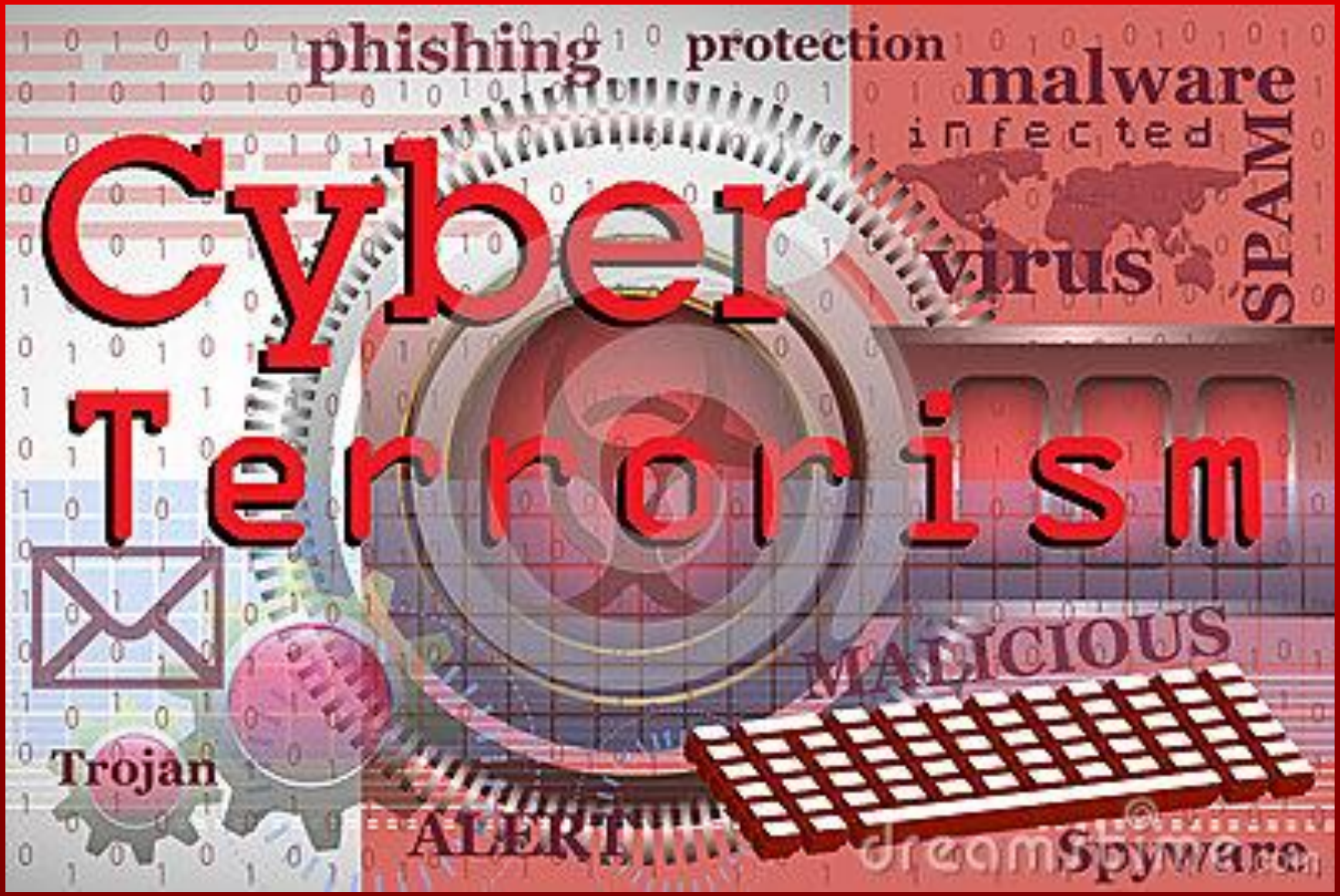
Present Situation of Cyber Terrorism in China and Its Legal Countermeasures

The People’s Republic of China The Interpretations of the Supreme People's Court

Li Ping, Senior Judge


phishing
protection
malware
infected
Cyber
virus
SPAM
Terrorism
MALICIOUS
Trojan
ALERT!!!
Spyware

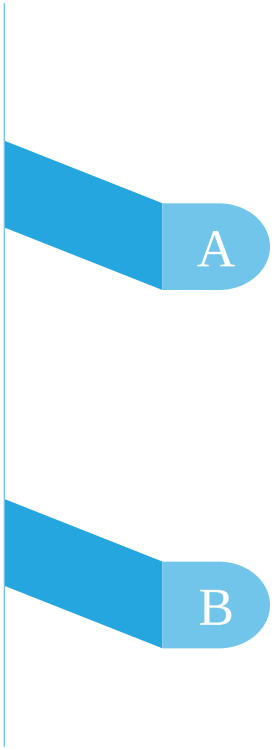
Present Situation of Cyber Terrorism in China

01 Having “seeds” overseas

02 Having “soil” in China

03 Having “marketplace” online

Forms of cyber terrorism in China



A Disseminating terrorism ideology using the Internet

B Imparting terrorist crime methods using the Internet

A. Disseminating terrorism ideology using the Internet

- Over the past few years, terrorists (mainly of overseas terrorists, such as the “ETIM”) have been publishing audios and videos on the Internet to advocate religious extremism and disseminated the same into China through multiple channels.
- Online terrorist audios and videos have become an important incentive to the frequent terrorist attacks in China at present.

