APIGA
ASIA PACIFIC INTERNET
GOVERNANCE ACADEMY

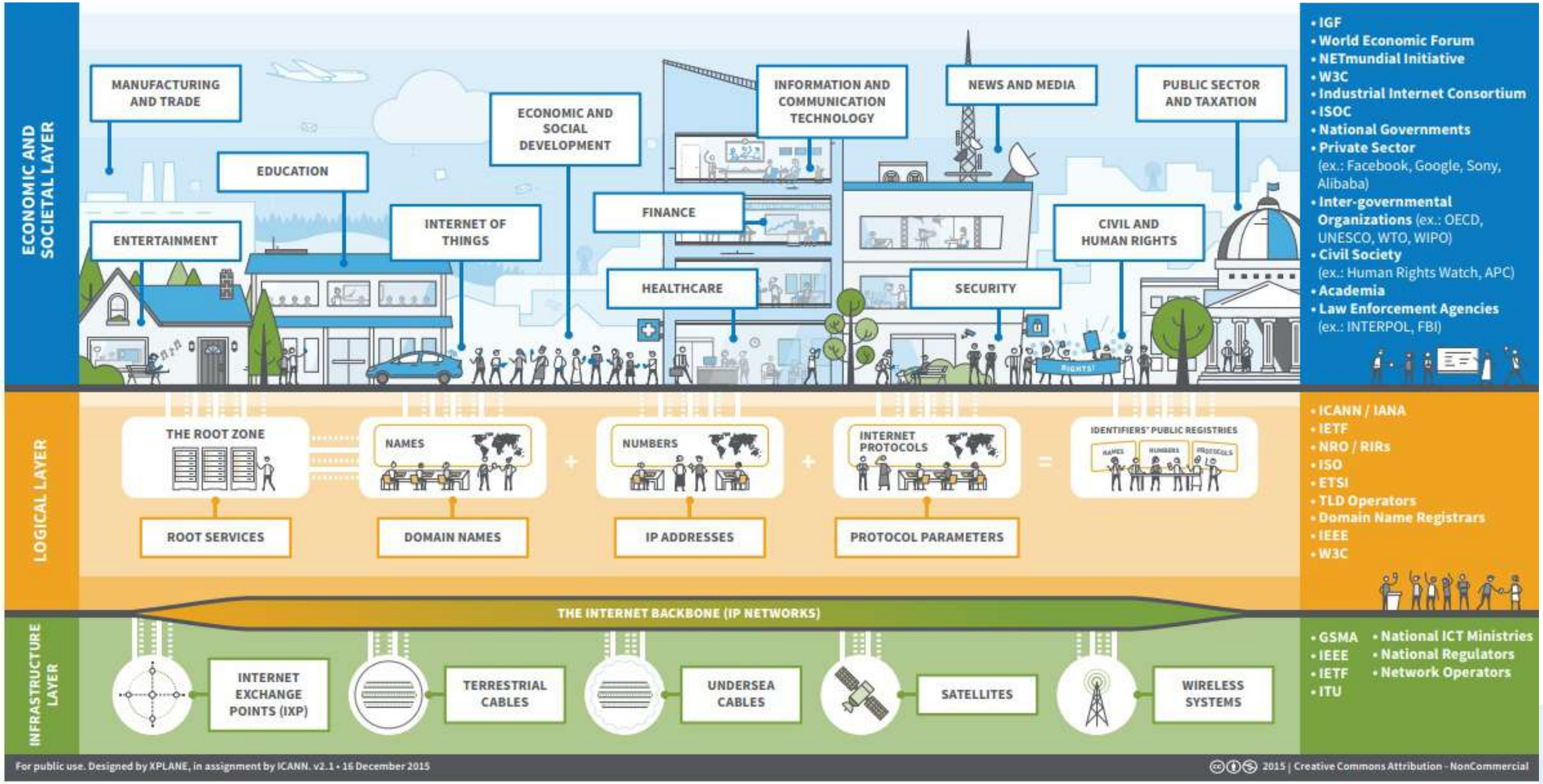
History of IG & IG Today

Dr. Kenny Huang 黃勝雄博士
Chair, TWNIC
Chair, APNIC

2023 Jul 24

Governance of the Internet

No one person, government, organization, or company governs the digital space. Digital Governance may be stratified into the three layers… Solutions to issues in each layer include **policies, best practices, standards, specifications, and tools** developed by the collaborations of stakeholders and experts from actors in **business, government, academia, technical, and civil society** (ICANN, 2015)



