Cyber Jurisdiction Review

Kenny Huang, Ph.D. 黃勝雄博士

CEO , Taiwan Network Information Center

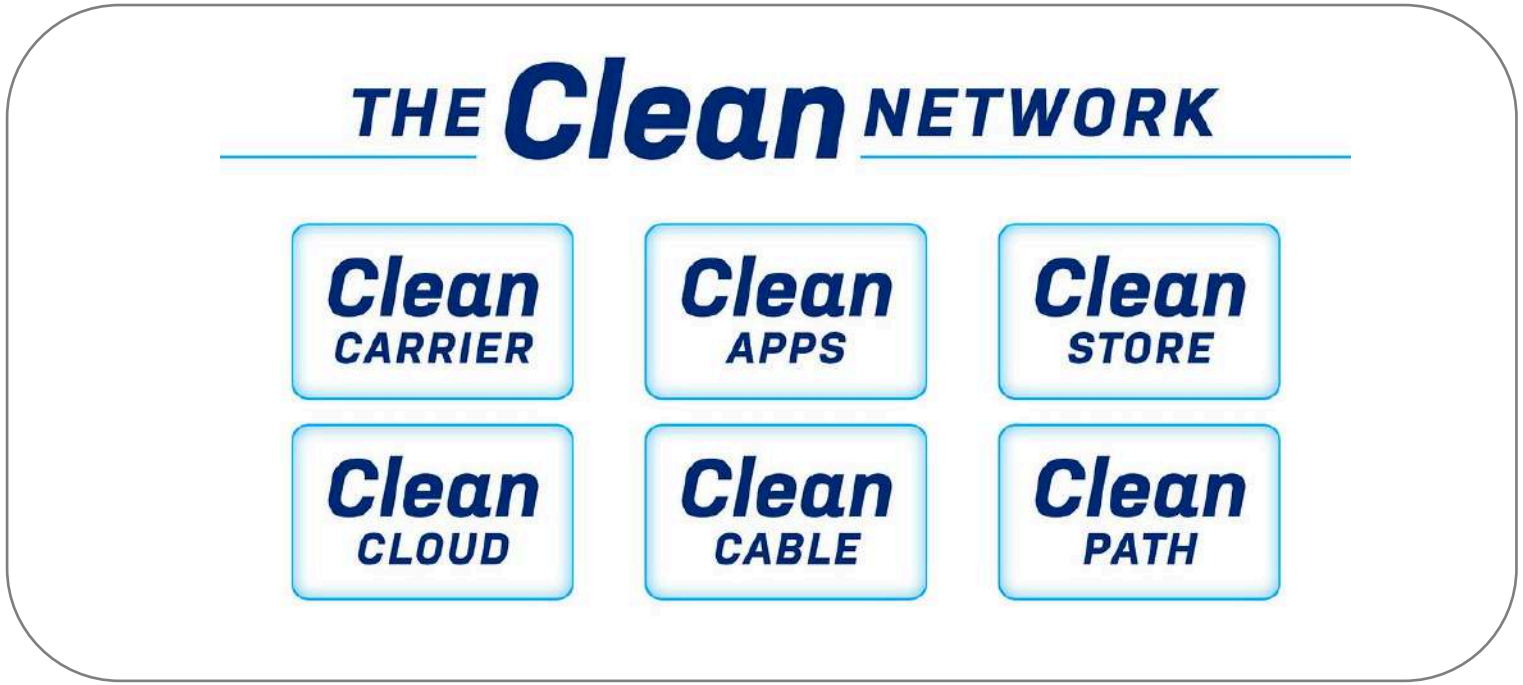
Taiwan Computer Emergency Response Team/Coordination Center

huangk@twnic.tw

Oct 2020

US

Clean Network Policy



China

New IP Proposal

INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2017-2020

TSAG-C83

TSAG

Original: English

Question(s): N/A

Geneva, 23-27 September 2019

CONTRIBUTION

Source: Huawei Technologies Co. Ltd. (China), China Mobile Communications Corporation, China Unicom, Ministry of Industry and Information Technology (MIIT)

Title: "New IP, Shaping Future Network": Propose to initiate the discussion of strategy transformation for ITU-T