Terrorist attack in Yunnan Kunming Railway Station

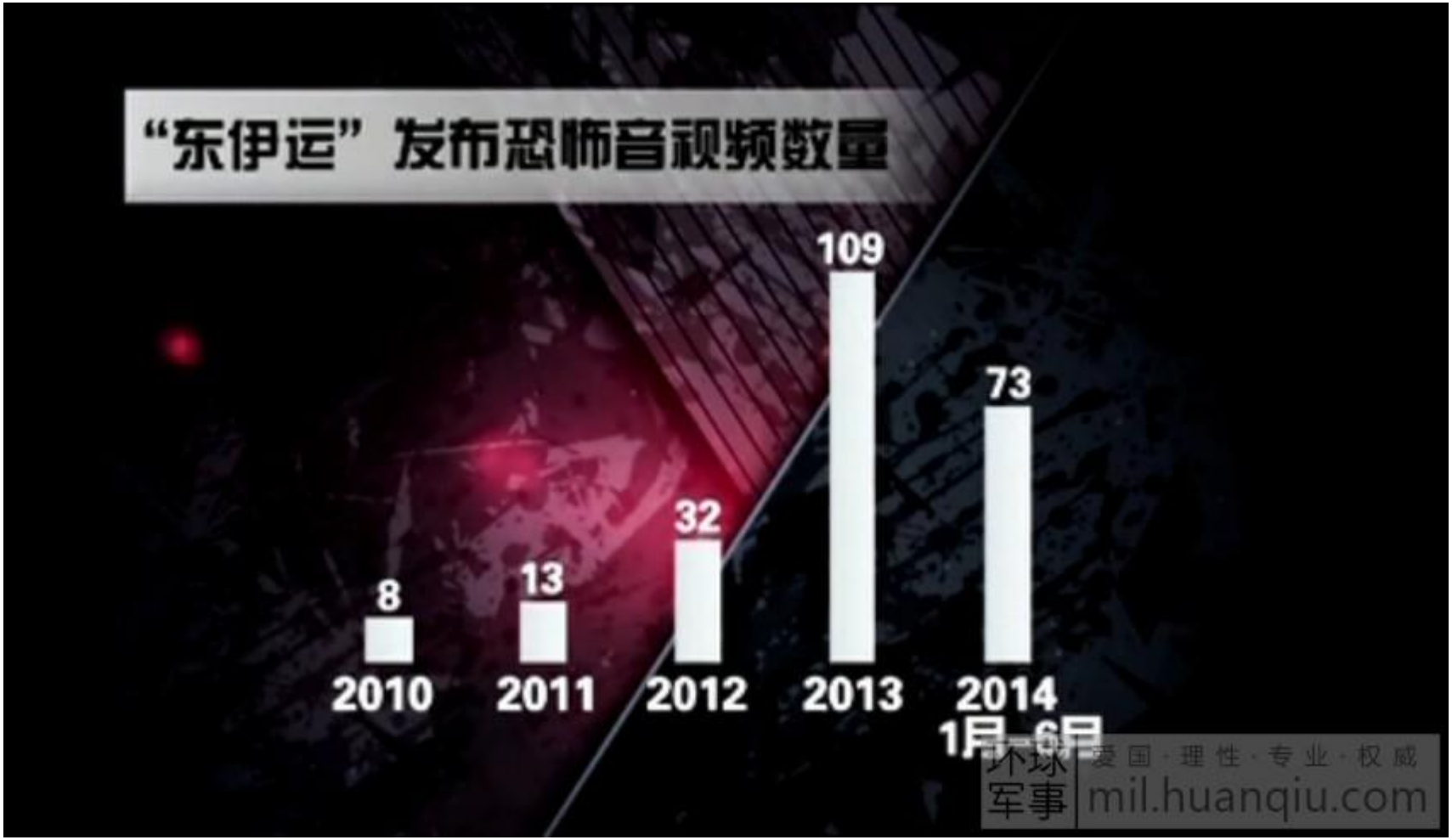
Terrorist attack in Urumqi South Railway Station

B. Imparting terrorist crime methods using the Internet

- Imparting crime skills
- Providing ways of initiating a terrorist attack
- Providing specific ways of making weapons

