District, Kaifeng City, Henan Province, and abducting the child taking advantage of Zuo So-and-So not paying attention. Later, Li Xia pretended to be Chen So-and-So's mother, and posted on the Internet to collect 50,000 yuan to put Chen So-and-So for adoption. Defendant Sun Zewei contacted Li Xia after seeing the message, and met and traded on May 23. Without verifying the identity and relationship between Li Xia and Chen So-and-So, after bargaining, Sun Zewei paid Li Xia 40,000 yuan to take Chen So-and-So to his home in Caoxian County, Heze City, Shandong Province. After the public security organ solved the case, Chen So-and-So was rescued and returned to his relatives.

The People's Court of Xiangfu District, Kaifeng City, Henan Province held that Li Xia abducted the child for the purpose of selling it, and his behavior constituted the crime of child abduction. Sun Zewei's buying of abducted children constituted the crime of buying children who were abducted and trafficked. According to the relevant provisions of the Criminal Law, the defendant Li Xia was sentenced to 10 years in prison and a fine of RMB 20,000 for the crime of abducting and selling children; the defendant Sun Zewei was sentenced to seven months imprisonment for the crime of buying and selling children who were abducted.

Question 2: Is cyberbullying punishable by law in your country? Please take into account a broad understanding of cyberbullying (cyber/online stalking, harassment, sexual harassment)?

Answer:

Please explain the applicable rules (all applicable legal qualifications/ articles, conditions for application, prescriptive period, and the range and types of punishment that may be imposed and jurisdictional aspects in cross-border cases) and applicable policy.

Yes. Within the framework of Chinese law, cyberbullying can be dealt with based on different crimes according to the judicial interpretation issued by the Supreme People's Court and the Supreme People's Procuratorate of the People's Republic of China in 2013, on the application of laws related to the use of information networks to carry out relevant crimes, which clearly stated that any one of the following circumstances shall be convicted and punished for the crime of defamation: 1. Fabricating facts that damage the reputation of others, disseminating them on the information network, or organizing , instigating personnel to spread on the information network. 2. The original content of information involving others on the information network is tampered with the facts that damage the reputation of others, and disseminated on the information network, or organized or instructed personnel to spread it on the information network.

Those who have one of the following circumstances shall be convicted and punished as the crime of picking quarrels and provoking trouble: 1. Using information networks to abuse or intimidate others, the circumstances are vile, and the social order is disrupted. 2. Fabricating false information, or

knowingly fabricating false information, spreading it on the information network, or organizing or instigating personnel to spread it on the information network, causing trouble and causing serious public disorder.

Please provide details on known issues of application.

Here is a case in which application of laws proved to be impossible. The Liu Xuezhou incident is a suicide incident involving human trafficking and cyber violence in the People's Republic of China in January 2022. The person involved, Liu Xuezhou,who was a second-year student of preschool education at Shijiazhuang Law and Commerce Secondary School. From December 14, 2021 to January 24, 2022, Liu Xuezhou searched for his biological parents and broke out conflicts with his biological parents. The Beijing News and Red Star News wrote articles implying that Liu Xuezhou was a "human tragedy" and destroyed his biological mother's "normal life", "White Eyed Wolf", a series of incidents of asking their parents to donate a house as compensation, encountering Internet bullying, and finally taking drugs and committing suicide. The incident has attracted official attention and prompted Chinese online platforms to advance measures to prevent cyberbullying. However, no person has ever been investigated or punished for the wrongdoing.

Question 3: When would misinformation and deception online constitute a criminal offence in your country? In other words, what potential qualifications could apply to wilful misinformation and deception on the internet?

Answer:

Please explain the applicable rules (all applicable legal qualifications/ articles, conditions for application, prescriptive period, and the range and types of punishment that may be imposed and jurisdictional aspects in cross-border cases) and applicable policy.

Yes. Within the framework of Chinese law, misinformation and deception online can be punishable according to several different laws, which provide classifications of information according to the contents, as well as offences in which information is exploited differently. Therefore, there are several legal instruments applicable.

Paragraph 6 of Article 14 of the 2019 "Regulations on the Administration of Business Sites for Internet Access Services": Internet access service business premises operators and online consumers shall not use the Internet access service business premises to produce, download, copy, consult, publish, disseminate or otherwise use information containing the following contents: (1) Opposing the basic principles established by the Constitution; (2) Endangering national unity, sovereignty and territorial integrity; (3) divulging state secrets, endangering state security or damaging state honor and interests; (4) Inciting ethnic hatred, ethnic discrimination, undermining ethnic unity, or infringing upon ethnic customs and habits; (5) Undermining the state's religious policy and promoting cults and superstitions; (6) Spreading rumors, disturbing social order, and undermining social stability; (7) Propagating obscenity, gambling, violence or instigating crimes; (8) Insulting or slandering others, infringing upon the lawful rights and interests of others; (9) Endangering social morality or excellent national cultural traditions; (10) Contains other content prohibited by laws and administrative regulations.

Article 48 of the 2017 "Emergency Regulations on Major Animal Epidemics": During the occurrence of major animal epidemics, those who drive up prices, deceive consumers, spread rumors, and disrupt social and market order shall be subject to administrative penalties by the competent pricing department, industry and commerce administrative department or public security organ according to law; if a crime is constituted, criminal responsibility shall be investigated according to law.

Paragraph 5 of Article 5 of the 2011 "Administrative Measures for the Security Protection of International Networking of Computer Information Networks": No unit or individual may use the international network to produce, copy, consult and disseminate the following information: (1) Incitement to resist or undermine the implementation of the Constitution and laws and administrative regulations; (2) Inciting subversion of state power and overthrow of the socialist system; (3) Incitement to split the country and undermine national unity; (4) Inciting ethnic hatred, ethnic discrimination, or undermining ethnic unity; (5) Fabricating or distorting facts, spreading rumors, and disrupting social order; (6) Advocating feudal superstition, obscenity, pornography, gambling, violence, murder, terror, or instigating crimes; (7) Openly insulting others or fabricating facts to slander others; (8) Damage to the credibility of state organs; (9) Other violations of the Constitution, laws and administrative regulations.