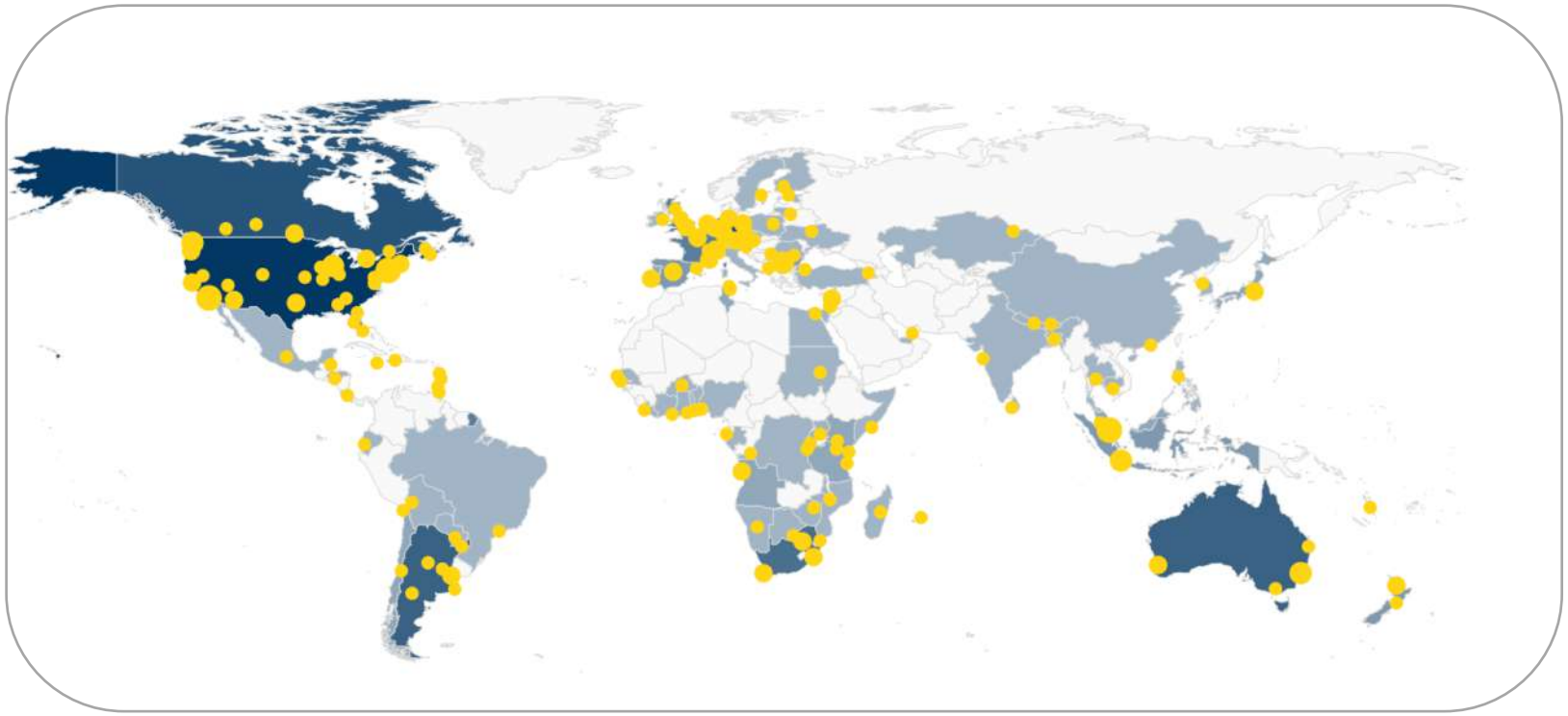
China New IP proposal

OSI Model	TCP/IP Model	DII Model
Application	Application	Third Party Application
Presentation		
Session		Resource Management
Transport	Transport	
Network	Internet	Blockchain
Data Link	Network Access	
Physical		Physical

OSI Model	Current Primary Organisations	DII Primary Organisations	DII Model
Application	Industry, W3C	W3C, ITU	Third Party Application
Presentation	IETF, W3C		
Session	IETF, W3C	ITU	Resource Management
Transport	IETF, ETSI		
Network	IETF, IANA, ETSI		Blockchain
Data Link	3GPP, IEEE, ETSI, ITU		
Physical	3GPP, ITU ETSI, GSMA	3GPP, ITU	Physical

Cyber jurisdiction : .TW

OR



Cybercrime : multiple layers of resistance

Servers
IP addresses from ARIN or RIPE or APNIC

Business
registered at Panama or other countries

Operators
operated from China or other countries

.. invasive attacks on a much regular basis, but IP address unknown

IP address and jurisdiction

IP address

(Physical location)

→

Cyber attribution

(Determining the actor responsible for a cyberattack)