ECONOMIC AND SOCIETAL LAYER

MANUFACTURING AND TRADE

ECONOMIC AND SOCIAL DEVELOPMENT

INFORMATION AND COMMUNICATION TECHNOLOGY

NEWS AND MEDIA

PUBLIC SECTOR AND TAXATION

EDUCATION

FINANCE

INTERNET OF THINGS

CIVIL AND HUMAN RIGHTS

ENTERTAINMENT

HEALTHCARE

SECURITY

- IGF
- World Economic Forum
- NETmundial Initiative
- W3C
- Industrial Internet Consortium
- ISOC
- National Governments
- Private Sector (ex.: Facebook, Google, Sony, Alibaba)
- Inter-governmental Organizations (ex.: OECD, UNESCO, WTO, WIPO)
- Civil Society (ex.: Human Rights Watch, APC)
- Academia
- Law Enforcement Agencies (ex.: INTERPOL, FBI)

LOGICAL LAYER

THE ROOT ZONE

NAMES + NUMBERS + INTERNET PROTOCOLS = IDENTIFIERS' PUBLIC REGISTRIES

ROOT SERVICES

DOMAIN NAMES

IP ADDRESSES

PROTOCOL PARAMETERS

- ICANN / IANA
- IETF
- NRO / RIRs
- ISO
- ETSI
- TLD Operators
- Domain Name Registrars
- IEEE
- W3C

THE INTERNET BACKBONE (IP NETWORKS)

INFRASTRUCTURE LAYER

INTERNET EXCHANGE POINTS (IXP)

TERRESTRIAL CABLES

UNDERSEA CABLES

SATELLITES

WIRELESS SYSTEMS

- GSMA
- IEEE
- IETF
- ITU

- National ICT Ministries
- National Regulators
- Network Operators

For public use. Designed by XPLANE, in assignment by ICANN. v2.1 • 16 December 2015

Internet governance model

Multistakeholder model

- ICANN
- RIRs
- IETF
- ccTLDs, gTLDs, Registrars

Multistakeholder shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.

Limited intervention

- UK Investigatory Powers Act
- US Rule 41
- AU Anti-encryption Law

Cyber sovereignty

- Great firewall of China
- Russia Internet Isolation Bill

Government determines cyberspace, control mechanism and cyberjuridiction.

