COMBATING CYBERCRIME: TOOLS AND CAPACITY BUILDING FO R EMERGING ECONOMIES

WSIS 2015, Geneva



Jinyong Chung May 25, 2015

Why combatting cybercrime matters to the World Bank

- Risk of "doing nothing"
- Fiduciary Obligation financier of essential communications and other critical infrastructure, services and applications in economic development projects; to ensure that our clients appropriately address cyber risks
- Convening power
- Status as an honest broker

The Bank provides millions of dollars in financing on projects across sectors (ICT/telecom infrastructure, transport, urban, energy, health, education, social protection, financial & markets) to ensure that critical infrastructure and systems and the data of government, business and citizen users that flow over those systems are protected.



Project Introduction

Donor Republic of Korea

Timing Effective Date – 1 July 2014 / Two Years

Mission To build capacity among policy-makers, legislators, public prosecutors & investigators, and civil society in developing countries

in the **policy**, **legal and criminal justice aspects** of the enabling environment to combat "cybercrime";

through synthesizing international best practice in these areas in a published tool that enables assessment of and best practice guidance with respect to the legal issues associated with combatting cybercrime; and field testing the tool in selected pilot countries.

It is expected that the tool will be made available as a global public good.



Project Partners







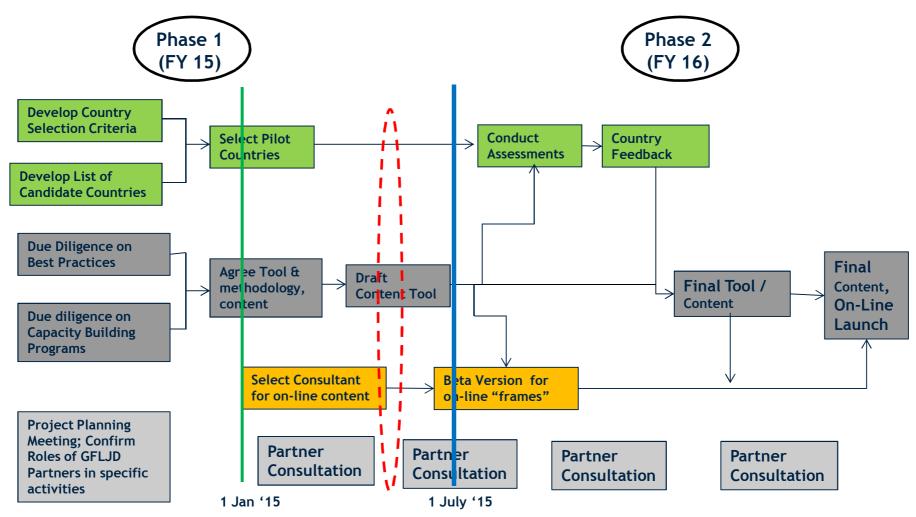








Project Progress



Current Status of Project

- Virtual library Established and growing
- Conducted mapping of partners' expertise & expected contributions
- Completed mapping of countries with cybercrime laws
- Conducting Comparative analysis of existing assessment tools
- Conducting Case Analysis
- Conducting Pilot Countries selection
- Toolkit drafting ongoing



Tool Kit

- Purpose
 - Initial self assessment tool for each countries
 - Platform for int'l cooperation for strategy establishment
- Method
 - Collaboration of each partners' expertise
 - Synthesize any existing guidelines by each partners with evaluation
 - Open to public to updates
- Process
 - By June 2015
 - Develop Basic Template (Key concepts Analyzing present status Best Practices – conclusion)
 - Kick off with certain fields and partners review
 - By Sep 2015
 - Develop each section of Tool Kits and put together for Draft Tool Kit
 - By June 2016
 - · Apply to Pilot countries and Finalize



Proposed Structure for Toolkit

Introductory Part	Best Practices Legal Enabling Environment*	International Instr u me nt s	National Legal Frameworks	Capacity Building	In-Country Assessment Tool	Analysis and conclusion
Purpose of toolkit	Working Definition of cybercrime	Multilateral & Regional cooperation & treaties Models Substantive Issues (crimes & safeguards) Procedural Issues Establishing international cooperation	Substantive law (crimes & safeguards)	Policies / defining key topics for legislation	Substantive law (crimes & safeguards)	Assessment of best practices, international instruments and national legislation
Phenomenon & Dimensions of cybercrime	Inventory of conduct that is criminalized		Procedural law	Capacity Building for Policy Makers / Legislators Training of law enforcement agencies, judges and prosecutors Education of consumers /end-users on cybersecurity—conscious behavior Ensuring cross-border cooperation	Procedural law	
Legal challenges of	Procedural Issues		Evidence/ Forensics Jurisdiction, inclu x-border cooperation Recent Cases (Interpreting Nat'l law)		Evidence/ Forensics Jurisdiction, inclu x-border cooperation Institutional Framework Capacity Building & Training	Assessment of best practices in capacity building
cybercrime	Evidentiary Issues Jurisdictional Issues					Lessons learned from in-country assessments
Capacity building challenges of	Institutional					
cybercrime	framework (regulation and law enforcement)					Way Forward
Recent Cases Dependencies	Recent developments and emerging trends (Cooperation with					
of Enabling Environment (Nat'l & Int'l) and Capacity Building	private sector and technical community, inclu resilience and security measures)			Cooperation with private sector and technical community, inclu resilience and security measures		



Case Analysis

- Purpose
 - Find out Regional & Industrial Vulnerability, Trends of cybercrime based on stages of victim countries' level of development
 - Provide Practical Map for policy making, int'l cooperation
- Methods
 - Based on Open Sources such as press releases, reports & media
 - In depth analysis of selected cases
- Current Status & Expectation
 - Cases Search 70 cases (growing)
 - Initial Analysis on types, origins & victim jurisdiction, damage estimate
- Challenges
 - Limited data
 - Govs' cooperation will be critical for in depth analysis



Thank you

Jinyong Chung jchung3@worldbank.org