Article 15 of the 2011 "Destructive Earthquake Emergency Regulations": Earthquake forecasts shall be issued uniformly by the people's governments of provinces, autonomous regions and municipalities directly under the Central Government in accordance with the provisions of the State Council on the issuance of earthquake forecasts, and no other organization or individual may issue earthquake forecasts. No organization or individual may spread rumors about the earthquake. When earthquake rumors occur, the competent department of earthquake prevention and disaster reduction work shall assist the people's government to quickly quell and clarify them.

Article 52 of the 2011 Regulations on Public Health Emergencies: During the occurrence of emergencies, those who spread rumors, drive up prices, deceive consumers, and disrupt social order and market order shall be given administrative penalties by the public security organs or the administrative departments for industry and commerce; if a crime is constituted, criminal responsibility shall be investigated according to law.

Article 74 of the 1998 Interim Regulations on the Administration of Stock Issuance and Trading: Any unit or individual who violates the provisions of these Regulations and commits one of the following acts shall, depending on the circumstances, be given a single or concurrent warning, confiscation of illegally obtained stocks and other illegal gains, and a fine: (1) Conducting stock trading outside the securities trading venues approved by the Securities Commission for stock trading; (2) Making false or seriously misleading statements or omitting material information in the process of stock issuance and trading; (3) Manipulating stock market prices by conspiring or concentrating funds, or influencing stock issuance and trading by means such as spreading rumors; (4) colluding with others in order to create false prices of stocks, without transferring the ownership or actual control of stocks, and buying and selling falsely; (5) Selling or offering to sell stocks that it does not hold, disrupting the order of the stock market; (6) Exploiting power or other illegitimate means to solicit or forcibly buy or sell stocks, or assist others to buy or sell stocks; (7) Trading stock and index options and futures without approval; (8) Failure to perform the obligations of reporting, disclosing and publishing relevant documents and information in accordance with regulations; (9) Forging, tampering with or destroying business records, financial account books and other documents related to stock issuance and trading; (10) Other illegally engaging in stock issuance, trading and related activities. A company limited by shares has the acts listed in the preceding paragraph, and if the circumstances are serious, its qualification to issue stocks may be suspended; if a securities business institution has the acts listed in the preceding paragraph, and the circumstances are serious, its securities business may be restricted, suspended or cancelled. license.

Article 25 of the Public Security Administration Punishment Law: Whoever commits any of the following acts shall be detained for not less than five days but not more than 10 days, and may concurrently be fined not more than 500 yuan; if the circumstances are relatively minor, he shall be detained for not more than five days or be fined not more than 500 yuan: (1) Spreading rumors and falsely reporting dangerous situations , epidemic situation, police situation, or intentionally disrupting public order by other means; (2) Disrupting public order by throwing false explosive, toxic, radioactive,

corrosive substances or infectious disease pathogens and other dangerous substances; (3) Threatening to commit arson, explosion, or throwing dangerous substances to disrupt public order.

Article 101 of the General Principles of Civil Law": Citizens and legal persons have the right to reputation, and citizens' personal dignity is protected by law. It is forbidden to damage the reputation of citizens and legal persons by means of insults and slander.

Article 120 of the General Principles of Civil Law: Citizens whose rights to name, portrait, reputation, and honor are infringed have the right to demand that the infringement be stopped, their reputation be restored, the impact removed, an apology be made, and compensation for losses may be demanded.

Paragraph 2 of Article 105 of the Criminal Law: The crime of inciting subversion of state power. Those who organize, plan, and carry out subversion of state power or the overthrow of the socialist system shall be sentenced to life imprisonment or fixed-term imprisonment of not less than 10 years for the ringleaders or if the crime is serious; those who actively participate shall be sentenced to fixed-term imprisonment of not less than three years but not more than 10 years; Those who participate shall be sentenced to fixed-term imprisonment of not more than three years, criminal detention, public surveillance or deprivation of political rights. Whoever incites subversion of state power or the overthrow of the socialist system by spreading rumors, slander or other means shall be sentenced to fixed-term imprisonment of not more than five years, criminal detention, public surveillance or deprivation of political rights; if the ringleader or the crime is serious, he shall be sentenced to fixed-term imprisonment of not less than five years.

Article 246 of the Criminal Law: Crimes of insult and libel. Whoever uses violence or other methods to publicly insult others or fabricate facts to slander others, if the circumstances are serious, shall be sentenced to fixed-term imprisonment of not more than three years, criminal detention, public surveillance or deprivation of political rights. The crimes in the preceding paragraph shall be dealt with only if they are notified, except those that seriously endanger social order and national interests. If the victim files a complaint to the people's court through the information network, but it is really difficult to provide evidence, the people's court may request the public security organ to provide assistance.

Paragraph 2 of Article 5 of the Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues Concerning the Application of Law in Handling Criminal Cases of Defamation by Using Information Networks (hereinafter referred to as the Interpretation). Those who use information networks to abuse or intimidate others, with vile circumstances and disrupt social order, shall be convicted and punished for the crime of picking quarrels and provoking trouble in accordance with the provisions of Article 293, Paragraph 1 (2) of the Criminal Law. Whoever fabricates false information, or clearly knows that it is fabricated false information, spreads it on the information network, or organizes or instructs personnel to spread it on the information network, causing trouble and causing serious chaos in the public order, according to Article 293 of the Criminal Law Item (4) of paragraph (4) shall be convicted and punished for the crime of picking quarrels and provoking trouble.

Paragraph 1 of Article 291-1 of the Criminal Law: The crime of fabricating and intentionally disseminating false terrorist information Fabricating terrorist information such as explosion threats, biological threats, and radiological threats, or deliberately spreading terrorist information knowing that it is fabricated, and seriously disrupting social order. Paragraph 2 of Article 291-1 of the Criminal Law: The crime of fabricating or intentionally disseminating false information The crime of fabricating or intentionally disseminating false information refers to fabricating false dangers, epidemics, disasters, and police situations, and disseminating them on information networks or other media, or Knowing that it is the above-mentioned false information, deliberately spreading it on the information network or other media, and seriously disrupting the social order.

Please provide case law to illustrate the application of the rules in practice.

The case (2020) Xiang 01 Xingzhong 79.