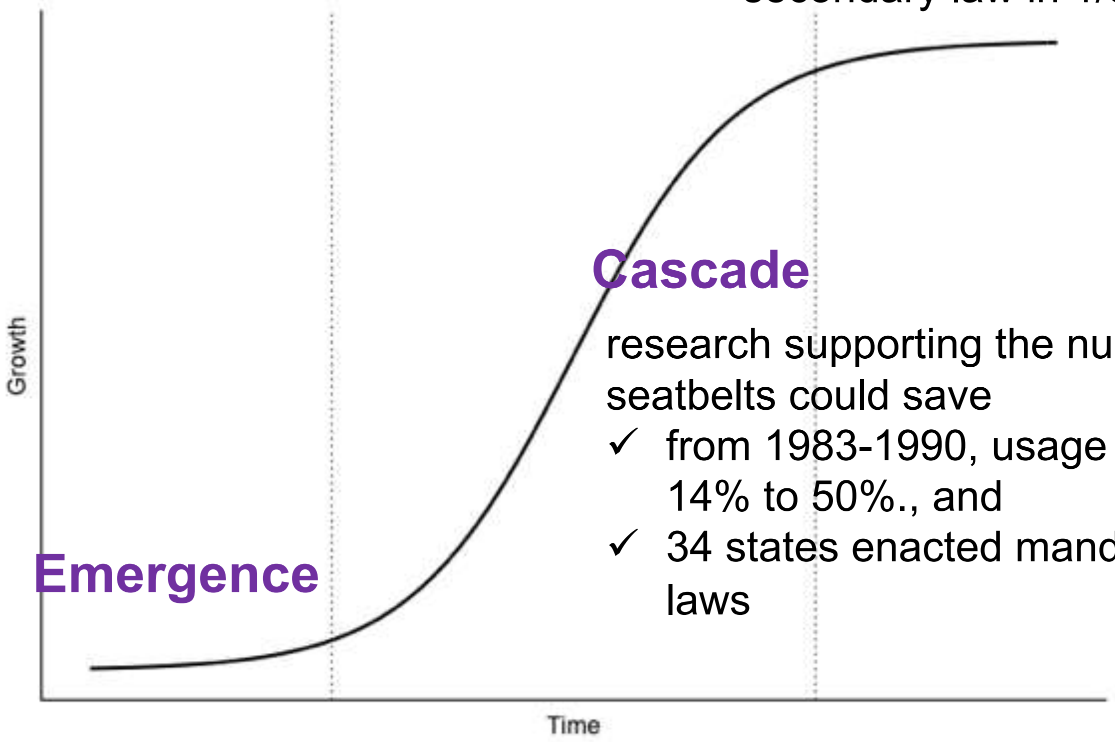
Case: US car seat belt

1968 – National Highway Safety Bureau requires seat belt fastening

Battles over regulation and civil liberties infringements

Entrenchment

In US, 87% of adults wear seatbelts all the time, despite it being a secondary law in 1/3 of states.



Cascade

research supporting the number of lives seatbelts could save

- ✓ from 1983-1990, usage went from 14% to 50%., and
- ✓ 34 states enacted mandatory usage laws

