UNIVERSITAS ISLAM INDONESIA, 28 NOVEMBER 2020

CYBER LAW AND THE COVID-19 PANDEMIC
International Students Colloquium on Law and Development in the Era of the Pandemic

DR. SONNY ZULHUDA
ASSOCIATE PROFESSOR
INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

UNIVERSITAS ISLAM INDONESIA, 28 NOVEMBER 2020
ONE
Reality Check on the Pandemic

TWO
Responses to a Health Concern

THREE
Understanding the Vulnerabilities

FOUR
Concerns and Strategies
MONTHS INTO THE PANDEMIC CRISIS

A Reality Check

1. Health Risks
   60 million infected; 1.4 million deaths in 214 countries & territories since December (WHO)

2. Lockdown
   Governments around the world impose lockdown, isolation or quarantine order

3. New Normal
   Work, Learn, Shop, Meet from Home

4. Lifestyle
   Physical distancing and its Ramifications

5. Vulnerabilities
   Social, Technical, Trusts, Governance Vulnerabilities

sonnyzulhuda.com
GLOBAL LOCKDOWN MEASURES PER APRIL 2020
RESPONSES TO THE PANDEMIC

Massive responses to the Pandemic had depleted the existing resources.

**Lockdown Deployment**
Governments deploy police and military forces for movement restriction, lockdown, surveillance, curfew, quarantine and border control.

**Public spending**
Massively required for medical treatment, public screening, medical research, public awareness, economic stimulus, forces deployment as well as other contingencies.

**Massive Campaign**
The effort requires active participation of all segments of public. Covid-19's threat is a bottom-up process, not a top-down one.
EMERGING RISKS

- Data exploitation through illicit requests of personal data for online services, Apps, etc;
- Fraud and scam via fake accounts begging for donation, fake charities, etc.
- Misinformation: Rise of citizen news portals with unaccountable stories – a test-bed for phishing attacks.
- Unsecured online platforms prone to personal data breaches (online shopping, online meeting, social media, etc).
- Rise of private surveillance
Critical system and infrastructures are at stake as they become a hot pot for both security and public health management system.

Technical Vulnerabilities

We witness how malicious minds potentially used this Covid-19 crisis as a window to exploit our vulnerabilities.

Weber for Cyber Criminals?

The concept of national critical infrastructure need to be relooked so as to accommodate this threat to national and public health as one critical security objectives.

Critical Infrastructure Protection
VULNERABILITIES OF THE INFORMATION SOCIETY

A Window for Cybercriminals?

People tend to collect information about the Pandemic, click on links and web pages, spreading the information with poor exercise of fact-checking.

People work on official documents using home-based computers, not subject to a security protection and support as they have in office.

Apps for social networking, e-shopping, e-meeting, e-learning and cloud services are mushrooming and widely used, but may not adequately equipped with rigorous security and privacy measures or policies.

Information-thirsty Society

Working from home.

Use of 3rd party Apps
Cybersecurity cases rise by 82.5% 

Sunday, 12 Apr 2020

By YUEN MEIKENG

MORE people are online now – be it for business, education, entertainment, socialising or working from home due to the movement control order (MCO).

But the higher usage of technology also means bigger risks of running into cyberthreats.

About 352 accounts on the video conferencing app Zoom were compromised on Wednesday, including a healthcare provider in the US and seven educational institutions.

There has yet to be any report on hacked Zoom accounts from Malaysia.
Terrorists and cybercriminals are always interested to exploit cyberspace vulnerabilities. The activity of cyber terrorism does not relax during Covid-19. Several cyber attacks do target a critical information infrastructure (CII), a traditional target for cyber terrorism.
ACTIVATE OUR CYBERLAWS

**LAW AGAINST COMPUTER MISUSE**
Criminal laws against illegal intrusion, Unauthorised modification, computer sabotage, interception, etc.

**LAW AGAINST CYBER FRAUD**
Online fraud, impersonation, social media hijacking, identity theft, online payment scam, etc.

**PERSONAL DATA PROTECTION LAW**
Laws to protect online privacy, personal data misuse, unauthorised data collection, breach of data security, etc.

**E-COMMERCE LAW**
Laws to protect online contract, electronic transaction, online payment methods, e-commerce consumer protection, mediation, etc.

**CYBER SECURITY LAW**
Laws to protect and encourage encryption, data security breach notification, data due diligence, cyber-terrorism law, etc.
WHERE TO START?

Understanding the vulnerabilities, Taking right actions

- Strengthen the Leadership & Governance
- Enhance social awareness
- “Distributed Security”
- Public-private Partnership
THANK YOU

FEEDBACK:

sonny@iium.edu.my
http://sonnyzulhuda.com