DEPARTMENT OF JUSTICE

Office of Cybercrime

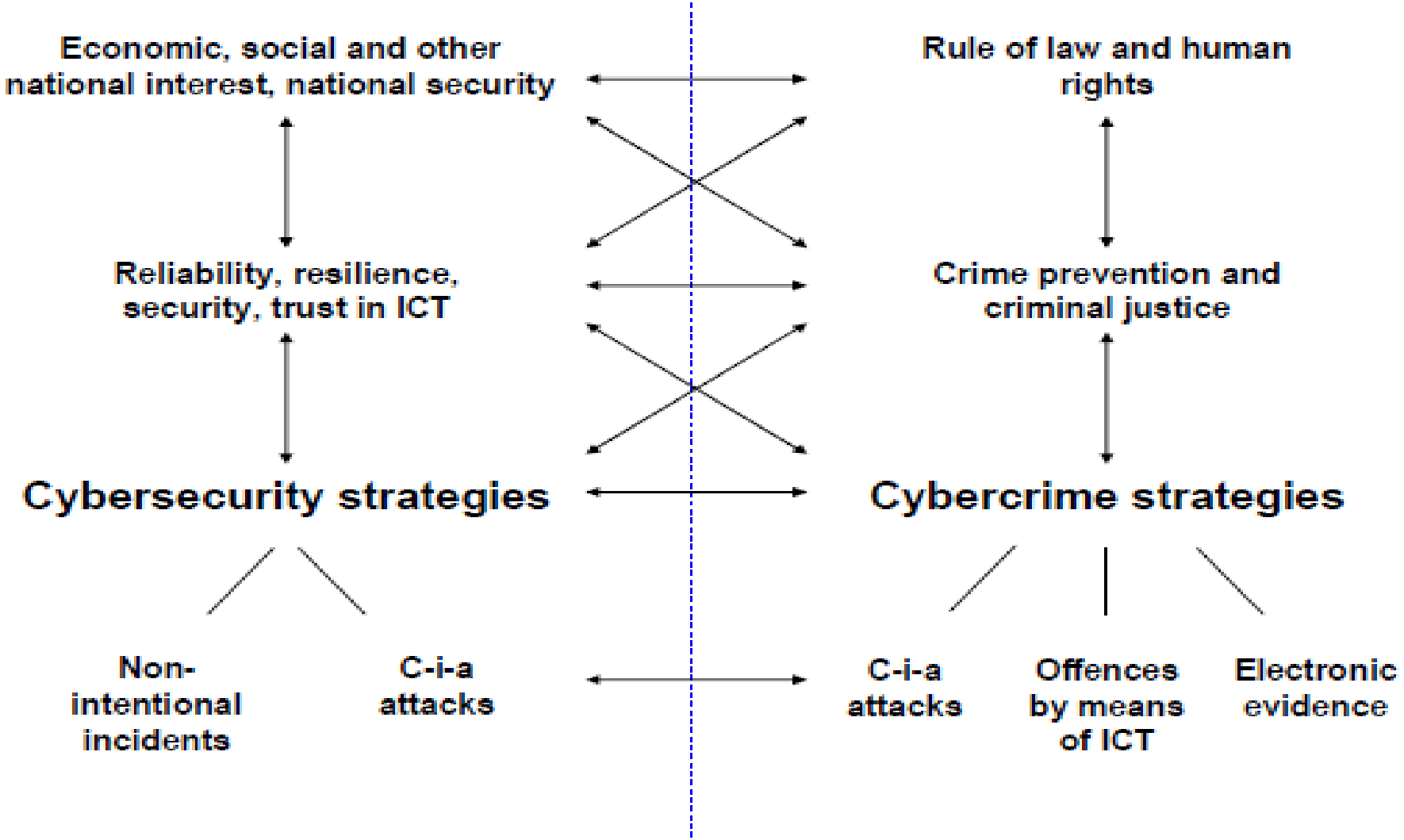
Peace and Order in Cyberspace: Status and Challenges

JED SHERWIN G. UY
OIC-Director
Office of Cybercrime
Department of Justice
Manila, Philippines

Outline

- Framework
- Cybercrime and Cybersecurity
- Challenges
- Developments

Cybersecurity vis-a-vis Cybercrime



- 1932 — Revised Penal Code
- 1965 — Anti-Wiretapping Law of 1965
- 1998 — Access Devices Regulation of 1998
- 2000 — E-Commerce Act of 2000
- 2000 — Rules on Electronic Evidence
- 2003 — Anti-Trafficking in Persons Act of 2003
- 2007 — Int'l Cybercrime Conference
  - Data Privacy
  - Cybercrime
  - Cybersecurity
- 2009 — Anti-Child Pornography Act of 2009
- 2009 — Anti-Photo and Video Voyeurism Act of 2009
- 2011 — Philippines was invited to accede to the Budapest Convention on Cybercrime
- 2012 — Cybercrime Prevention Act of 2012
- 2012 — Establishment of DOJ – Office of Cybercrime