Defendant Li was dissatisfied with the government's demolition of self-built illegal buildings, and published an article "Report: Huangtutang Demolition Headquarters in Furong District, when will you hang the oxygen of the veterans of the Anti-Japanese War", the article was forwarded 5020 times, Commented 603 times; published "The whole life of the war veteran's family is threatened! Four sons of veterans were arrested for no reason", "Public officials, where is the conscience, the backbone of the nation, how can they be trampled on like this", the content is "Huang, a staff member of the Huangtutang Demolition Headquarters in Furong District, Changsha City, on the afternoon of July 17, 2017. At 4:39, after driving a car (Xiang A × × xx) at the bus stop in front of the Yahua Hotel in Bayi Road, he deliberately hit the 98-year-old Anti-Japanese War veteran, and then ran backwards at full speed for dozens of meters to hit and run! Haven't shown up yet!". The two Weibo posts were read 14,851 times and reposted 3,344 times respectively; the content of "Snatch the Corpse! This way to comfort the anti-Japanese hero" reads "At 4:40 a.m. on January 3, 2018, multiple police cars and more than 100 staff members, forcibly rushed into the mourning hall of the Anti-Japanese War veteran Li Mou (the children of the Anti-Japanese War veteran Li Mou had not arranged the indoor mourning hall for him). Under the strict supervision of dozens of staff members, he forcibly took away the remains of the Anti-Japanese War veteran Li Mou." This Weibo has been read 2298 times, reposted 24 times, commented 9 times, and reposted on Tianya Forum, Xichihong Jiexun, Zhimeng 58, Entertainment Full Search, Xuancai News Network and other websites, seriously damaging the image of the local government, the social impact is bad. The court held that in order to realize his unreasonable demands, Li distorted the facts and used the real-name registration of the "Rescue Soldier" Weibo account to spread false information such as his father's being bumped into and his body being robbed. Damage the image of the local government and cause serious chaos in the network public order, and his behavior constitutes the crime of picking quarrels and provoking trouble. Defendant Li was sentenced to one year in prison for the crime of picking quarrels and provoking trouble.

The case (2020) Lu 01 Xing Zhong 80.

Defendant Peng So-and-So publicly published more than 50 articles and messages on the Internet, including "Real-Name Report of Shandong Departmental-level Cadres Living Promiscuously, Bank Assets Lost Nearly 3 Billion Yuan". It contains "Jinan Nongmou concealed a case involving financial fraud, resulting in a loss of nearly 3 billion yuan in bank assets", "Ding So-and-So and Zong So-and-So B, Wang So-and-So and Lu So-and-So have improper sexual relations and have children"" Peng So-and-So was downgraded for violation of regulations, and there was no response to the petition report", "The Provincial Rural Credit Cooperative Fund Center has a 'small treasury' without accountability, and the loan to Shandong Hongfan Energy Technology Co., Ltd. caused losses" and other false information. The above articles and information were reprinted and reported by more than 10 online media including Sina, Sohu, Phoenix, Tencent, NetEase, etc., which triggered a large number of clicks, retweets and negative comments by netizens, and the number of clicks exceeded 10 million times, causing serious public disorder. The court held that the behavior of the defendant Peng So-and-So constituted the crime of picking quarrels and provoking trouble. According to the facts, nature, circumstances and degree of harm to society of Peng So-and-So's crime, in accordance with Article 293(1)(4) of the Criminal Law of the People's Republic of China, Article 25(1), Article 64 and Paragraph 2 of Article 5 of the Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues Concerning the Application of Law in Handling Criminal Cases of Defamation by Using Information Networks, defendant Peng So-and-So was sentenced to four years of imprisonment for the crime of picking quarrels and provoking trouble.

Question 4: What constitutes human trafficking and how is human trafficking facilitated by electronic means punished in your country? Are online grooming activities to find victims (e.g. lover boys) before the actual human trafficking punishable in itself? In addition, are these activities punishable as a separate crime if human trafficking does take place afterward?

Answer:

According to the Criminal Law of the People's Republic of China, Article 240, Whoever abducts and traffics women or children shall be sentenced to fixed-term imprisonment of not less than five years but not more than 10 years and shall also be fined; whoever falls under any of the following circumstances shall be sentenced to fixed-term imprisonment of not less than 10 years or life imprisonment, and shall also be fined or confiscation of property; If the circumstances are particularly serious, the death penalty shall be imposed and the property shall be confiscated:

(1) Leaders of groups that traffic in women and children;

(2) Trafficking in three or more women and children;

(3) raping a woman who has been abducted;

(4) Luring or forcing abducted women into prostitution or selling abducted women to others to force them into prostitution;

(5) Kidnapping women or children by violence, coercion or anesthesia for the purpose of selling;

(6) Stealing infants and young children for the purpose of selling;

(7) Causing serious injury, death or other serious consequences to the abducted women, children or their relatives;

(8) Selling women and children abroad. Abduction of women and children refers to any of the acts of abducting, kidnapping, buying, selling, picking up or transferring women or children for the purpose of selling.

Article 241 Whoever buys abducted women or children shall be sentenced to fixed-term imprisonment of not more than three years, criminal detention or public surveillance. Whoever buys a trafficked woman and forcibly has sexual relations with her shall be convicted and punished in accordance with the provisions of Article 236 of this Law. Whoever buys abducted women or children, illegally deprives or restricts their personal freedom, or commits crimes such as harming or insulting them, shall be convicted and punished in accordance with the relevant provisions of this Law. Whoever buys abducted and trafficked women or children and commits the criminal acts specified in the second and third paragraphs shall be punished in accordance with the provisions of combined punishment for multiple crimes. Whoever buys abducted and trafficked women or children and then sells them shall be convicted and punished in accordance with the provisions of Article 240 of this Law. Bought abducted women and children, if there is no abuse of the children to be bought, and does not hinder their rescue, a lighter punishment may be given; according to the wishes of the women being bought, if they do not hinder their return to their original place of residence, they may be given a lighter or reduced punishment penalty.

Article 242 Whoever obstructs, by means of violence or threats, the staff of state organs to rescue the women or children who have been bought off shall be convicted and punished in accordance with the provisions of Article 277 of this Law. The ringleader who gathers a crowd to obstruct state organ staff from rescuing the women or children who have been bought shall be sentenced to fixed-term

imprisonment of not more than five years or criminal detention; other participants who use violence or threats shall be punished in accordance with the provisions of the preceding paragraph.

