

財團法人台灣網路資訊中心因公出國人員報告書 108年8月20日

報告人姓名	黃勝雄	服務單位及職稱	執行長
出國期間	108/8/12-16	出國地點	Seoul, South Korea
出國事由	參加 Asia Pacific Internet Governance		
報告書內容包含： 一、 出國目的 二、 會議行程 三、 考察、訪問心得			
授權聲明欄	本出國報告書同意貴中心有權重製發行供相關研發目的之公開利用。  授權人： 黃勝雄  (簽章)		

附註二、請於授權聲明欄簽章，授權本中心重製發行公開利用。  
 附一、請以「A4」大小紙張，橫式編排。出國人員有數人者，依會議類別或考察項目，彙整提出報告。

一、出國目的：

參加 Asia Pacific Internet Governance 。

二、會議行程：

詳如會議網站

<https://www.icann.org/news/announcement-2-2019-05-14-en> 。

三、考察、訪問心得：

應 ICANN 之邀擔任講師，其講議如附為該項報告內容。

# Cybersecurity Governance and Coordination in Taiwan

Kenny Huang, Ph.D. 黄勝雄博士

CEO & Board Director,

Taiwan Network Information Center

Taiwan Computer Emergency Response Team/Coordination Center

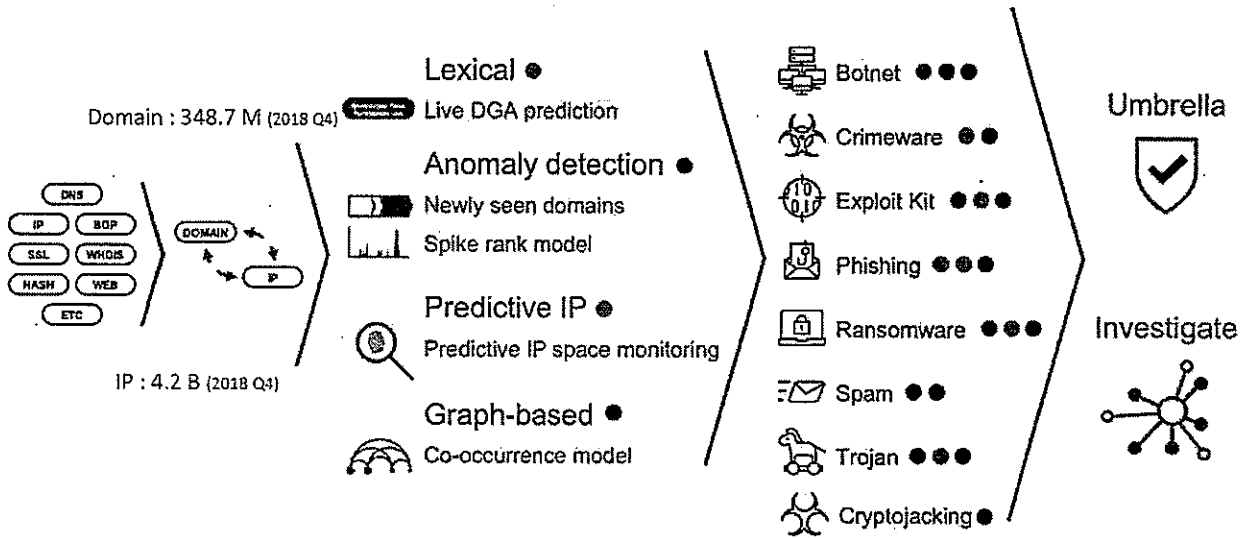
huangk@twnic.tw

2019 Aug 14

## Attributes of abusive domains

- Malware
- Botnets
- Phishing
- Piracy
- Trademark
- Copyright infringement
- Fraudulent
- Engaging in activity contrary to applicable law