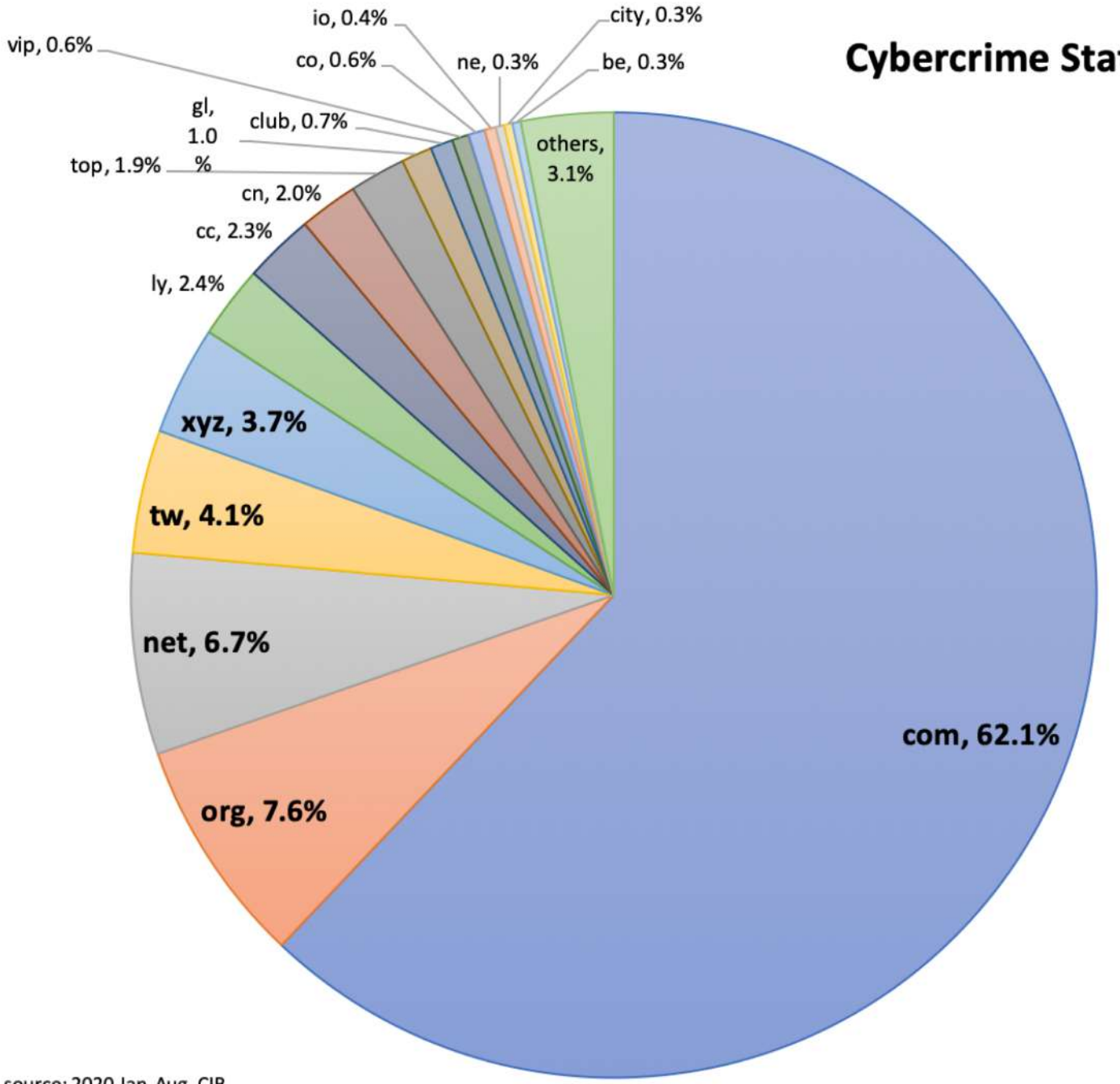
Jurisdiction

(By Court)

→

No Jurisdiction,
No authority,
No Law enforcement

Cybercrime Statistics



source: 2020 Jan-Aug, CIB

95.9% cases

UNSOLVED

Legal solutions of cyber jurisdiction

- **MLAT** (Mutual Legal Assistance Treaties)
- **Budapest Convention** (Convention on Cybercrime)
  - *Slow and complex*
  - *Not scalable to all countries*
- **Legal Cooperation**
  - *Lacks transparency*
  - *Depends on private network of law enforcement agencies*
  - *Questions around admissibility of evidence*
  - *Conflicts of laws*

域外效力：限制網路內容接取

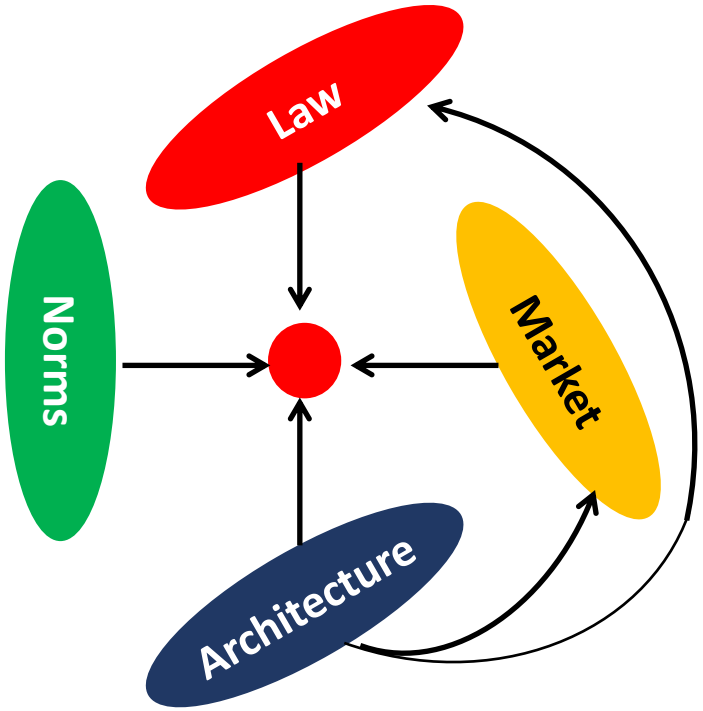
- 法律依據：現有具限制網路內容接取之法律
  - 兒少法46條 (衛福部)
  - 動物傳染病管制條例38-3條 (農委會)
- 限制接取、瀏覽及移除不當網路內容範例
  - 網路違法內容經目的事業主管機關公告者，網路平台提供者、應用服務提供者、電信業者應限制內容接取、瀏覽或移除相關網路內容
- 依行政程序法執行域名沒入處份
  - 沒入處份應以域名註冊人為相對人，以書面送達或其他適當方法使其知悉才能發生效力。
  - 提供沒入處份網頁讓社會大眾與註冊人知悉法律依據及原因。