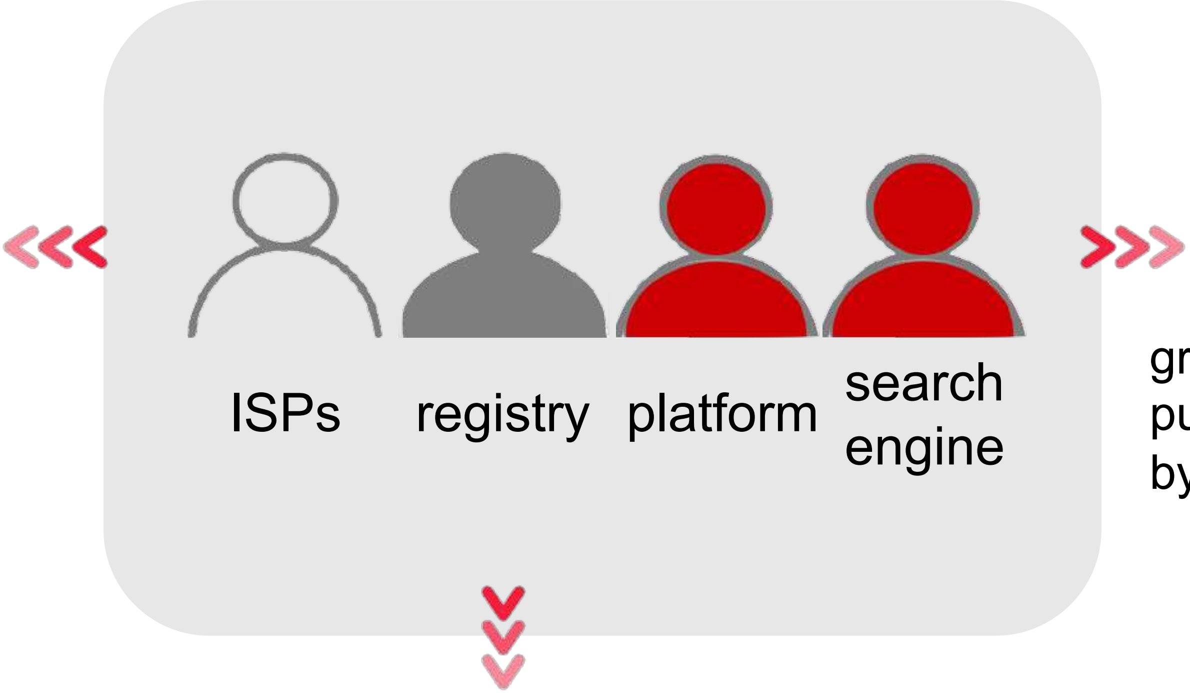
Emergence

Intermediary Responsibility

Power of Enforceability

Well-positioned to impose internet policy or regulatory functions

Internet Intermediaries



Telecommunication Act

Net neutrality,
Universal Service

CDA Sec. 230

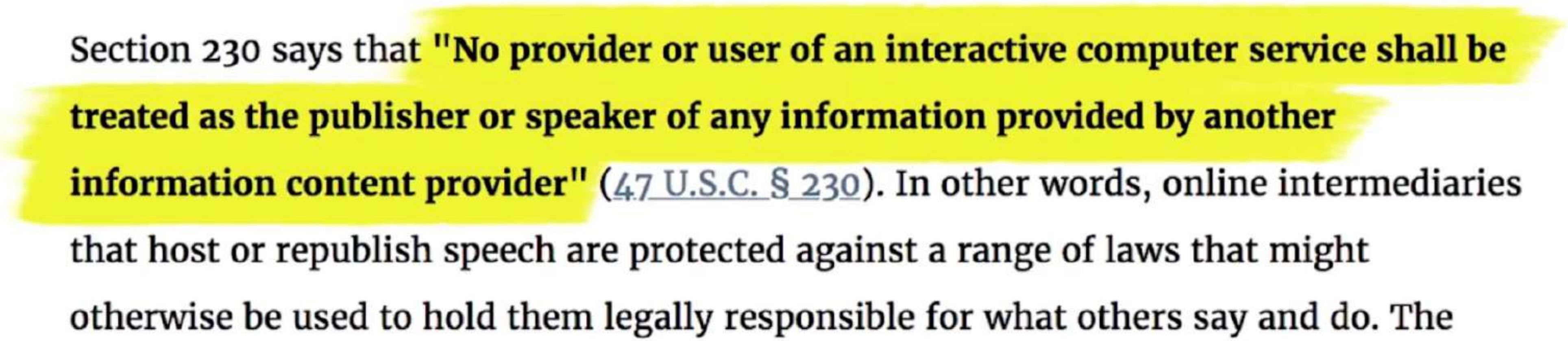
grants legal immunity to online publishers for content provided by third parties.

