

COMBATING CYBERCRIME: TOOLS AND CAPACITY BUILDING FOR EMERGING ECONOMIES

Geneva 18 April 2016





David Satola

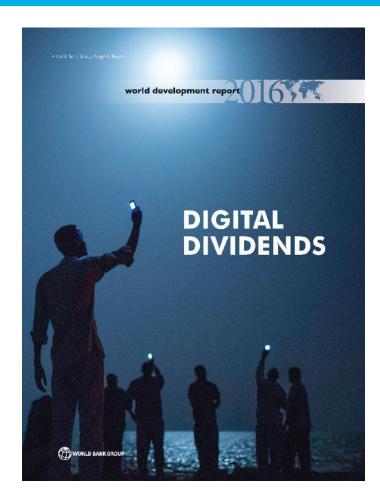
Why combatting cybercrime matters to the World Bank

- Demand for a single source of access to capacity building resources
- 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.



Now the Broader Context



Chapt 4 - Cybersecurity & Human Rights

Chapt 6 - Internet Governance

http://www.worldbank.org/en/publication/wdr2016



Project Introduction

3

- Donor Republic of Korea through the Korea World Bank Partnership Facility (KWPF)
- 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

Korea Supreme Prosecutors' Office

ITU

UN ODC

UN ICRI

UNCTAD

Council of Europe

International Association of Penal Law

Oxford Cyber Security Capacity Building Centre





Project Ethos

- Focus on "legal" (mix of policy, legal, criminal justice)
- Common Portal
 - No duplication
 - Synthesize
- Introduce new, cutting-edge issues
- Validate through field-testing



- Portal
 - Toolkit
 - Assessment
 - Library
- In-Country Assessment Pilots



New Emphasis on

Substantive Issues

- Safeguards with Privacy & Data
 Protection
- Intermediary Liability
- "Informal" Collaboration
 - NCFTA
 - Egmont Group
- Financial Sector
- Intellectual Property
- "New" crimes

Features

- Multistakeholder
- Case Study orientation
- Role of the Private Sector
- Maturity model / Self Assessment
- "Future Proofing"



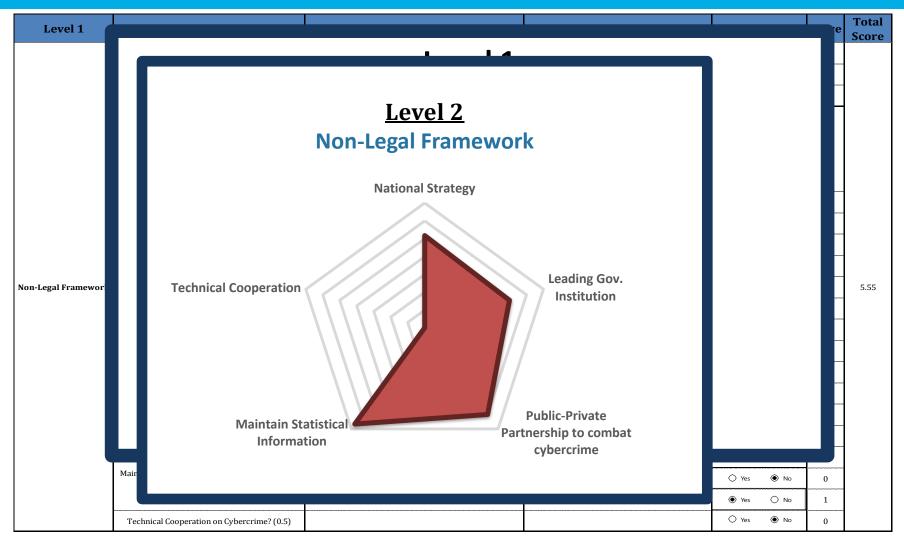
Toolkit Structure

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

* = inclu literature review



Assessment Tool







- Reference to understand Issues relevant to Cybercrime
- Guide to find commonly discussed Issues need to be considered in your home country
- Map to understand where your are & where you need to go
- "Self" assessment tool to check your country's progress



How to use this "Assessment Tool"?

Check

- Based on your best knowledge
- Work with Experts in each area

Discuss

- Clarify any uncertain issues
- Choose the most objective answer

Decide

- Relative strengths and weakness
- Prioritize allocation of resources





Thank you

David Satola

<u>dsatola@worldbank.org</u>