Training video released by the “ETIM”, even for children

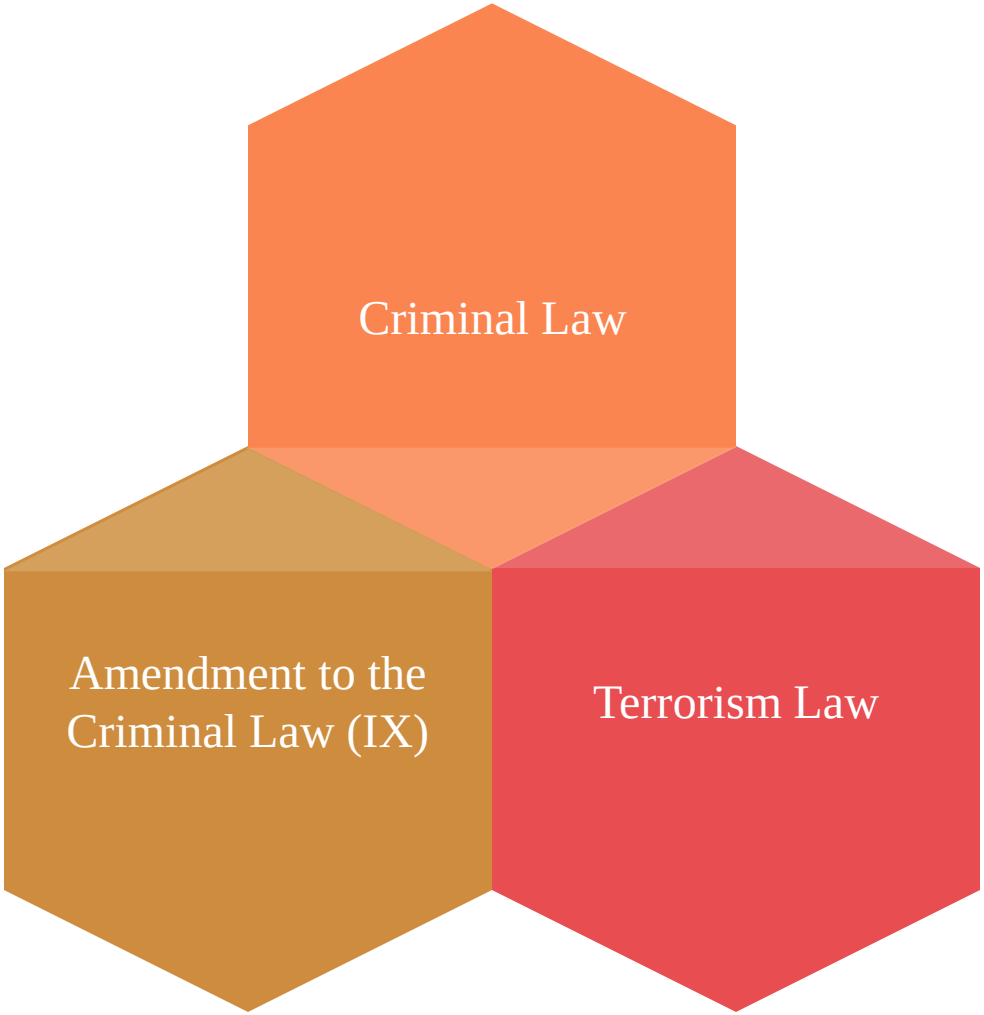
Quantity of audios and videos released by the “ETIM”



Damage by cyber terrorist attacks is not prominent at present.

- Informatization and Internetization of industries concerning livelihood was relatively late
- Enclosed management of computers and network systems of key areas
- Early attention to security management
- Criminals engaged in terrorist activities in China have not possessed the technology, competence, and conditions for launching cyber terrorist attacks

II. Legislation and Regulations of China on Cracking down on Cyber Terrorism



(I) Specifying Liabilities of Internet Service Providers

- The *Terrorism Law* prescribes the liabilities to be assumed by telecommunication operators and Internet service providers in cyber terrorism.
- Effective as of January 1, 2016

Provisions of the Terrorism Law

1. Telecommunication operators and Internet service providers must provide technical support and assistance for public security authorities and national security authorities. in preventing and investigating terrorist activities

2. Telecommunication operators and Internet service providers must implement supervision system of network security and information content and take security preventive measures, prevent dissemination of any information relating to terrorism and extremism, and stop transmission of the information mentioned-above, preserve relevant records, and delete relevant information, as well as report to public security authority or relevant authorities.

3. Telecommunication operators and Internet service providers must verify the identities of their customers and may not provide service for those whose identity is unknown or who refuses to identity verification.