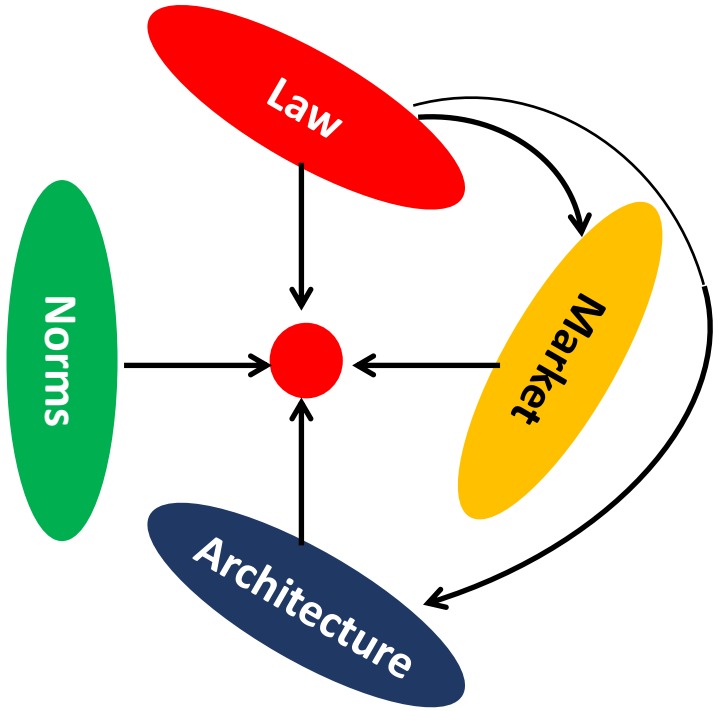
How is cyberspace regulated

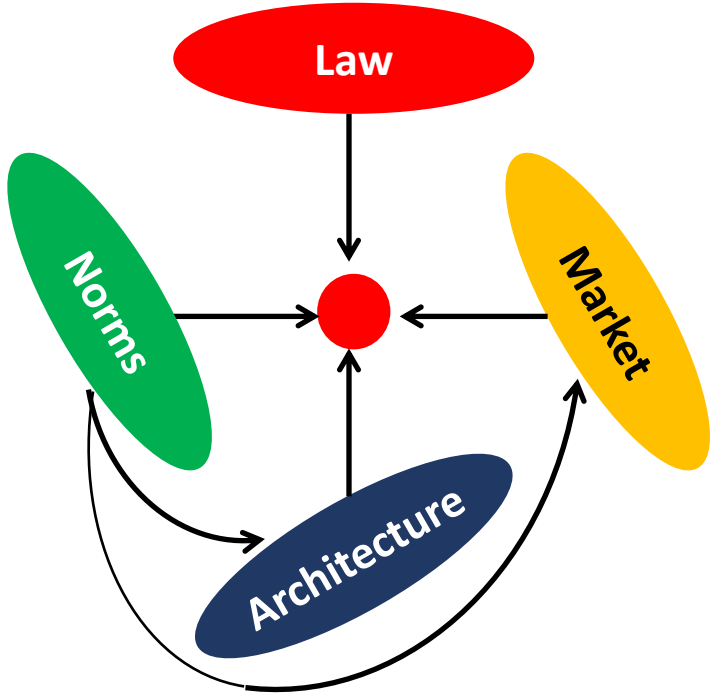
Code is Law

Law is Code

Cyber Norms







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

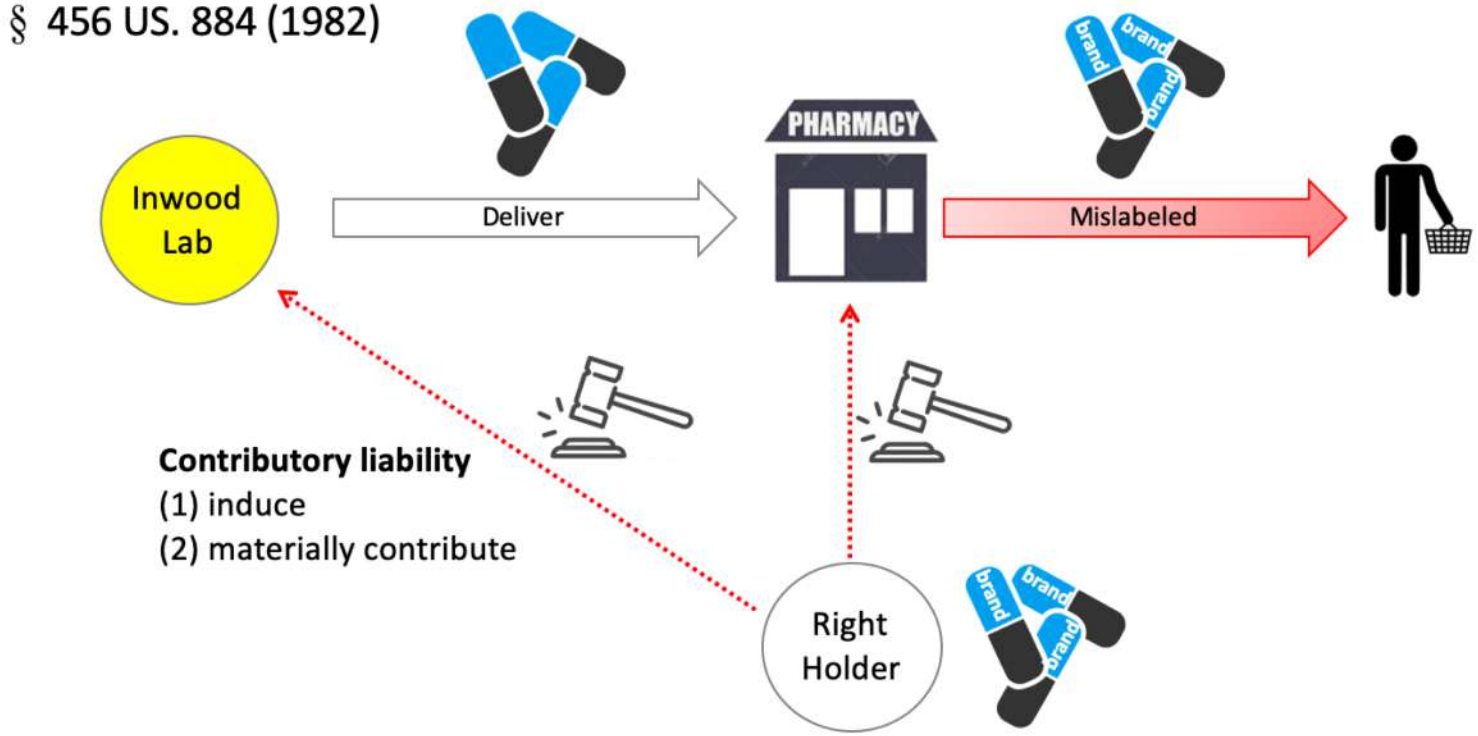
From intermediary liability to intermediary responsibility