Multistakeholder Model

Fiduciary duty

CDA Section 230

Communications Decency Act



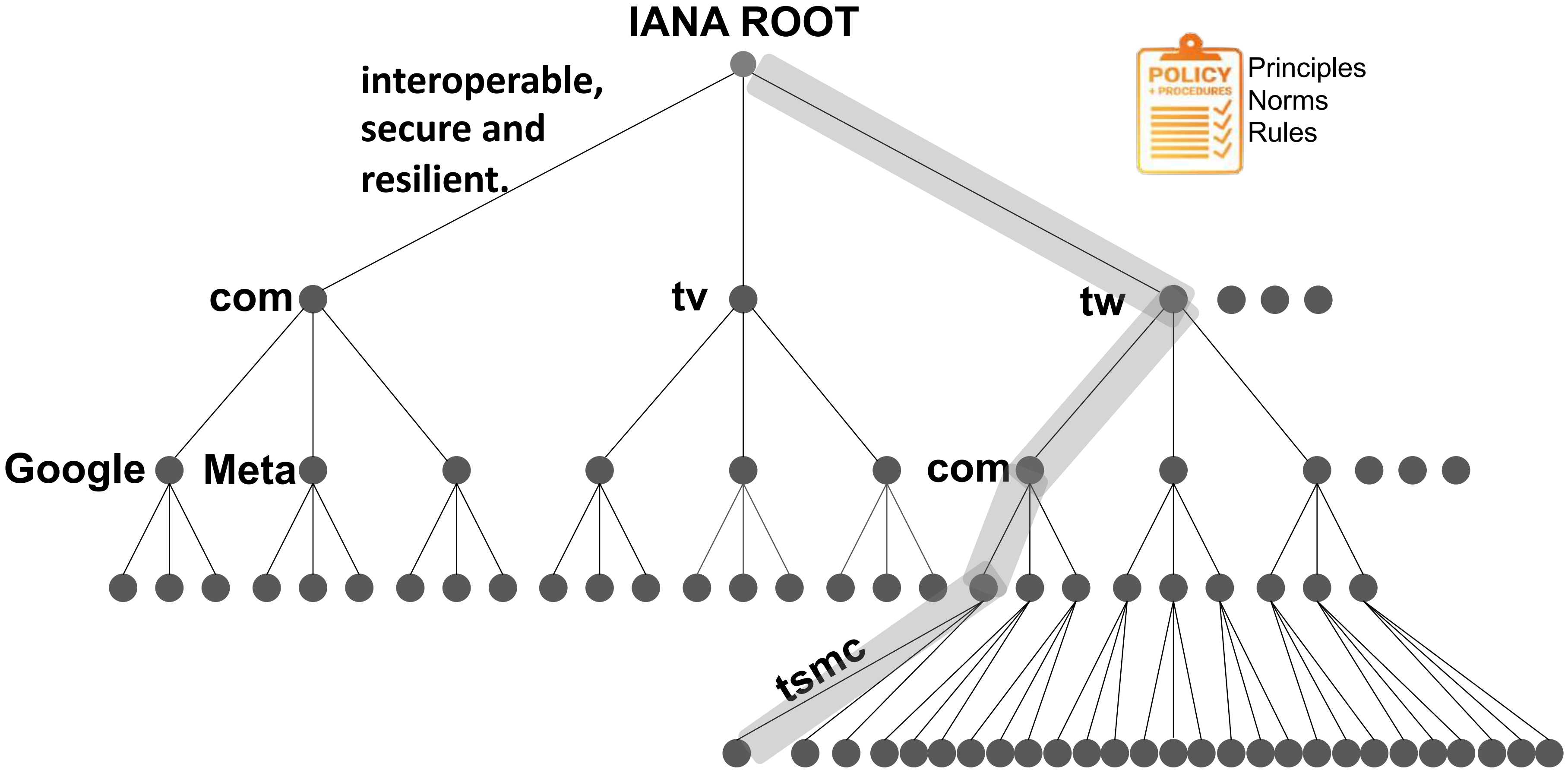
Section 230 says that **"No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider"** (47 U.S.C. § 230). In other words, online intermediaries that host or republish speech are protected against a range of laws that might otherwise be used to hold them legally responsible for what others say and do. The

Protects freedom of speech

Stimulating innovations

Norms (Manila Principles)

