# ROLE OF LAW & CHALLENGES IN GOVERNING DIGITAL ENVIRONMENT

**Dr. Hartini Saripan**
**Senior Lecturer**
**Faculty of Law**
**Universiti Teknologi MARA**

# CONTENTS

- Concept of cybercrime
- Governing digital world – theory of governance
- Role of law
- Development of cyberlaws in Malaysia
- Challenges in governing digital environment
- The way forward

# GOVERNING DIGITAL WORLD

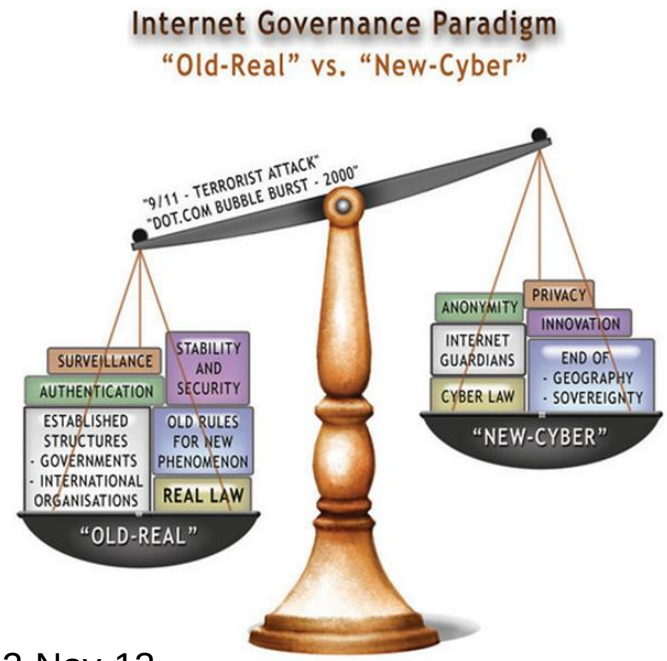
- Can the Internet be governed?
- How to govern?
- Who should govern?

# NEW FORM OF GOVERNANCE?

- A broad view of global governance as result of the processes of globalization
- Globalization has changed the traditional approach to security, which is associated with the shift from government to governance

# ROLE OF LAW

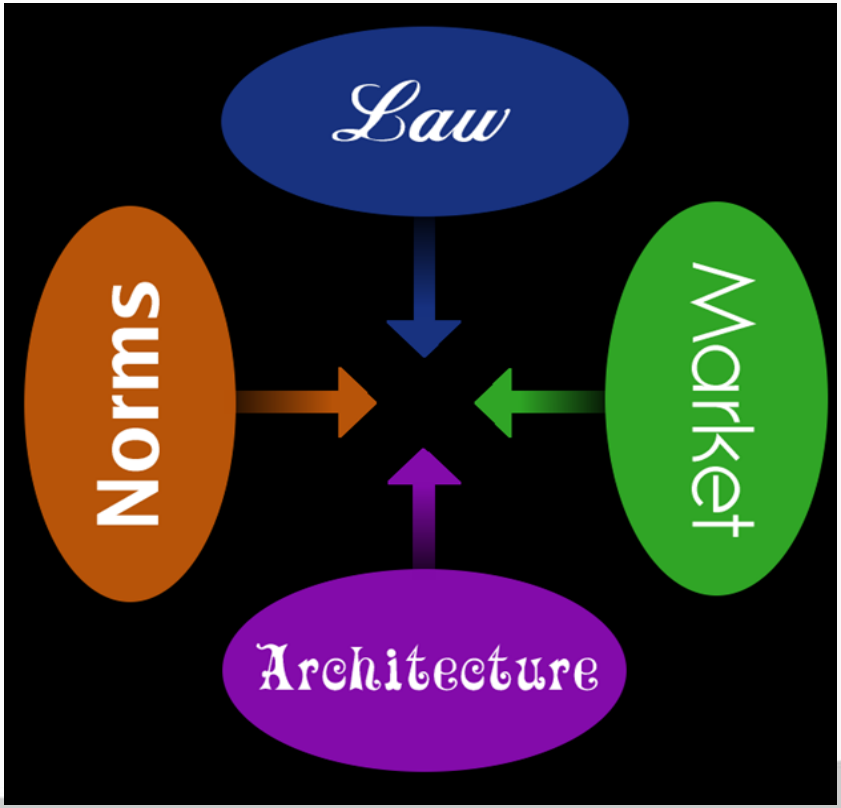
- cyber-libertarianism approach
- cyber-realism/cyber-paternalism approach