MANILA PRINCIPLES ON INTERMEDIARY LIABILITY

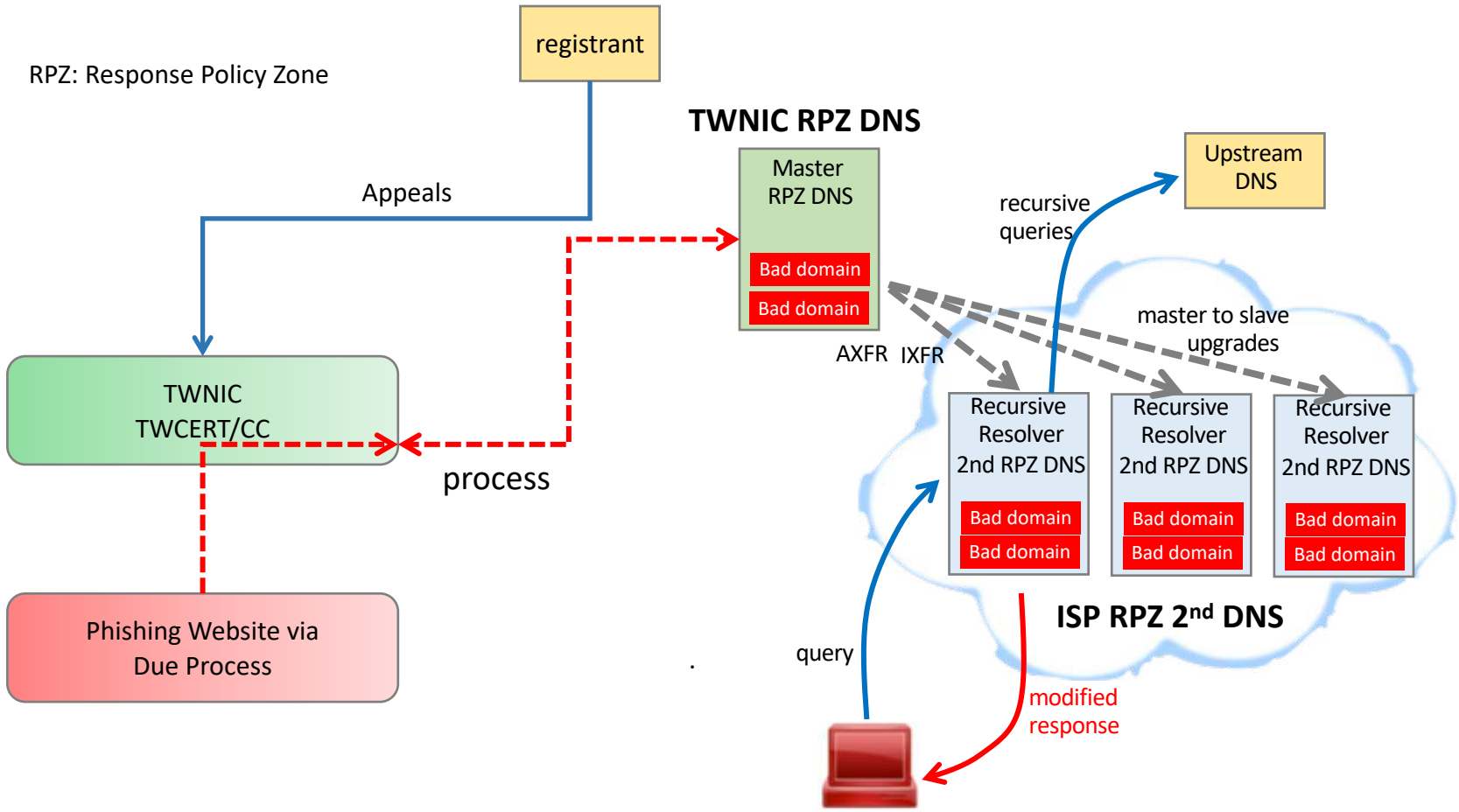
1. 中間人應免於對第三方內容承擔責任
2. 沒有司法機關命令，不得要求對內容進行限制
3. 內容限制請求必須清晰、明確，且依照正當程序
4. 法律、內容限制命令，和實務做法必須通過必要性和比例原則的檢驗
5. 法律、內容限制政策，和實務做法必須遵循正當程序
6. 透明度和問責機制必須建立在法律、內容限制政策和實務做法中

→ **Inwood Principles**

§ 456 US. 884 (1982)



DNS RPZ architecture



RPZ service scenarios

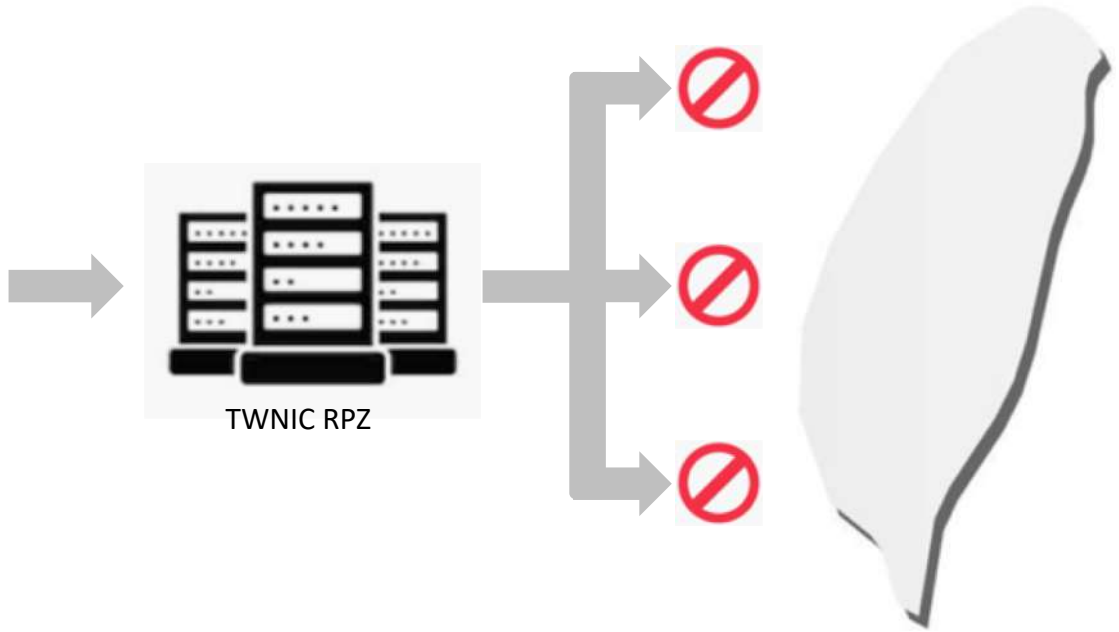
Court Order
(法院命令)

Injunction
(禁制令)

Executive Order
(行政命令)

Cyber Norm
Dispute Resolution Mechanism
(網路自律爭議治理機制)