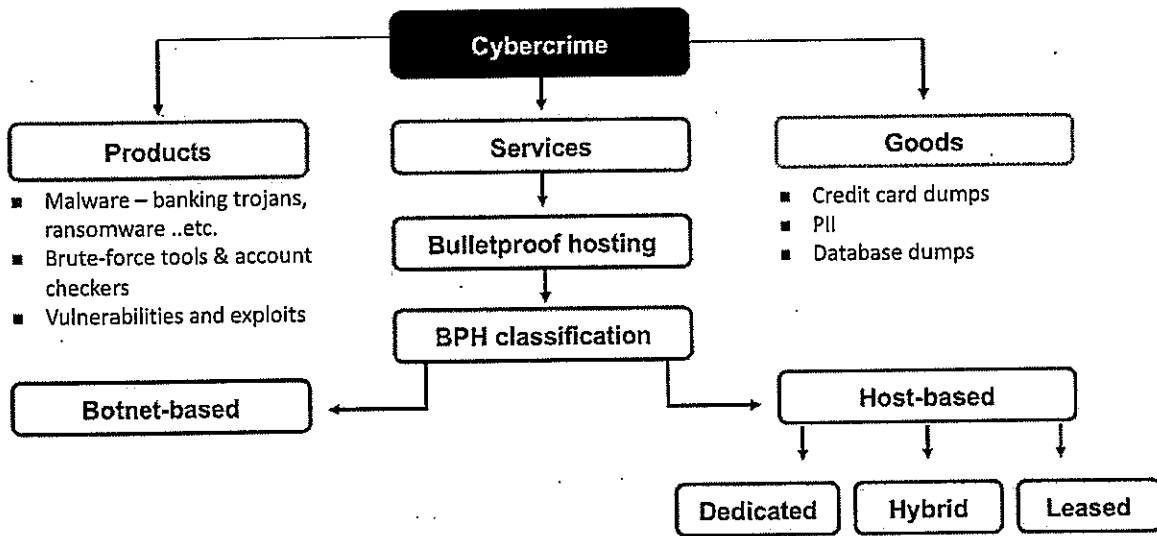
# Threats detection at scale



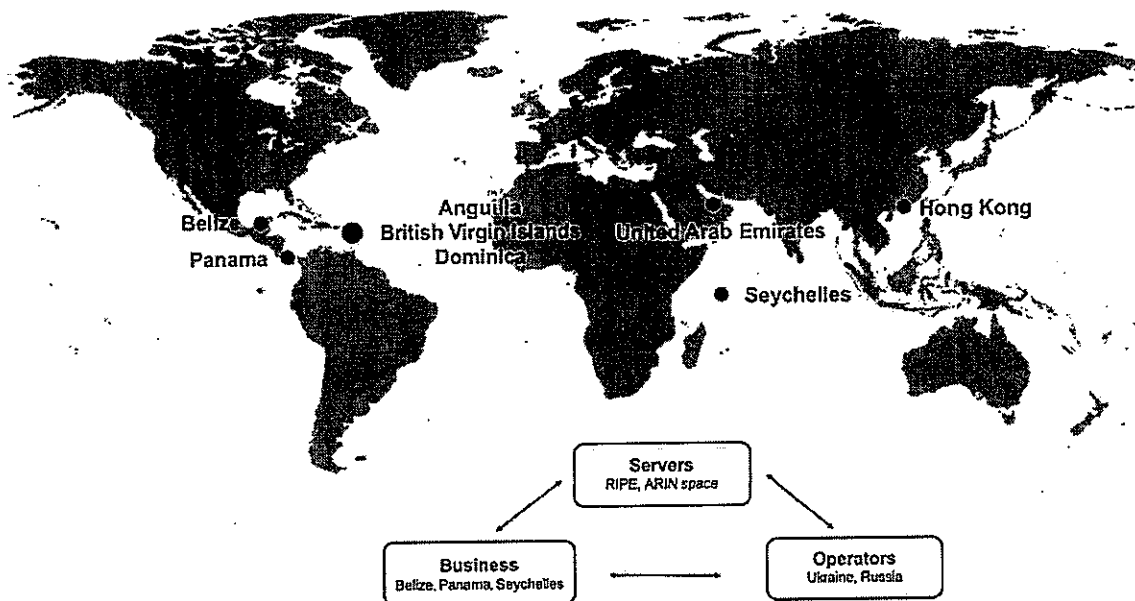
# Internet resources vs. cybercrime attacks

IP space	Domain space
<p><b>Rogue outgoing traffic</b></p> <ul style="list-style-type: none"> <li>■ SSH/WordPress brute-force attack</li> <li>■ Mass scans</li> <li>■ DDoS attacks</li> <li>■ Spam sending</li> </ul>	<p><b>Toxic hosted content</b></p> <ul style="list-style-type: none"> <li>■ Phishing</li> <li>■ Malware C&amp;C</li> <li>■ Ransomware C&amp;C</li> <li>■ Cybercrime forums</li> <li>■ Stolen credentials marketplaces</li> <li>■ Criminal jabber servers</li> </ul>