Questions regarding cybercrime or cyber-facilitated crime committed by minors

Question 5: How is crime committed by minors dealt with in your country, in general? Is there a specific juvenile justice system? If yes, please explain in detail how this works.

Answer:

According to the Criminal Law of the People's Republic of China, Article 17, A person who has reached the age of sixteen commits a crime and shall bear criminal responsibility. Persons between the age of fourteen and sixteen who commit intentional homicide, intentional injury to cause serious injury or death, rape, robbery, drug trafficking, arson, explosion, or throwing dangerous substances shall bear criminal responsibility. A person who has reached the age of 12 but has not yet reached the age of 14 commits the crime of intentional homicide or intentional injury, causing death or causing serious injury by particularly cruel means and causing serious disability. Persons under the age of 18 who are investigated for criminal responsibility in accordance with the provisions of the preceding three paragraphs shall be given a lighter or reduced punishment. For those who are not subject to criminal punishment because they are under the age of 16, their parents or other guardians shall be ordered to discipline them; when necessary, special correctional education shall be conducted in accordance with the law.

Article 38 of China Law on the Protection of Minors stipulates: "For minors who violate the law and commit crimes, the policy of education, probation, and rescue shall be implemented. The principle of education as the main and punishment as the supplement shall be adhered to."

Article 44 of the "Law of the People's Republic of China on the Prevention of Juvenile Delinquency" also clearly stipulates: "The juvenile who commits a crime shall be investigated for criminal responsibility, the policy of education, probation and rescue shall be implemented, and the principle of education as the main and punishment as the supplement shall be adhered to.."

In China, crime committed by minors is dealt with according to the principle of divisional handling, which refers to the separation of legal procedures, separate detention and separate execution of juvenile cases and adult cases.

Separation of proceedings refers to cases where minors and adults commit a crime or are involved together, as long as the proceedings are not hindered, they should be handled separately.

Article 40 of the "Law of the People's Republic of China on the Protection of Minors" clearly stipulates: "Public security organs, people's procuratorates, and people's courts handling juvenile crime cases shall take care of the physical and mental characteristics of juveniles, and may set up special agencies or designate Professional handling." Article 20 of the Supreme People's Procuratorate's "Regulations on the Handling of Juvenile Criminal Cases by the People's Procuratorate" clearly stipulates that "a minor and an adult criminal case initiated by the People's Procuratorate for public prosecution shall be handled separately if it does not interfere with the trial of the case."

Separate detention means that when compulsory measures such as detention and arrest are applied to minors, minors and adults are to be detained separately for custody. Article 41 of the "Law of the People's Republic of China on the Protection of Minors" clearly states: "The public security organs, the people's procuratorates, and the people's courts shall take care of the minors in pretrial custody separately from the detained adults." Article 46 of the "Law of the People's Republic of China on the

Prevention of Juvenile Delinquency" also clearly stipulates that minors and adults who are detained, arrested and executed shall be detained, managed and educated separately.

Separate enforcement refers to the enforcement of effective judgments and rulings on minors, which must be separated from adults and cannot be placed in the same place to prevent adult criminals from having adverse effects on juvenile criminals. In my country's judicial practice, juvenile offenders are generally executed in juvenile correctional centers. Paragraph 2 of Article 41 of the "Law of the People's Republic of China on the Protection of Minors" clearly stipulates: "Minors who have been sentenced by people's courts to serve their sentences shall be detained and managed separately from the adults serving their sentences." The second half of Article 46 of the Crime Law also clearly stipulates: "During the period when a juvenile offender is being sentenced, the enforcement organ shall strengthen legal education for juvenile offenders, and conduct vocational and technical education for juvenile offenders. For juvenile delinquents who are educated, the executive organ shall ensure that they continue to receive compulsory education.

Question 6: Are there specific rules or is there a specific policy that deals with cybercrime by minors as a special topic, acknowledging the special characteristics of crime by minors in the cyber environment, and the fact that minors may not knowingly or intentionally break rules (issues with criminal intent)? Even absent a written policy, are minors prosecuted for cybercrime in practice?

Answer:

It could be safe to say that any minor suspects shall be dealt with according to specific rules or specific policy applicable in dealing with all crimes. However, there are hardly any specific rules specifically applicable in dealing with minor suspects involved in cybercrime.

Question 7: Can minors be punished for online grooming in your country? I.e. the situation of a minor capable of providing sexual consent (e.g. 17 year-old) grooming a minor who has not reached the age of sexual consent (e.g. 13 years old) to meet up with the intent to perform sexual activities? Please focus not only on the specific crime of online grooming (which, if present as a separate crime in your jurisdiction, often requires an adult perpetrator), but also on other crimes that would punish the activities that constitute online grooming (i.e. the use of different strategies to force a meeting with the minor victim with the intent to perform sexual activities). If criminal sanctions could apply, are minors prosecuted in practice?

Answer:

Yes. According to Criminal Law of the People’s Republic of China, people beyond the age of 14 years old can be held responsible for grooming a female minor under the age of 14 years old, if the victim was raped with or without her consent.

If the victim is beyond the age of 14 years old, the perpetrator shall only be held responsible if the victim was raped forcibly by the perpetrator.

Question 8: Can minors be punished for purely online behaviour with a sexual intent when other minors are the victim? E.g. the situation where a minor perpetrator obtains sexually explicit material from the minor victim in order to sell this or to force the victim to do something. If criminal sanctions could apply, are minors prosecuted in practice?

Answer:

This question can be answered from two aspects on the legal context of China. On one hand, according to Criminal Law of the People's Republic of China, people beyond the age of 16 years old shall be responsible for any crimes regardless of the age of the victim. On the other hand, acquiring, holding, transferring, saving, spreading, buying and selling sexually explicit materials, whether they are texts, photos, videos, audios, etc, all constitute punishable crimes, regardless of the victim's age.

Question 9: Can minors be punished for cyberbullying behaviour, without there being a physical component to the crime? This includes behaviours such as cyberstalking and cyberharassment. If criminal sanctions could apply, are minors prosecuted in practice?

Answer:

According to the Public Security Administration Punishment Law of the People's Republic of China, Article 12 Where a person who has reached the age of fourteen but under the age of 18 violates the administration of public security, he shall be given a lighter or mitigated punishment; a person under the age of fourteen who violates the administration of public security shall not be punished, but his guardian shall be ordered to impose stricter discipline. It does not constitute a crime, and according to the specific circumstances, a public security punishment shall be imposed.