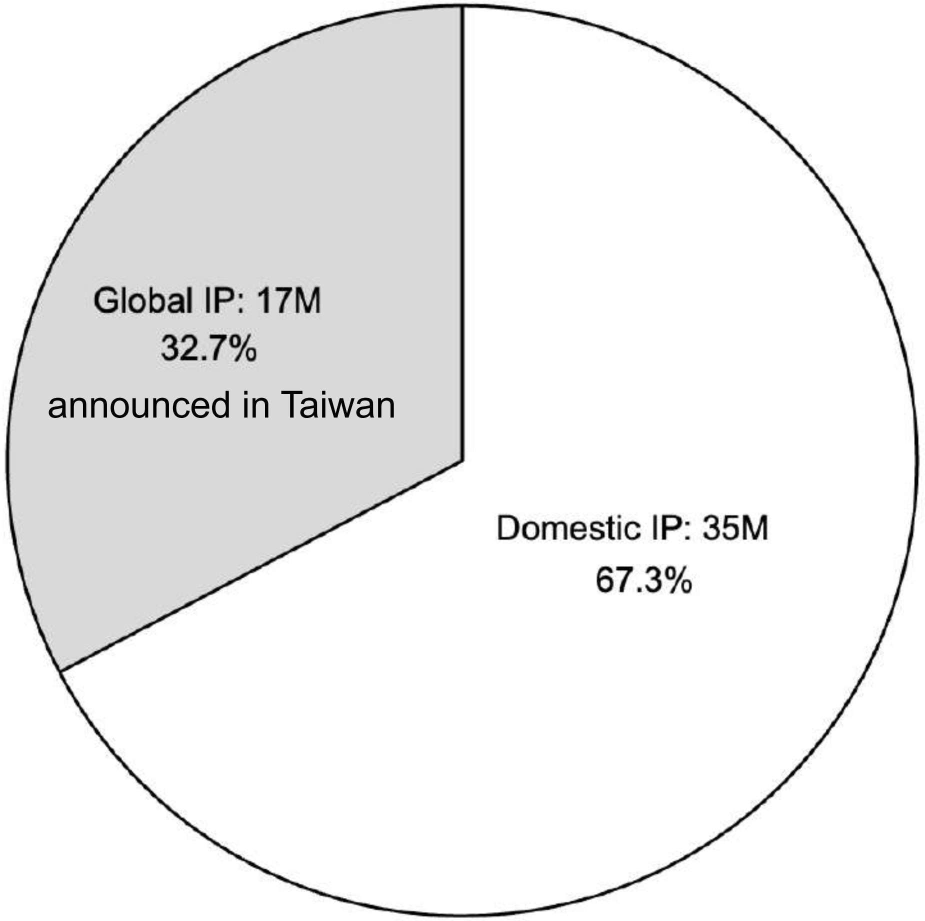
DNS architecture



interoperable, secure and resilient.