## Cybercrime ecosystem and services



## Business registration & multiple layers of resistance



## DNS cybersecurity measures for large scale DUM

### ■ Confidentiality

- ◆ Prevention of unauthorized disclosure of information
- ◆ Risk measure: extremely low
  - Personal data protection act (Taiwan)
  - GDPR compliance
  - Reported personal data infringement : 0

### ■ Integrity

- ◆ Prevention of unauthorized modification of information
- ◆ Risk measure : extremely low
  - DNSSEC (.tw signed in root zone)
  - Reported data breach : 0

### ■ Availability

- ◆ Prevention of unauthorized withholding of information or resources
- ◆ Risk measure: extremely low
  - ICANN-ccTLD service level commitments
  - Reported service outage : 0

## Cyberspace expansion discussion

### ■ Propositional fallacy for cyberspace expansion

- ◆ Increase the size of .tw domains will increase the threats from invaders

### ■ Value of cyberspace (.tw) expansion

- ◆ Law, policies (e.g., TWDRP) and governance framework validation
- ◆ DNS capabilities and capacity validation
- ◆ Cyber resilience capabilities and capacity validation
- ◆ expanding Taiwan cyberspace coverage and cyber jurisdiction

### ■ Cyber jurisdiction

- ◆ The .tw domain is an intrinsic part of the identity of many Taiwanese businesses and organizations operating on the internet. Consumers visiting .tw sites know they are protected under Taiwan consumer laws.
- ◆ .tw 受我國司法管轄權保障，任何.tw 域名之網路犯罪行為可依循我國相關法律並屬於有效之刑法效力範圍

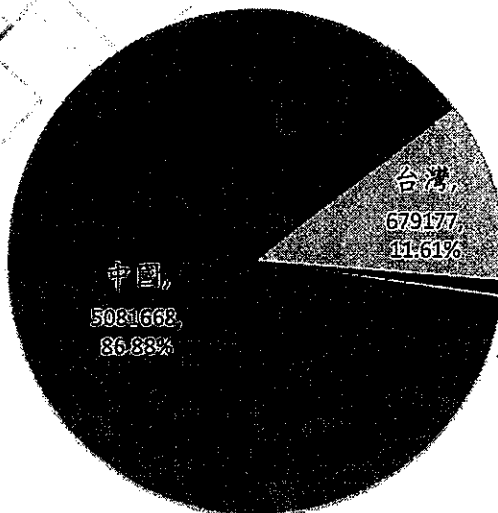
# MANILA PRINCIPLES

## ON INTERMEDIARY LIABILITY

- 1 Intermediaries should be shielded from liability for third-party content
- 2 Content must not be required to be restricted without an order by a judicial authority
- 3 Requests for restrictions of content must be clear, be unambiguous, and follow due process
- 4 Laws and content restriction orders and practices must comply with the tests of necessity and proportionality
- 5 Laws and content restriction policies and practices must respect due process
- 6 Transparency and accountability must be built into laws and content restriction policies and practices

## .tw registrant distribution

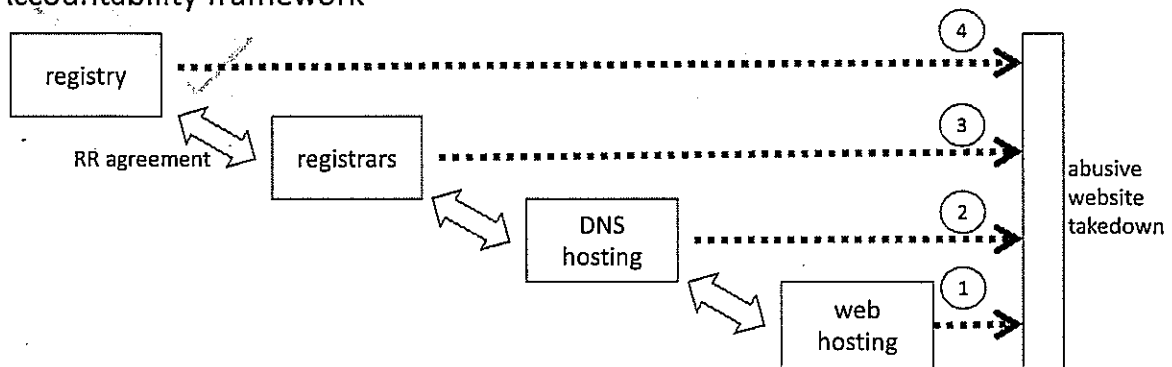
4M domains from CN will be expired by the end of Oct 2019. The renewal ratio will be teeny based on business forecast.