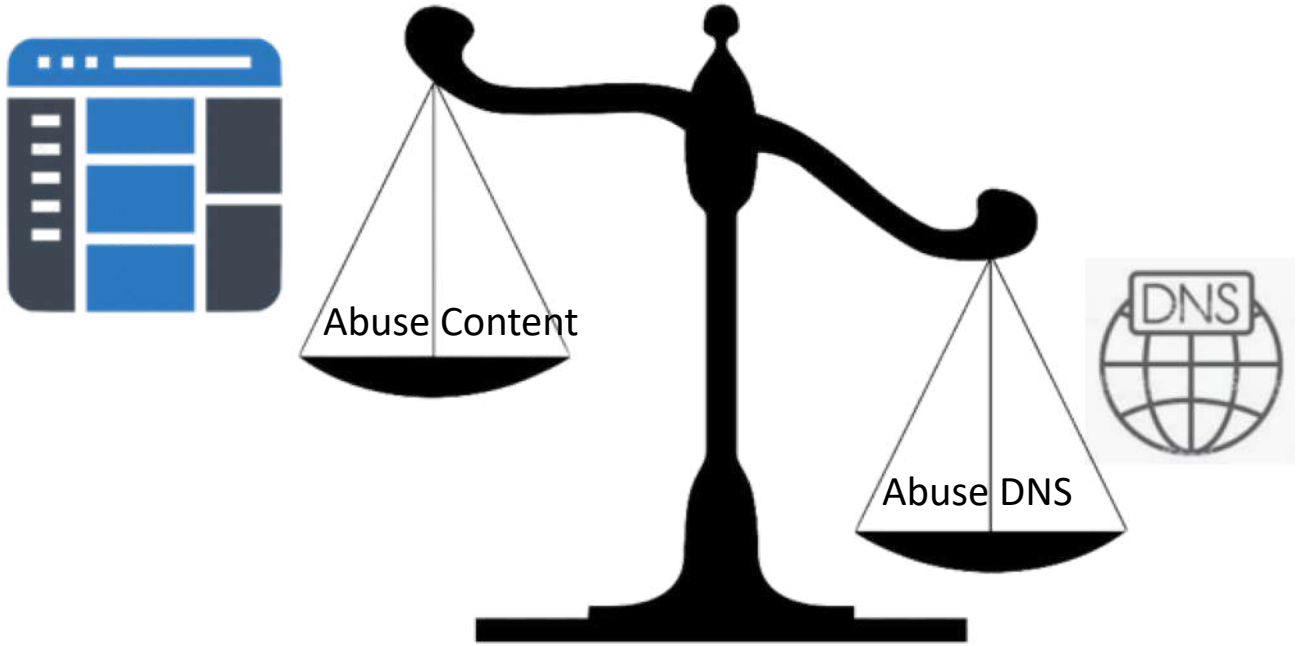
Threat Intelligence Suppliers
(資安威脅情資)

