Capacity Building for the Fight against Cybercrime :

A Case Study from China

Prof. Dr. Shenkuo WU

Beijing Normal University

shenkuo.wu@hotmail.com

Capacity Building for the Fight against Cybercrime :

A Case Study from China

I. Opportunities and Threats Related to new ICT Technologies

II. Elements of Capacity Building for Law Enforcement and Investigation

III. Capacity Building in China: A Case from Beijing Municipality

IV. Inspirations from the Chinese Practices for Capacity Building

I. Opportunities and Threats Related to new ICT Technologies

A. New Opportunities Related to new ICT Technologies

1. new techinical supports: big data, AI, etc.;
2. new operation models: cloud computing, IoT, etc.;
3. new business applications: eHealth, eLife, eFinance, etc.

B. New Threats Related to new ICT Technologies

1. new techinical offences: dark net, DDos attack, etc.;
2. new organizational offences: ICT fraud, etc.;
3. new content offences: child pornography, terrorist propaganda, etc.

II. Elements of Capacity Building for Law Enforcement and Investigation

1. Constant training of competent officials;
2. Effective technical supports;
3. All-round knowledge assistances;
4. Active public-private partnerships.

III. Capacity Building in China: A Case from Beijing Municipality

Initiatives within the People's Procuratorate of Beijing Municipality

1. Cyber Prosecutor Initiative;

2. Technical Committee Initiative;

3. Advisory Committee Initiative;

4. Procuratorate-Industry Anti-Cybercrime Initiative.

IV. Inspirations from the Chinese Practices for Capacity Building

1. Rights protection and due process are the logical starting point;
2. Constant technical supports are fundamental to overcome new challenges;
3. Updated legal insights are highly necessary to deal with cybercrime industry;
4. Public-private partnerships are effective for better cybercrime prosecution.