China and International Governance of Cybercrime

Prof. Dr. Shenkuo WU

Law Professor of CCLS, Beijing Normal University

Head of Research Centre of Internet Society of China

Consultant of Supreme Court of China

SHENKUO.WU@HOTMAIL.COM

1. Introduction
2. China and systematic preparation of domestic regulation
3. China and constant accumulation of best practice
4. China and active contribution for transnational cooperation
5. Conclusion

1. Introduction

more opportunities

a. new techinical supports: Big Data, AI, etc.

b. new operation models: Cloud computing, IoT, etc.

c. new business applications: eHealth, eLife, etc.

1. Introduction

more offences

a. new techinical offences: Virus, DDos etc.

b. new organizational offences: ICT fraud, etc.

c. new content offences: Child pornography, terrorist propaganda, etc.

2. China and systematic preparation of domestic regulation

2.1 Related national policies

a. 2015 "Internet Plus" Action Plan
b. 2015 "Made in China 2025" Plan
c. 2015 National Strategy for Big Data
d. 2016 13th Five-Year Plan for Informatization
e. 2016 National Cyberspace Security Strategy
f. 2017 International Strategy of Cooperation on Cyberspace
g. 2017 Plan for new generation of AI technologies

2. China and systematic preparation of domestic regulation

2.2 Related basic legislations

a. Cybersecurity Law 2017

b. E-commerce Law 2018 (estimated)

c. Personal Information Law (preparing)

d. Telecommunication Law (preparing)

e. Internet Service Law (preparing)

f. Criminal Law 2016/Civil Law 2017/Admin. Law 2018

China and International Governance of Cybercrime

Criminal Law of PRC

Article 253-1 Crime against personal information

Article 285 Illegal accesss, illegal obtaining, illegal control

Article 286 Damage to information system

Article 286-1 Refusing network security obligation

Article 287-1 Illegal using of information network

Article 287-2 Assistance for information crime

China and International Governance of Cybercrime

Criminal Law of PRC

Article 286-1

Any network service provider that fails to perform the information network security management obligation as prescribed in any law or administrative regulation and refuses to make corrections after being ordered by the regulatory authority to take correction measures shall be sentenced to imprisonment of not more than three years, criminal detention or surveillance in addition to a fine or be sentenced to a fine only under any of the following circumstances: (1) Causing the spread of a large amount of illegal information;

(2) Causing the leakage of users' information, with serious consequences;

(3) Causing the loss of criminal case evidence, with serious circumstances;

(4) Any other serious circumstance.

China and International Governance of Cybercrime

Criminal Law of PRC

Article 287-1

Whoever commits any of the following conducts by using the information network shall, if the circumstances are serious, be sentenced to imprisonment of not more than three years or criminal detention in addition to a fine or be sentenced to a fine only:

(1) Establishing a website or a communication group mainly for committing fraud, teaching on how to commit a crime, producing or selling any prohibited or controlled article, or committing any other illegal or criminal activity;

(2) Issuing any information on the production or sale of drugs, guns, obscene articles, or any other prohibited or controlled article or any other illegal or criminal conduct;

(3) Issuing any information for committing fraud or any other illegal or criminal activity.

China and International Governance of Cybercrime

Criminal Law of PRC

Article 287-2

Whoever, while obviously aware that any other person is committing a crime by using an information network, provides Internet access, server custody, network storage, communication transmission or any other technical support, or provides advertising, payment settlement or any other assistance for the crime shall, if the circumstances are serious, be sentenced to imprisonment of not more than three years or criminal detention in addition to a fine or be sentenced to a fine only.

2. China and systematic preparation of domestic regulation

2.3 Other related dispositions (1): Cyberspace Administration of China

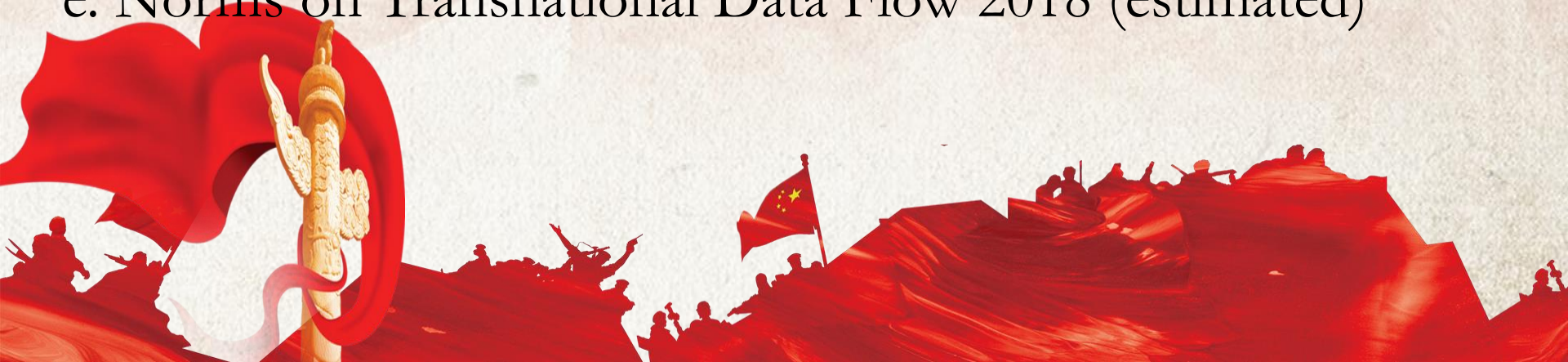
a. Dispositions on Instant Message 2014

b. Dispositions on Internet Broadcasting 2016

c. Norms on Cybersecurity Standardization 2016

d. Norms on Personal Information Security 2018

e. Norms on Transnational Data Flow 2018 (estimated)