Article 42 of the "Public Security Administration Punishment Law" who commits any of the following acts shall be detained for not more than 5 days or fined not more than 500 yuan; if the circumstances are more serious, he shall be detained for not less than 5 days but not more than 10 days, and may concurrently be fined not more than 500 yuan : (1) Writing threatening letters or threatening the personal safety of others by other means; (2) Openly insulting others or fabricating facts to slander others; (3) fabricating facts to falsely accuse and frame others in an attempt to subject others to criminal investigation or public security administration punishment; (4) Threatening, insulting, beating or retaliating against witnesses and their close relatives; (5) Sending obscene, insulting, intimidating or other information multiple times to interfere with the normal life of others; (6) Peeping, secretly photographing, eavesdropping, or spreading the privacy of others.

Theoretically, in China, the determination of sexual harassment, can consider the following:

1. The subjective purpose of the behavior contains sexual demands or intentions involving sexuality. That is, the subjective aspect of the behavior of the perpetrator to carry out sexual harassment must contain the sexual purpose, and such behavior is unwelcome, unwilling, or not interested in the victim the behavior of. However, in view of my country's national conditions, large social places such as stations and squares are often crowded and collided due to limited conditions, so strict identification standards should be adopted.

2. Determination of behavioral patterns. In a broad sense, rape, forced indecency and insulting women are also harassment of women, but to a certain extent, it is more appropriate to call it sexual assault. severe punishment. Sexual harassment is a relatively minor form of sexual assault. Sexual harassment is usually the harasser making unwelcome sexually related language or actions to the harassed person, including physical contact, words, graphic display, eyes and gestures, etc., such as: telling pornographic jokes, commenting, showing pornographic pictures, Publications and supplies, inquiring about sexual privacy, dating, erotic vision, sexual positions, body touching, sexual organ exposure, and more.

3. Definition of occasions for sexual harassment. Sexual harassment can be divided into three situations: one is sexual harassment between superiors and subordinates, employers to employees or colleagues in administrative organs, enterprises and institutions; the second is the situation where employees are

sexually harassed by customers while working for the unit; Sexual harassment among strangers in public places, such as on a bus.

4. The objects of sexual harassment include both women and men; both the opposite sex and the same sex.

Question 10: Can minors be punished for wilful misinformation or deception online (sharing false news, false information, pretending to be someone else, pretending to be an expert, etc.)? Which crimes/qualifications could possibly apply? If criminal sanctions could apply, are minors prosecuted in practice?

Answer:

According to the Public Security Administration Punishment Law of the People\s Republic of China, Article 25, Whoever commits any of the following acts shall be detained for not less than five days but not more than 10 days, and may concurrently be fined not more than 500 yuan; if the circumstances are relatively minor, he shall be detained for not more than five days or be fined not more than 500 yuan: (1) Spreading rumors, falsely reporting danger, epidemic situation, police situation, or intentionally disrupting public order by other means; (2) Disrupting public order by throwing false explosive, toxic, radioactive, corrosive substances or infectious disease pathogens and other dangerous substances; (3) Threatening to commit arson, explosion, or throwing dangerous substances to disrupt public order.

According to the Criminal Law of the People's Republic of China, Article 278, Whoever incites the masses to violently resist the implementation of state laws and administrative regulations shall be sentenced to fixed-term imprisonment of not more than three years, criminal detention, public surveillance, or deprivation of political rights; if serious consequences are caused, they shall be sentenced to fixed-term imprisonment of not less than three years but not more than seven years. Article 287-1 Whoever uses an information network to commit any of the following acts, if the circumstances are serious, shall be sentenced to fixed-term imprisonment of not more than three years or criminal detention, and shall also or only be fined: (1) Establishing websites or communication groups for illegal and criminal activities such as defrauding, imparting criminal methods, producing or selling prohibited items and controlled items; (2) Publishing information about the production or sale of drugs, guns, obscene items and other prohibited items, controlled items, or other illegal and criminal information; (3) Publishing information for the purpose of committing fraud or other illegal and criminal activities. If a unit commits the crime in the preceding paragraph, the unit shall be fined, and the persons in charge and other persons who are directly responsible for it shall be punished in accordance with the provisions of the first paragraph. Whoever commits the acts in the preceding two paragraphs and constitutes other crimes at the same time shall be convicted and punished in accordance with the provisions on heavier punishment.

Article 287-2 Knowing that others use information networks to commit crimes, and providing technical support such as Internet access, server hosting, network storage, communication transmission, or other assistance for their crimes, or providing assistance in advertising promotion, payment and settlement, etc., if the circumstances are serious , shall be sentenced to fixed-term imprisonment of not more than three years or criminal detention, and shall be concurrently or solely fined. If a unit commits the crime in the preceding paragraph, the unit shall be fined, and the persons in charge and other persons who are directly responsible for it shall be punished in accordance with the provisions of the first paragraph. Whoever commits the acts in the preceding two paragraphs and constitutes other crimes at the same time shall be convicted and punished in accordance with the provisions on heavier punishment.

Article 291-1 Putting false explosive, toxic, radioactive, infectious disease pathogens and other substances, or fabricating terrorist information such as explosion threats, biochemical threats,

radiological threats, etc., or knowingly spreading terrorist information that is fabricated, Whoever seriously disturbs social order shall be sentenced to fixed-term imprisonment of not more than five years, criminal detention or public surveillance; if serious consequences are caused, he shall be sentenced to fixed-term imprisonment of not less than five years. Whoever fabricates false dangers, epidemics, disasters, or police situations, and spreads them on information networks or other media, or knowingly spreads the above-mentioned false information on information networks or other media on purpose, and seriously disrupts social order, shall be sentenced to fixed-term imprisonment of not more than three years. criminal detention or public surveillance; if serious consequences are caused, they shall be sentenced to fixed-term imprisonment of not less than three years but not more than seven years.