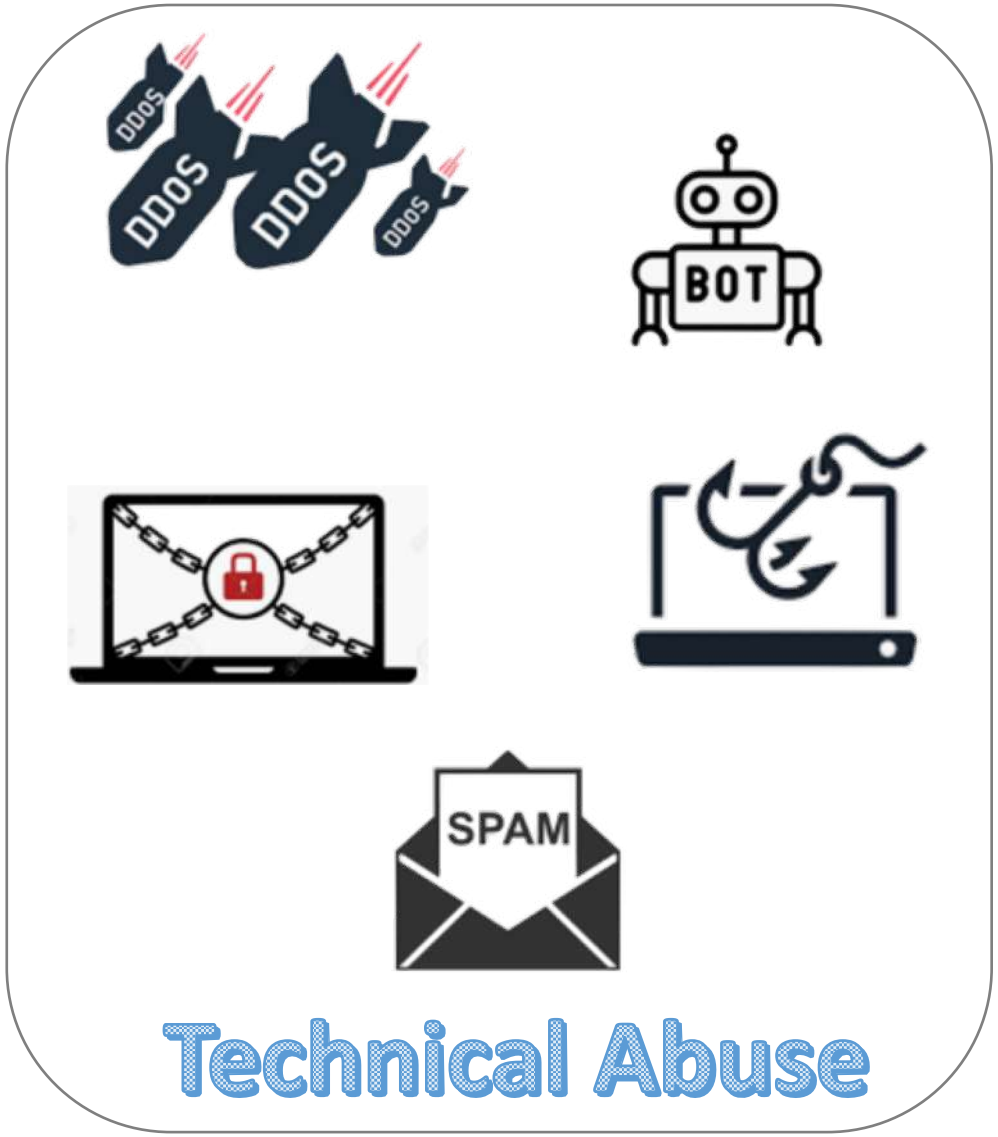


Potential Cyber Norms

違反公共秩序 Disrupt public order
人身傷害Personal injury
金錢損失Monetary damages
兒少侵害 child abuse
非法交易Illegal trades
非法活動 Threats of illegal activity

Principle of Proportionality : DNS Regime





DNS abuse

Technical Regime
.TW DNS query : 1.7T queries =>1.2T abuse queries
TWCERT : 200K cases / month

Law Regime
Disinformation cases
通報>10000, 提報 2953, 偵辦 589, 移送地檢 93, 三審定讞 0

Gap assessment

From intermediary liability to intermediary responsibility

Abuse framework

Technical abuse
1 malware
2 botnet
3 ransomware
4 DDoS
5 phishing
6 spam

Cyber norms
1 MANII
2 iWin
3 **Emergent abuse**