2. China and systematic preparation of domestic regulation

2.3 Other related dispositions (2): Supreme Judicial Authorities

a. Interpretations on ICT Fraud 2017

b. Interpretations on Personal Information 2017

c. Interpretations on Fake Radio Station 2017

d. Interpretations on Cybercrimes 2018 (estimated)

2. China and systematic preparation of domestic regulation

Note:

a. Balance between security and development

b. Attention for technology, organization and content elements

c. Integration between principles and flexibility

3. China and constant accumulation of best practice

3.1 Public awareness

3.2 Talent formation

3.3 Public private partnership

3. China and constant accumulation of best practice

3.1 Public awareness

a. “Cybersecurity Week” initiative

b. “Cyberseurity in Campus” initiative

……

3. China and constant accumulation of best practice

3.2 Talent formation

a. 7 “Fisrt-class Cybersecurity Colleges” : Beijing, Xi'an, Wuhan, etc.

b. Cyberseurity&cybercrime course at schools

……

“Cybersecurity&cybercrime” course at BNU, China

“Cybersecurity&cybercrime” course at BNU, China

“Cybersecurity&cybercrime” course at BNU, China

3. China and constant accumulation of best practice

3.3 Public private partnership

a. Authorities

b. Private Entities

c. Research Institutions

3. China and constant accumulation of best practice

3.3 Public private partnership

a. Authorities

Preliminary research

Text preparation

Implementation evaluation

3. China and constant accumulation of best practice

3.3 Public private partnership

b. Private Entities

Promotion of Cybercrime awareness

Development of innovative instruments

Participation into emergency response

3. China and constant accumulation of best practice

3.3 Public private partnership

c. Research Institutions

Formation

Research

Consultation

Cooperation

3. China and constant accumulation of best practice

Note:

a. More public private investment

b. More participation of citizens

c. More risk managment oriented efforts

4. China and active contribution for transnational cooperation

International Strategy of Cooperation on Cyberspace (2017)

"5. International Cooperation on Cyber Terrorism and Cyber Crimes

i. Along with other countries, China will explore norms of behavior and concrete measures for international cooperation against cyber terrorism, including discussion on **an international convention** on combating cyber terrorism and consensus building on fighting cyber crimes and cyber terrorism, to provide the basis for law enforcement cooperation among countries."

4. China and active contribution for transnational cooperation

International Strategy of Cooperation on Cyberspace (2017)

"ii. China supports the UN Security Council to play an important part in international cooperation against cyber terrorism.

China supports and contributes to UN effort on fighting cyber crimes. China will participate in the work of the UN CCPCJ and UNGGE and promote discussion and formulation within the framework of the UN of **a global legal instrument**."

4. China and active contribution for transnational cooperation

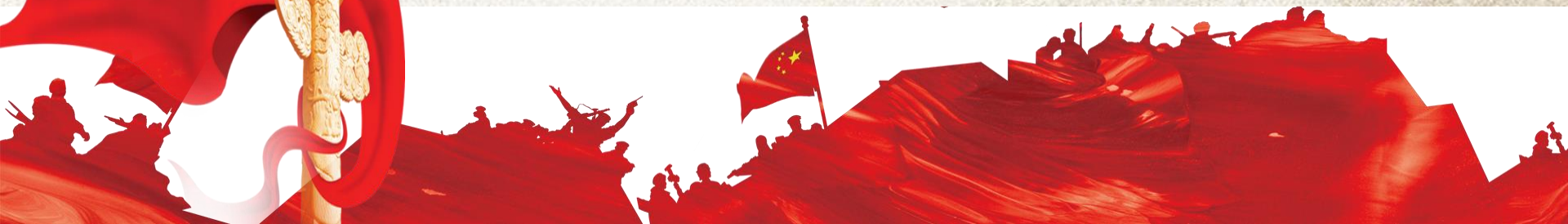
International Strategy of Cooperation on Cyberspace (2017)

"iii. China will enhance **regional cooperation** and pursue cooperation on ICT-enabled crimes within the framework of the Asia-Pacific meeting and coordination mechanism. China will take part in cooperation within regional organizations such as the ARF, and work on arrangement among BRICS countries on fighting cyber crimes and cyber terrorism."

4. China and active contribution for transnational cooperation

International Strategy of Cooperation on Cyberspace (2017)

"iv. China will step up **policy exchange and law enforcement cooperation** with other countries on cyber crimes and cyber terrorism. It will explore institutionalized dialogue and communication on cyber terrorism, establish **bilateral police cooperation mechanisms** with other countries, improve **judicial assistance mechanism** and promote **technology and experience sharing** on fighting cyber crimes."



4. China and active contribution for transnational cooperation

a. China & UN (*Cybercrime Experts Meeting*)

b. China & EU, ASEAN, Brics, etc - 31.05-01.06 4th EU China dialogue

c. China & USA, UK, Russia, etc - 01.06 China-USA-India dialogue

Key issues:

Information sharing, joint investigation, evidence supporting, etc.

5. Conclusion

Transparency, Openness and Participation

THANK YOU !

Prof. Dr. Shenkuo WU

Law Professor of CCLS, Beijing Normal University

Head of Research Centre of Internet Society of China

Consultant of Supreme Court of China

SHENKUO.WU@HOTMAIL.COM