Article 181 Whoever fabricates and spreads false information that affects securities and futures trading, disrupts the securities and futures trading market, and causes serious consequences, shall be sentenced to fixed-term imprisonment of not more than five years or criminal detention, and concurrently or separately shall be sentenced to not less than 10,000 yuan and 10,000 yuan. A fine of less than 10,000 yuan. Employees of stock exchanges, futures exchanges, securities companies, futures brokerage companies, and staff of securities industry associations, futures industry associations, or securities and futures supervision and administration departments who intentionally provide false information or forge, alter, or destroy transaction records, and deceive If an investor buys or sells securities or futures contracts, causing serious consequences, he shall be sentenced to fixed-term imprisonment of not more than five years or criminal detention, and shall concurrently or solely be sentenced to a fine of not less than 10,000 yuan but not more than 100,000 yuan; if the circumstances are especially serious, he shall be sentenced to fixed-term imprisonment of not less than five years but not more than 10 years. Imprisonment and a fine of not less than 20,000 yuan but not more than 200,000 yuan. Where a unit commits the crimes mentioned in the preceding two paragraphs, the unit shall be sentenced to a fine, and the persons directly in charge and other persons directly responsible shall be sentenced to fixed-term imprisonment of not more than five years or criminal detention.

Question 11: Can minors be punished for online actions facilitating human trafficking? Typically this includes the selection and grooming of victims (e.g. lover boy phenomenon). If criminal sanctions could apply, are minors prosecuted in practice?

Answer:

Yes. Theoretically, people beyond the age of 14 years old are punishable for online actions facilitating human trafficking. Traditionally, human traffickers in China have been normally from the middle-aged or old-aged persons. However, in recent year, there have also been case in which young females were also found to be involved in such cases, particularly where exploitation of their young female friends in prostitution was the purpose.

Question 12: Can minors be punished for acts of online piracy in your jurisdiction, i.e. the illegal use and/or distribution of content protected by intellectual property rights? Please focus on the elements of criminal nature. If criminal sanctions could apply, are minors prosecuted in practice?

Answer:

Only those who are beyond the age of 16 years old are punishable for the crimes of online piracy.

According to the Criminal Law of the People's Republic of China, Article 217, Whoever, for the purpose of making profits, commits any of the following violations of copyright or copyright-related rights, where the amount of illegal gains is relatively large or has other serious circumstances, shall be sentenced to fixed-term imprisonment of not more than three years, and concurrently or exclusively

Fines; if the amount of illegal gains is huge or there are other particularly serious circumstances, the sentence shall be fixed-term imprisonment of not less than three years but not more than 10 years, and a fine:

(1) Without the permission of the copyright owner, copying, distributing, and disseminating to the public their written works, music, art, audio-visual works, computer software and other works stipulated by laws and administrative regulations;

(2) Publishing books for which others have exclusive publishing rights;

(3) Reproducing, distributing, and disseminating the audio and video recordings produced by them to the public through information networks without the permission of the producers of the audio and video recordings;

(4) Reproducing and distributing audio and video recordings of their performances without the performers' permission, or disseminating their performances to the public through information networks;

(5) producing or selling works of art that counterfeit the signature of others;

(6) Without the permission of the copyright owner or the copyright-related obligee, intentionally avoid or destroy the technical measures taken by the obligee to protect the copyright or copyright-related rights for their works, audio and video recordings, etc.

Article 218 Whoever sells, for the purpose of making a profit, knowingly sells the infringing copies specified in Article 217 of this Law, with a huge amount of illegal gains or other serious circumstances, shall be sentenced to fixed-term imprisonment of not more than five years and shall also be sentenced to Or just fine.

Question 13: Can minors be punished for acts of hacking (i.e., unauthorized access to a computer system)? In particular, would this also apply to various scenarios exploiting vulnerabilities in IoT and connected devices? If criminal sanctions could apply, are minors prosecuted in practice?

Answer:

The prerequisite for punishing such crimes is that the suspect is beyond the age of 16 years old.

The "Network Security Law" clearly stipulates that no individual or organization shall engage in activities that endanger network security, such as illegally intruding into other people's networks, interfering with the normal functions of other people's networks, stealing network data, etc.; Measures, stealing network data and other programs and tools that endanger network security activities.

According to the Public Security Administration Punishment Law, Article 29 Whoever commits any of the following acts shall be detained for not more than five days; if the circumstances are more serious, he shall be detained for not less than five days but not more than 10 days: (1) Violating state regulations, intruding into computer information systems and causing harm; (2) Violating state regulations by deleting, modifying, adding, or interfering with the functions of the computer information system, causing the computer information system to fail to operate normally; (3) Deleting, modifying or adding data and application programs stored, processed or transmitted in the computer information system in violation of state regulations; (4) Deliberately creating or spreading destructive programs such as computer viruses that affect the normal operation of computer information systems.

According to the Criminal Law of the People’s Republic of China, Article 285, Whoever violates state regulations and invades computer information systems in the fields of state affairs, national defense construction, and advanced science and technology shall be sentenced to fixed-term imprisonment of not more than three years or criminal detention. Violating state regulations, hacking into a computer

information system other than those specified in the preceding paragraph or using other technical means to obtain data stored, processed or transmitted in the computer information system, or illegally controlling the computer information system, if the circumstances are serious, he shall be sentenced to three years The following fixed-term imprisonment or criminal detention shall be concurrently or solely fined; if the circumstances are particularly serious, the sentence shall be fixed-term imprisonment of not less than three years but not more than seven years and a fine. Whoever provides programs or tools specially used to invade or illegally control computer information systems, or provides programs or tools for others knowingly committing illegal and criminal acts of invading or illegally controlling computer information systems, if the circumstances are serious, shall be punished in accordance with the provisions of the preceding paragraph. If a unit commits the crimes mentioned in the preceding three paragraphs, the unit shall be fined, and the persons in charge and other persons who are directly responsible for it shall be punished in accordance with the provisions of the respective paragraphs.

Article 286 Whoever, in violation of state regulations, deletes, modifies, adds or interferes with the functions of a computer information system, causing the computer information system to fail to operate normally, and the consequences are serious, shall be sentenced to fixed-term imprisonment of not more than five years or criminal detention; if the consequences are especially serious , shall be sentenced to fixed-term imprisonment of not less than five years. Violation of state regulations to delete, modify or add data and applications stored, processed or transmitted in computer information systems, with serious consequences, shall be punished in accordance with the provisions of the preceding paragraph. Deliberately making or spreading destructive programs such as computer viruses that affect the normal operation of the computer system, with serious consequences, shall be punished in accordance with the provisions of the first paragraph. If a unit commits the crimes mentioned in the preceding three paragraphs, the unit shall be fined, and the persons in charge and other persons who are directly responsible for it shall be punished in accordance with the provisions of the first paragraph.