Source: TWNIC Stat 2019.03.20

## Business strategy

- Diversified IDN
  - ◆ Japanese, Korean, Thai ..
- Diversified international registrars
  - ◆ US, Japan, Korea, Malaysia, Thai, UK, France ..etc.
- Accountability framework



## Registry-Registrar agreement

- TWNIC includes a provision in its registry-registrar agreement that requires registrars to include in their registration agreements a provision prohibiting registered name holders from distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, engaging in activity contrary to applicable law, and providing consequences for such activities including suspension of the domain name.

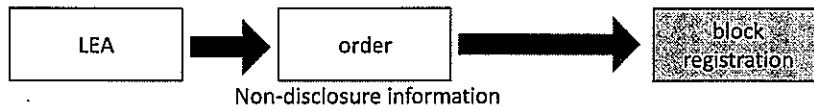


# Registrars abusive report 2018 Oct 01-2019 Mar 31

registrar					
reported abusive domains	0	0	0	0	0
registrar					
reported abusive domains	0	0	1	0	0
registrar					
reported abusive domains	0	0	0	0	0

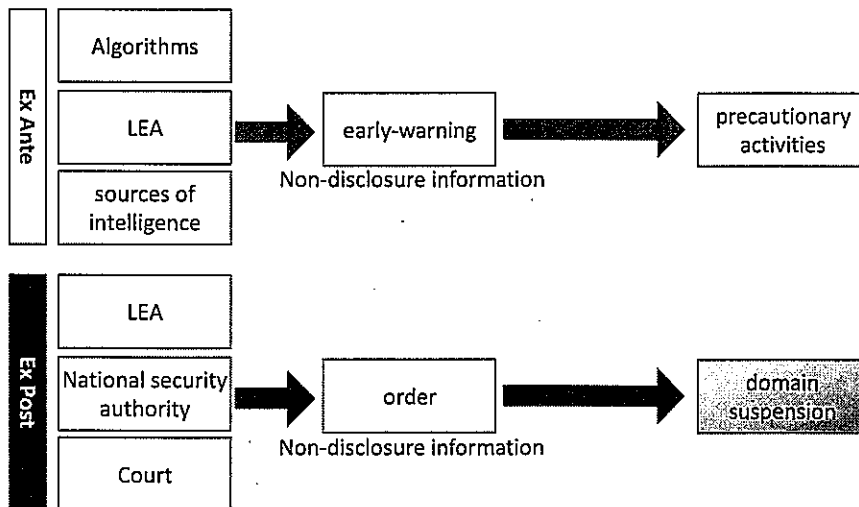
Edited by Dr. Kenny Huang, 2019.04.27

## Pre-registration



Non-disclosure information

## Post-registration



Non-disclosure information

	Key risk	Likelihood	Consequence	Risk indicator	Details	Actions
1	Brute-force attack	Very Unlikely	Moderate		attacker submit many passwords with the hope of eventually guessing correctly	Coordination
2	DDoS	Very Unlikely	Major		a malicious attempt to disrupt normal traffic to a web property	Coordination
3	Spam	Likely	Minor		unsolicited messages sent in bulk by email	Coordination
4	Phishing	Likely	Moderate		attempts to trick targets into sensitive/ valuable information	Coordination
5	C&C servers	Very Unlikely	Major		computer controlled by cybercrime and issues commands to a botnet	Coordination
6	Unlawful content (NTL security)	Likely	Major		online content violates national security laws and regulations	Order & suspension
7	Unlawful content (others)	Likely	Moderate		online content violates laws and regulations	Order & suspension
8	Cybercrime marketplaces	Unlikely	Major		online marketplaces where cybercrime trade goods or information	Order & suspension

## Internet policy development reference frameworks

	non-enforceable policy	Enforceable norms recognized within international law
Global public goods	X	
International spaces and shared resources		X
Critical infrastructure protection		X

characteristics	ICANN	ITU	IGF	APNIC	TWNIC	IETF	NATO
multistakeholder	X		X	X	X		
bottom-up model of governance	X		X	X		X	
standard setting	X	X		X	X	X	
operates based on contractual compliance	X			X	X		
governmental		X					X
sets internationally enforceable obligations for states		X					X