# MODALITIES OF REGULATION

- 4 ‘modalities of regulation’

1) Laws
2) Markets
3) Architecture
4)Social Norms



# LESSIG'S MODALITIES OF REGULATION

- 4 modalities control the activities of individuals
- Each modality functions as a constraint on the choices of actions that individuals have

1) Law constrains through the threat of punishment
2) Market constrains through price and price-related signals
3) Architecture constrains through physical devises
4) Social norms constrains though the application of societal sanctions

# CYBERLAWS IN MALAYSIA

- Computer Crimes Act 1997 (CCA)
- Digital Signature Act 1997 (DSA)
- Copyright (Amendment) Act 1997
- Telemedicine Act 1997
- Communications and Multimedia Act 1998 (CMA)
- Malaysian Communications and Multimedia Commission Act 1998
- Electronic Commerce Act 2006
- Electronic Government Activities Act 2007
- Personal Data Protection Act 2010

# APPLICATION OF CYBERLAWS

- An analysis shows minimal application of cyberlaws
- Most application involves the CCA, the CMA and the Copyright (Amendment) Act 1997
- Other cyberlaws have not been tested in courts

# COMPUTER CRIMES ACT 1997

- Governs limited aspects of cybercrimes
- Focusing on:
  - -hacking
  - -unauthorized access offence
  - -unauthorized modification offence
  - -wrongful communications
  - -attempts and preparation

# DIGITAL SIGNATURE ACT 1997

- Aimed at making provisions for, and regulating the use of a digital signature technology
- Modelled after the Utah Digital Signature Act 1995
- Adopts a prescriptive approach
- Designates 3 primary players – subscriber, recipient and certification authority

# PERSONAL DATA PROTECTION ACT 2010

- Sets out rules in processing personal data for commercial purposes
- Applies to a data user:

-established in Malaysia and processes data

-processing is done by any person employed or engaged by the data established in Malaysia

-not established in Malaysia but uses equipment to process (must designate a representative in Malaysia)

# PERSONAL DATA PROTECTION ACT 2010

- Exemption:
  - Federal and State governments
  -Credit reporting business
  -Personal, family, household affairs, recreational (total exemption)
  -Some processing activities such as crime, taxation, mental and physical health (partial exemption)
- Observed seven data protection principles

# EVIDENCE (AMENDMENT) (NO 2) ACT 2012

- Presumption of fact in publication
- Aimed at addressing the issue of Internet anonymity
- Not presumption of law
- Rebuttable presumption

# EVIDENCE (AMENDMENT) (NO 2) ACT 2012

- 3 presumptions:

1) If your name, photograph or pseudonym appears on any publication, representing yourself as the publisher, you are presumed to have published such contents unless contrary is proved
2) If a posting originates from your account with a network provider, you are deemed to be the publisher unless contrary is proved
3) If a publication is traced to a computer either owned by or over which you have a custody and control, you will be deemed to be the publisher unless contrary is proved

# CHALLENGES

- Minimal application of cyberlaws
- Non-enforceable statute
- Outdated approach of law
- Multiple investigation procedures

# CHALLENGES

- Admissibility and authenticity of digital evidence
- Jurisdictional disparities
- Mistrust of computer forensic experts
- Legal knowledge of enforcement officer

# CHALLENGES

- Knowledge of judges and practitioners
- Integrity of Internet service provider – cloud computing
- Invasion of privacy
- Prescriptive approach of the law
- Under-reporting

# THE WAY FORWARD

- International initiatives
- Cyber court
- Legislative approach
- Consolidation of law
- Specific law on cyber security
- Advancement of technical and legal knowledge
- Cooperation between investigators and prosecutors
- Horizontal mode of governance
- Self-regulation

# CONCLUSION

- Can the legal framework alone provide a safe and secure digital environment?
- How to establish trust?
- Bridging the gap between the industry and academia
- Continuous research and education on cyber security

# THANK YOU

**Dr. Hartini Saripan**
**Senior Lecturer**
**Faculty of Law**
**Universiti Teknologi MARA**
**012-3945232**
**hartinisaripan@salam.uitm.edu.my**
**hartinisaripan@gmail.com**