Question 14: Can minors be punished for acts of using Cybercrime as a Service? If yes, under what qualification? In particular, how would this apply to using such services for exploiting vulnerabilities in IoT and connected devices e.g., the device of a friend or acquaintance? Does it matter if the intent is somewhat innocent (i.e., the minor thinks it's a joke or a prank)? If criminal sanctions could apply, are minors prosecuted in practice?

Answer:

Please explain the applicable rules (all applicable legal qualifications/articles, conditions for application, prescriptive period, and the range and types of punishment that may be imposed and jurisdictional aspects in cross-border cases) and applicable policy.

The prerequisite for punishing such crimes is that the suspect is beyond the age of 16 years old.

1. General questions regarding cross border cybercrime, international legal instruments applicable to fighting cybercrime and regarding international cooperation

Question 15: How does your country deal with the cross-border nature of many cybercrimes? When is jurisdiction established? Can judgements have extra-territorial effect?

Answer:

According to the Criminal Law of the People\s Republic of China, Article 6, This Law shall apply to all crimes committed within the territory of the People's Republic of China, unless otherwise specified by law. This Law shall also apply to anyone who commits a crime on a ship or aircraft of the People's Republic of China. If one of the criminal acts or results occurs within the territory of the People's Republic of China, it shall be deemed to be a crime within the territory of the People's Republic of China.

Article 7 This Law shall apply to citizens of the People's Republic of China who commit crimes stipulated in this Law outside the territory of the People's Republic of China, but if the maximum punishment stipulated in this Law is fixed-term imprisonment of not more than three years, they may not be investigated. This Law shall apply to state functionaries and military personnel of the People's Republic of China who commit crimes specified in this Law outside the territory of the People's Republic of China.

Article 8 If a foreigner commits a crime against the country or citizens of the People's Republic of China outside the territory of the People's Republic of China, and the minimum sentence prescribed by this Law is fixed-term imprisonment of not less than three years, this Law may be applied, but he shall not be punished according to the law of the place where the crime was committed. except.

Article 9 This Law shall apply to the crimes stipulated in the international treaties concluded or acceded to by the People's Republic of China, where the People's Republic of China exercises criminal jurisdiction within the scope of its obligations under the treaty.

Article 10 Anyone who commits a crime outside the territory of the People's Republic of China and who shall bear criminal responsibility in accordance with this Law may still be investigated in accordance with this Law even though he has been tried in a foreign country, but if he has already received criminal punishment in a foreign country, his punishment may be exempted or mitigated.

Article 11 The criminal responsibility of foreigners who enjoy diplomatic privileges and immunities shall be resolved through diplomatic channels.

Paragraph 1 of Article 77 of the Interpretation of the Supreme People's Court on the Application of the Criminal Procedure Law of the People's Republic of China in 2021 stipulates: "For evidence materials from abroad, the people's procuratorate shall transfer the relevant source, provider, and extractor along with the case. , extraction time, etc. After review by the people's court, if the relevant evidence materials can prove the facts of the case and meet the provisions of the Criminal Procedure Law, they can be used as evidence, but the scope of use of the materials by the provider or the bilateral treaties signed between my country and the relevant countries Except for those with clear restrictions; if the source of the material is unknown or the authenticity cannot be confirmed, it shall not be used as the basis for the verdict." Paragraph 2 of this article relaxes the procedural requirements for the parties, their defenders, and agents ad litem to provide overseas evidence.

Articles 58 and 59 of the 2021 "People's Procuratorate's Regulations on Handling Cybercrime Cases" make detailed provisions on the transfer and custody of overseas criminal evidence. What needs further attention is that different types of foreign evidence should be treated differently, and special rules for judging the admissibility of foreign criminal evidence should be established.

Question 16: What international legal instruments (bi-lateral, multi-lateral) apply in your country to the fight against (cross-border) cybercrime and how have they been implemented in national law (if implementation is necessary)?

Answer:

There have not been known international treaties specifically dealing with cybercrime. However, an increasing number of countries have concluded treaties or established other mechanisms on criminal judicial assistance. Many cybercrime cases involving Chinese and foreign perpetrators were solved based on case-to-case cooperating mechanisms.

Question 17: What forms of international cooperation exist in your country to the fight against cross-border cybercrime? Please describe different routes/options/procedures and the measures that can be requested (e.g., asking for investigative actions, exchange of information/evidence, etc.)?

Answer:

Here are some example international actions taken by Chinese authorities to fight against cross/border cybercrime.

In 2002, APEC released the Cyber Security Strategy, which has been incorporated into the Shanghai Declaration. The strategy outlines six areas of cooperation between member economies, including legal development, information sharing and cooperation, safety and technical guidelines, public awareness, and training and education.

In 2003, China signed the UN General Assembly Resolution 57/239 on "Creating a Global Cybersecurity Culture".

In 2003, China signed the Geneva Declaration of Principles of the World Summit on the Information Society.

In 2005, China signed the London Spam Action Plan, an international effort to curb the problem. Held the anti-spam "Beijing Declaration" 2006 International Anti-Spam Summit.

In July 2006, the ASEAN Regional Forum (ARF), which includes China, issued a statement asking its members to enforce cybercrime and cybersecurity laws "in accordance with their national circumstances and with reference to relevant international instruments".

In 2009, the China-ASEAN Network and Information Security Emergency Response Framework Agreement was adopted.

In 2009, an agreement was reached within the Shanghai Cooperation Organization on information security. The APEC Telecommunications Working Group agreed on an action plan for 2010-2015, which includes "cultivating a secure and trustworthy ICT environment".

In January 2011, China and the United States for the first time pledged at the head of state to work together on a bilateral basis on cybersecurity issues. "Building Trust with Spam" will be the first effort to help overcome the lack of trust between the U.S. and China over cybersecurity.