Core Cybercrimes

Offenses against confidentiality, integrity and availability of computer data and systems

- Illegal Access
- Illegal Interception
- Data Interference
- System Interference

Computer-related Offenses

- Computer-related Identity Theft
- Computer-related Fraud
- Computer-related Forgery

Content-related Offenses

- Online Child Abuse/Child Pornography

Cyber Pillars

	Cybersecurity	*Cybercrime*	*Data Privacy*
Policy Legislation	***National Security and Cybersecurity Plans***	***Cybercrime Law*** ***Cybercrime Strategy***	***Data Privacy Law*** ***Rules and Regulations***
Primary Agencies	***Department of ICT***	***DOJ Office of Cybercrime***	***Data Privacy Commission***

Cybercrime Investigation and Coordinating Council (CICC)

- Established for policy coordination among concerned agencies

- Composed of:
  - DICT Secretary (Chair)
  - NBI Director (Vice Chair)
  - PNP Chief
  - DOJ – OOC Head
  - Representatives from the private sector

Law Enforcement Authorities

- NBI Cybercrime Division & PNP Anti-Cybercrime Group
  - Investigate all cybercrimes where computer systems are involved.
  - To conduct data recovery and forensic analysis on computer systems and other electronic evidence seized.

Department of Justice (DOJ) – Office of Cybercrime (OOC)

- Designated as the *Central Authority* in all matter relating to international mutual assistance and extradition for cybercrimes and cyber-related matters.

- To require the submission of timely and regular reports including pre-operation, post-operation and investigation results and such other documents from the PNP and NBI for monitoring and review
  - coordinate the investigation of cases and prevent or avoid conflict situations due to the nature of cybercrimes

Department of Justice (DOJ) – Office of Cybercrime (OOC)

- Designated as the *Operations Center (OpCen)* of the CICC
  - essential given the 24/7 requirement of running a cybercrime unit with crimes that are trans-border, beyond regular working hours and requires immediate responses
- Serves as the focal unit of the Philippines for cybercrimes
- Philippine Point-of-Contact (POC) for the National Center for Missing and Exploited Children (NCMEC)
- To issue and promulgate guidelines, advisories, and procedures, and prescribe forms and templates, in all matters related to cybercrime investigation

National Privacy Commission (Data Protection Authority)

- Special independent body tasked to implement/enforce the Data Privacy Act of 2012
- Has the power to adjudicate, award indemnity, issue cease and desist orders, compel actions affecting data privacy
- Provide assistance on matters relating to privacy or data protection at the request of a national or local agency, a private entity or any person;

Department of Information and Communications Technology

- Tasked to formulate the National Cybersecurity Plan
- Establish the National Computer Emergency Response Team (CERT)
- Facilitate cooperation on cybersecurity matters

Challenges

- Its borderless nature
- Encryption, cloud computing, high capacity RAM storage
- Not all law enforcers are trained with cyber incident response, cybercrime investigation, and handling electronic evidence
- Lack of information sharing and coordination between enforcement authorities
- Public awareness
- National Cybersecurity Plan and National Cybersecurity Incident Response Team yet to be established
- Lack of cooperation from ISPs and ICHs
- Insufficient funding

Plans and Programs

- Ratification of the Budapest Convention
- National Law Enforcement Coordinating Committee (NALECC) Sub-Committee on Cybercrime
  - Coordination between law enforcement authorities (NALECC-SOCY)
- Constitution of Prosecution Task Forces on Cybercrime
- Creation of Cybercrime Courts

Plans and Programs

- Establishment of National Cybersecurity Incident Response Team (NCSIRT)
- Continuous trainings for investigators, prosecutors, public attorneys, state counsels, and judges
  - Cybercrime Investigation Training: Focus on electronic evidence for investigators, prosecutors, state counsels, and public attorneys
  - First cybercrime responders – to capacitate traditional first responders
  - Basic and Advance Judicial Training on Cybercrime
  - Digital Forensics Investigation Course
- Implementation of the National Justice Information System (NJIS)
  - Establishment of the Victim Identification Program –to include NCMEC and ICSE

Plans and Programs

- Bachelor Degrees in Computer Science Major in Digital Forensics
- Drafting of special Rules on Cybercrime with the Supreme Court
- Drafting of the Guidelines on Cybercrime Investigation
- Establishment of the National Computer Forensics Training Program
- Establishment of additional computer forensic laboratories
- Strict enforcement of the law

LET`S WORK TOGETHER