4. Competent authorities of network security and informatization, telecommunication, public security, and national security must, within their respective terms of reference, order relevant entities to stop transmission and delete any information relating to terrorism and extremism or shut down relevant websites and suspend provision of relevant service.

(II) Cracking down on cyber terrorist activities conducted using the Internet

Criminal Law prescribes the crimes of:

- Activities of advocating terrorism and extremism and instigating terrorist activities, in order to punish those who propagate terrorism and extremism using the Internet;
- Activities of organizing, leading, and participate in terrorist organization, in order to punish those who provide contacts for terrorist activities and recruits and trains terrorists using the Internet;
- Activities of assisting in terrorist activities and crime of money laundering, in order to punish those who raise fund for and finance terrorist activities using the Internet.

(II) Cracking down on cyber terrorist activities conducted using the Internet

- The *Amendment to the Criminal Law (IX)*, effective as from November 1, 2015, beefed up the role of the criminal law in coping with cyber terrorism and extremism by amending crimes and introducing new crimes.

Crimes amended in the *Amendment to the Criminal Law (IX)*

Adding provisions on methods of assisting crimes of terrorist activities:

- Such as funding trainings on terrorist activities;
- Recruiting and transporting persons involved in the organization and implementation of terrorist activities.

New crimes added in the *Amendment to the Criminal Law (IX)*

- Newly added crime of illegally using information network
- Newly added crime of assisting in information network crime
- Newly added crime of preparing for theimplementation of terrorist activities
- Newly added crime of advocating terrorism and extremism and instigating terrorist activities

(III) Cracking down on cyber terrorist activities targeting the Internet

A

Crime of illegally intruding computer information system

B

Crime of illegally accessing to the data of computer information system and illegally controlling computer information system

Its legislative maturity exceeds the widely recognized international legislation and, in many aspects, approximates to the Cyber-Crime Convention of the European Council which sets forth even higher standards.

D

Crime of providing programs and tools for illegal intrusion and control of computer information system

C

Crime of damaging computer information system

III. Chinese judicial practice in cracking down on crimes of cyber terrorism

01

Equal emphasis on strengthening trial of cyber terrorist criminal cases and protecting human rights

02

Consolidating analysis, study, and judgment of various terrorist attacks to provide information support for cracking down on terrorist crimes

03

Strengthening anti-terrorism security and ensuring elimination of terrorist and extremist activities in buds

04

Strengthening network supervision and curbing the dissemination of terrorist and religious extremist ideologies via the Internet

(I) Equal emphasis on strengthening trial of cyber terrorist criminal cases and protecting human rights

- Strictly abide by provisions of the *Criminal Procedure Law*, put equal emphasis on punishing criminals according to laws and protecting human rights by laws, and fully protect the lawful rights and interests of the accused;
- Insist on the criminal policies of temper justice with mercy, under which the organizer, commander, and backbone members of crimes of terrorist activities and those committing serious crimes must be punished according to laws in a stringent way and those falling under circumstances in which lesser punishment, mitigated punishment, or exemption from punishment must be awarded lesser or mitigated punishment or exempted from punishment.

Trial of terrorist attack in Beijing on October 28, 2013

- Protect the rights of the accused to use their own language in the proceedings
- Tried by a court in Xinjiang where the terrorist attack was conceived

Trial of terrorist attack in Kunming on March 1, 2014

- The court provided the five accused with simultaneous interpretation in the session to fully protect their rights to use their own language in the proceedings.

(II) Consolidating analysis, study, and judgment of various kinds of terrorist attacks

- Further improved the informatization of dealing with terrorist cases, fully applied technical means such as big data and cloud computing, and unremittingly increased the timeliness and accuracy of information collection, analysis, and judgment.
- Facilitated improvement of real-time information sharing and consultation mechanism so as to detect any intended terrorist attack and deal with the same as early as possible.

Holding working meetings on terrorism, consolidating analysis, study, and judgment of various kinds of terrorist attacks

Northwest University of Political Science and Law established the School of Terrorism Law and held academic seminars on anti-terrorism

(III) Strengthening anti-terrorism security and ensuring elimination of terrorist and extremist activities in buds

- Important festivals and key places such as bars, restaurants, stadiums, malls, stations, and parks.
- Linked cameras, sensors, controllers, robots, and personnel in key areas together by communication means and formed a connection between people and tools and among tools to realize a informatized intelligent network controlled remotely to monitor populous premises in a real time. With these efforts, we have ensured the disruption of terrorist and extremist activities before they were launched and the elimination of them in buds.

(IV) Strengthening network supervision and curbing the dissemination of terrorist and religious extremist ideologies through the Internet

- Specifying liabilities and duties of telecommunication operators and Internet service providers
- Beefed up cooperation to block, intercept, and delete hazardous information and effectively curb the online dissemination of terrorist and religious extremist ideologies so as to purify the Internet environment.

THANK YOU