In 2020, the "Global Data Security Initiative" will be proposed, focusing on major issues such as critical infrastructure and personal information protection, overseas data storage and retrieval of enterprises, and supply chain security, and propose constructive solutions for maintaining global data and network security. The public security organs promote the establishment of closer and more efficient cooperative relations with other countries to jointly combat transnational cybercrime activities. my country has established bilateral police cooperation relations with the police of nearly 30 countries including the United States, the United Kingdom, and Germany; relying on the Interpol Asia-Pacific Working Group on Combating Information Technology Crimes, a cooperation mechanism for annual meetings has been established in the Asia-Pacific region; The country has established a liaison mechanism for cybercrime investigation personnel; it has jointly established the Asian Computer Crime Internet Network (CTINS)

with 14 countries including Japan and South Korea to exchange cybercrime trends and share investigation and evidence collection technologies in a timely manner; relying on the Shanghai Cooperation Organization, it has formulated the "Shanghai Cooperation Organize member states to ensure international information security action plan, and established a cooperation mechanism for cybercrime investigation and evidence collection.

In December 2015, China and the United States signed the Guiding Principles on Combating Cybercrime and Related Matters, which played a positive role in coordinating differences in network management and control and establishing a dialogue mechanism to jointly combat cybercrime. "

Question 18: Do the rules (national, international) and policies mentioned in your answers in this section have any particular effect or impact on cybercrime committed by minors?

Answer:

It is not clear whether these rules and policies have any particular direct effect or impact on cybercrime committed by minors. However, as a part of the whole social control system, Chinese law emphasizes “comprehensive management of social security”. Regardless of its practical effects, these rules and policies could play a role in educating, deterring, and punishing potential minor actors, partly due to the severe punishment and partly due to prevention by motivated families, schools and even residential areas.

Other

Question 19: Do you have any information on the rates/statistics of cybercrime in your country and their recent evolution? Of particular interest would be statistics related specifically to the crimes covered in this questionnaire and statistics on cybercrime by minors (ideally also specifically for the crimes covered above)? If there were any (relatively) recent legislative or policy changes, please try to find statistical information on how this has impacted the incidence of cybercrime in practice, and in particular cybercrime by minors.

Answer:

Due to the sophistication of cybercriminal offenses and difficulties in categorizing them, there has not been a unified approach of statistics in China. We could only get information on the scale of cybercrime from different viewpoints from different authorities.

From the points of view of courts, in terms of cybercrime cases, from 2016 to 2018, more than 48,000 cybercrime cases have been closed, and the number of cases and the proportion of all criminal cases in the total number of criminal cases have been increasing year by year. In 2018, the number of cases increased significantly, with a year-on-year increase of 50.91 %; the proportion of defendants under the age of 18 is decreasing year by year.

From the points of view of police, in 2020, public security organs across the country further promoted the "Cleaning the Internet 2020" special campaign. In the whole year, a total of 56,000 cybercrime cases were investigated and more than 80,000 criminal suspects were arrested. Among these cases, 6,524 cases of infringing on citizens' personal information were investigated and 13,000 criminal suspects were arrested; 1,782 hacking and new technology crime cases were investigated and 2,975 criminal suspects were arrested; more than 10,000 cyber criminal cases were investigated and handled , arrested 15,000 criminal suspects, seized more than 5.48 million "mobile phone black cards", seized more than 220 million online accounts involved in the case, and promptly prevented more than 18.5 million IoT cards from entering the black market.

From the points of view of prosecutors, in 2020, procuratorial organs nationwide prosecuted 142,000 cybercriminals, a year-on-year increase of 47.9%; national courts concluded 33,000 criminal cases such as cyber fraud, online pyramid schemes, online gambling, cyber hacking, and cyber rumors.

In 2021, a report cponmcluded that, after the Supreme People's Procuratorate, together with the Ministry of Public Security, had issued guidelines for handling criminal cases such as telecommunication and network fraud, with a full-chain crackdown and integrated prevention and control, and prosecuted 282,000 people for crimes such as fraud, gambling, and dissemination of obscene materials using the Internet, a year-on-year increase of 98.5%. Severely prosecuted online defamation, insults, infringement of citizens' personal information and other crimes that seriously endangered social order and violated citizens' rights, and prosecuted 3,436 people, a year-on-year increase of 51.3%.

Question 20: Do you have any other comments to make that may be relevant to your jurisdiction?

Answer:

Here are some more personal observations for your reference:

1. There are many laws and regulations in China in place for investigating, prosecuting and punishing cybercrime, including those against minors and committed by minors. However, the Criminal Law of the People's Republic of China is the primary substantive law that is directly effective on such acts, if they constitute a "crime". Such a crime is due to investigation by the police, prosecution by the procuratorate, as well as judgment and punishment by the court. Another substantive regulation is "Regulations of the People's Republic of China on Administrative Penalties for Public Security", which is against such harmful acts that are not severe enough to be punishable according to the Criminal Law. Such an act is due to penalties imposed solely and directly by the police.

2. In China, no case law exists. Any case decided by any court is not binding for any other courts. Therefore, in practice, cases are not referable in other courts. It does not exclude the fact that some cases made publicised by the Supreme People's Court can be read or studied by judges at lower level courts, even if these are not explicitly written in judgments and decisions. In fact, the Supreme People's Court regularly or irregularly publicises cases that it regards as important, with an implicit purpose of guiding local courts of all levels. Under such circumstances, there have been no systematically compiled cases, nor sufficient cases to reflect how laws and regulations have been applied.

3. To Chinese authorities, the most critical challenge is to deal with online fraud from both domestic and foreign perpetrators (but not so much sexual exploitation and human trafficking). In many cases, perpetrators, who stay in China or foreign countries and speak Chinese language, committed severe telecommunications fraud against people inside China. This has been the primary field on which international cooperation is focused. This could mean either online grooming and transborder human trafficking are not so prevalent, or they are not so emphasized. From author's personal experience, Chinese law, armed with serious punishments up to death penalty, whether scholars and rights groups hold positive or negative positions, nowadays has more deterrence on offences such as online grooming, human trafficking and even drug trafficking. I wonder whether there were hidden cases that were never found.

4. In addition, for cyber perpetrators, online fraud is safer and more profitable than other crimes, for example, human trafficking, drug trafficking, and robbery in real life, because fraud is not punishable by death penalty. On the other hand, perpetrators of other offences which bear death penalty, would not be successfully extradited to China due to potentiality of such a punishment. Is it possible that is the

reason why no such cases as perpetrators involving human trafficking were ever extradited to China through any international mechanisms?