(1) public order
(2) personal injury
(3) monetary damages
(4) child abuse *
(5) illegal trade
(6) threat of illegal activity

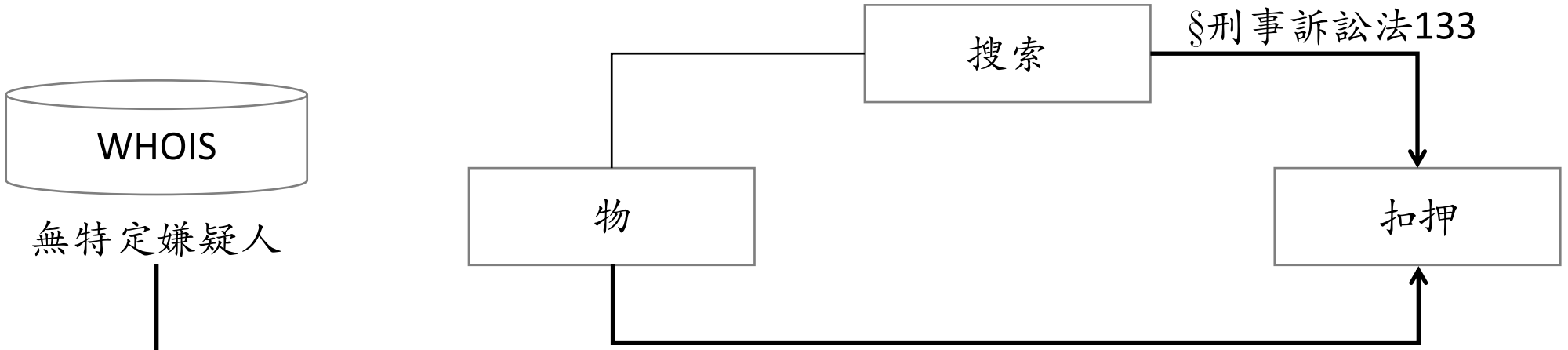
Unlawful abuse
1 court order
2 injunction
3 executive order
4 threat Intelligence

Cyber Jurisdiction

Current solutions
1. MLAT
2. Budapest Convention
(1) slow
(2) not scalable
3. Legal cooperation
(1) lack of transparency
(2) admissibility of evidences
(3) conflict of laws

Extraterritorial effectiveness
1兒少法46 條
2 動保條例 38-3 條

虛擬資源扣押



Domain/IP 非附隨於搜索之扣押命令

§刑事訴訟法133-2　應扣押之物: DN/IP

Domain / IP 單獨宣告沒收程序

§刑事訴訟法455-34

原則：經法院裁定

例外：

1. 證據扣押
2. 同意扣押
3. 緊急扣押

*沒入與扣押為實質控制其使用、阻礙其原本使用

Q
A