## Other referenced areas of international law

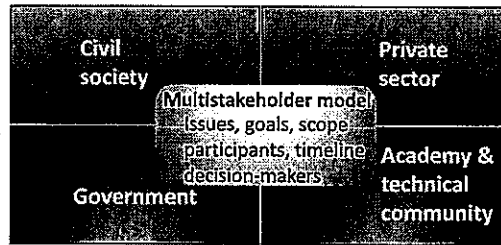
<p>Areas of international law that can be used for reference with regard to protecting the core of the Internet include:</p>	law of the sea
	air law
	space law
	international human rights law
	international telecommunication law
	law of treaties
	international trade law
	antiterrorist laws and policies

## Public Goods Governance Models

		Governance Capability & Capacity for Public Goods		
Non-state Actors	X	O	O	
Governments	O	O	X	
Governance Model	State Regulation  (Neoliberalism)	Cooperation <small>(Knill, 2002)</small>	Private Self Regulation	
		Co-Regulation <small>(Tanja Borzel, 2007)</small>		
		Delegation <small>(Tanja, Borzel, 2007)</small>		
				<small>(Knill, 2002)</small>

Dr. Kenny Huang

## 多方利害關係人模式



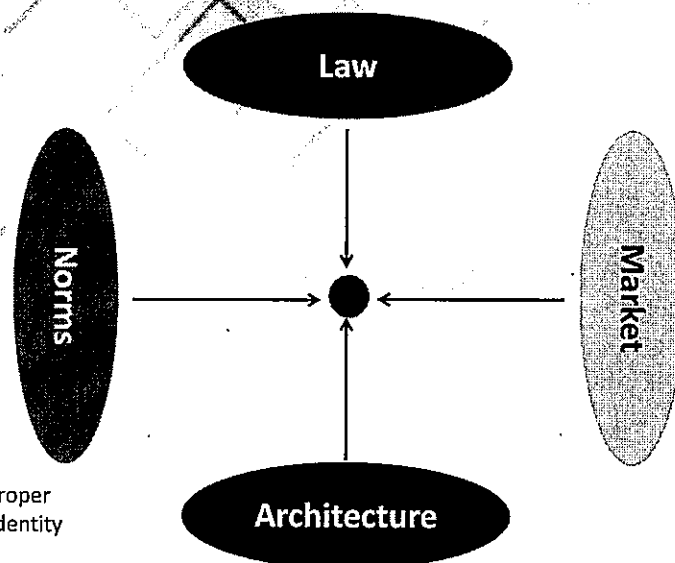
Source: IEEE Internet Computing, Jan 2015

### Internet Governance (WSIS 2005)

The development and application by governments, the private sector and civil society, in their respective roles, of *shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet.*

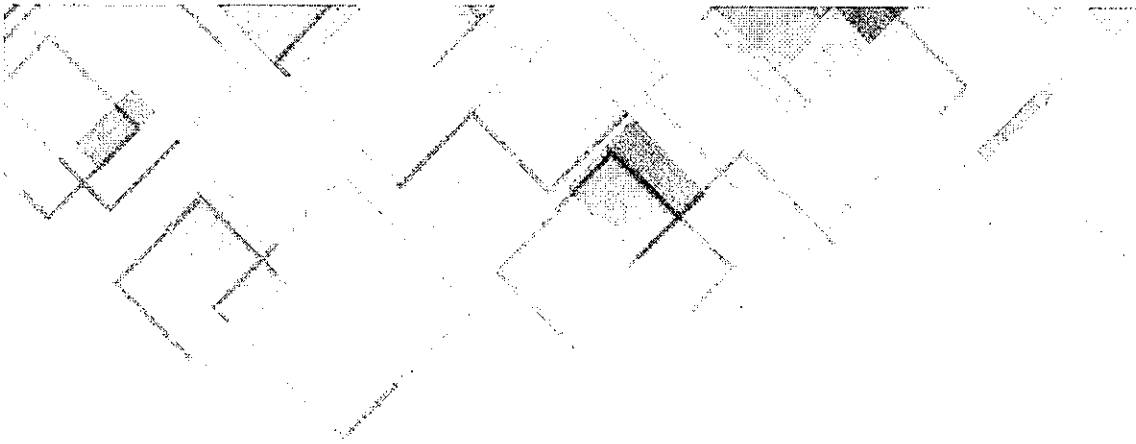
多方利害關係人依據各自共識原則、規範、管理辦法、決策程序來塑造 Internet 的使用與演化。

## Pathetic dot theory (New Chicago School theory)



Cyber Norms:  
Collective expectations for the proper behavior of actors with a given identity  
Source: Katzenstein, 1996

Source: Lawrence Lessig, 1999; illustrated by Dr. Kenny Huang



**thank you**