Principles
Norms
Rules

Internet from different lenses



2.6 days

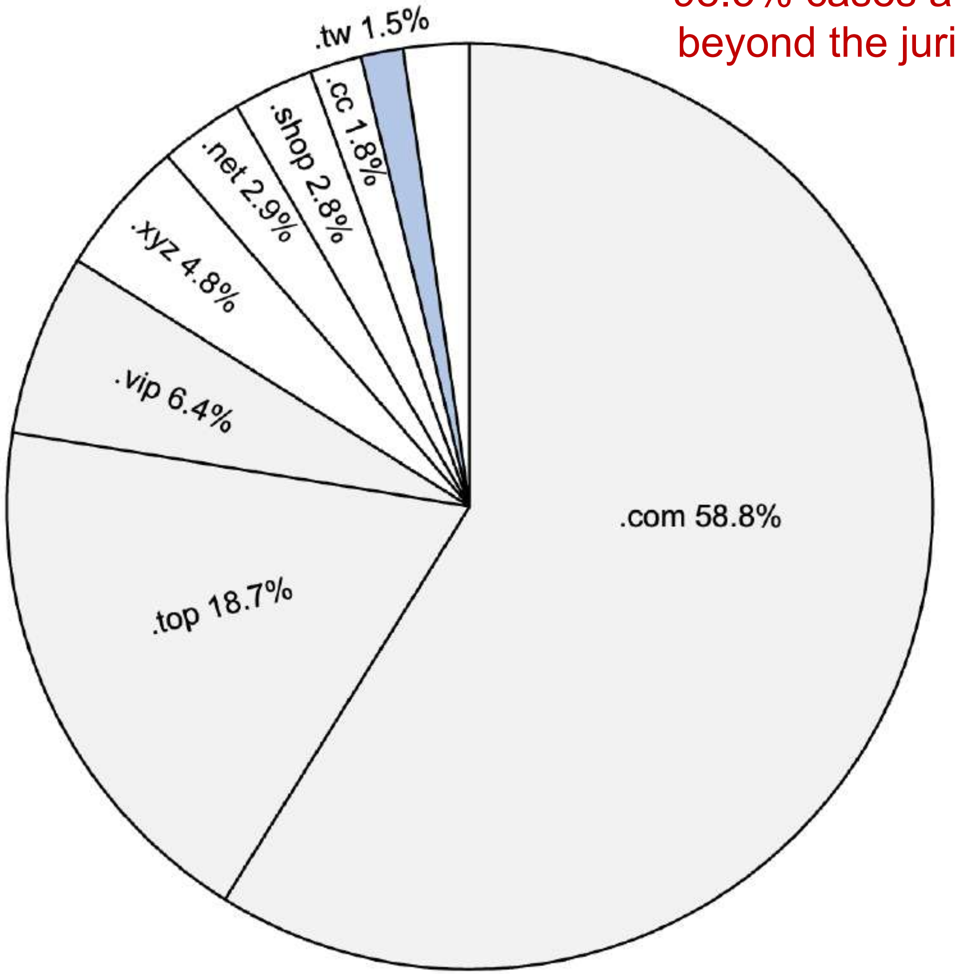
abuse IP life cycle

16.5 days

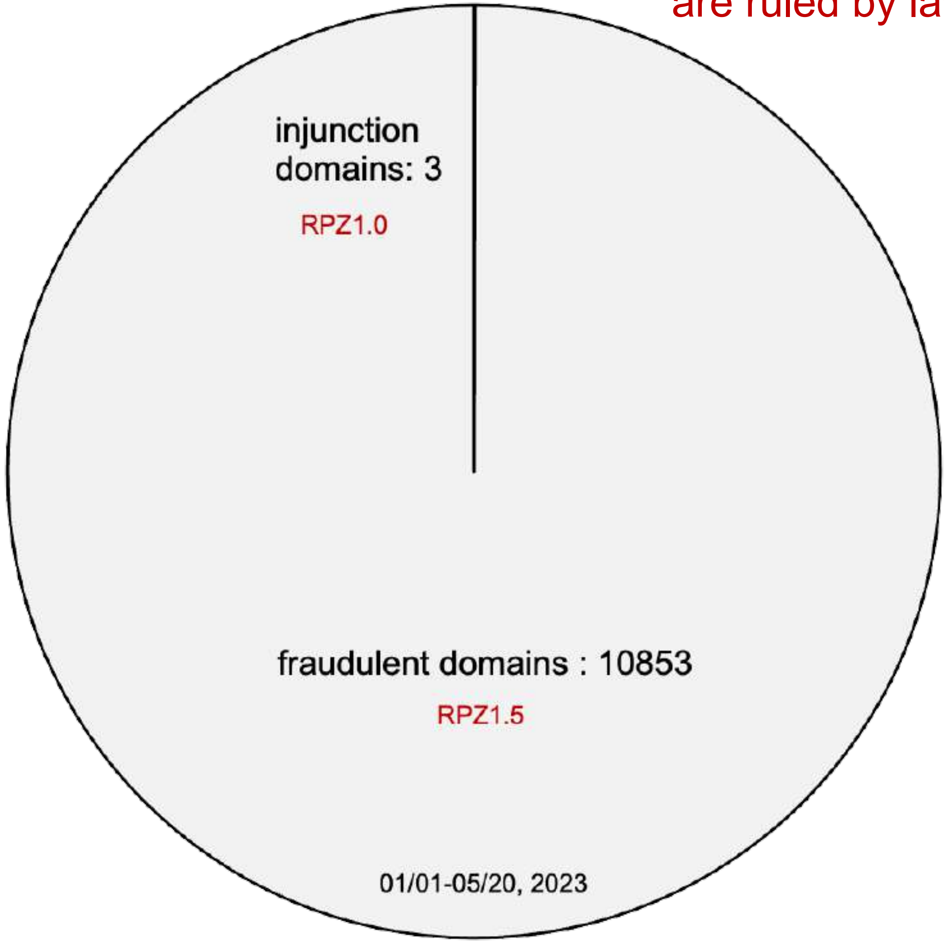
abuse domain life cycle

Source: TWNIC

Cybercrime statistics



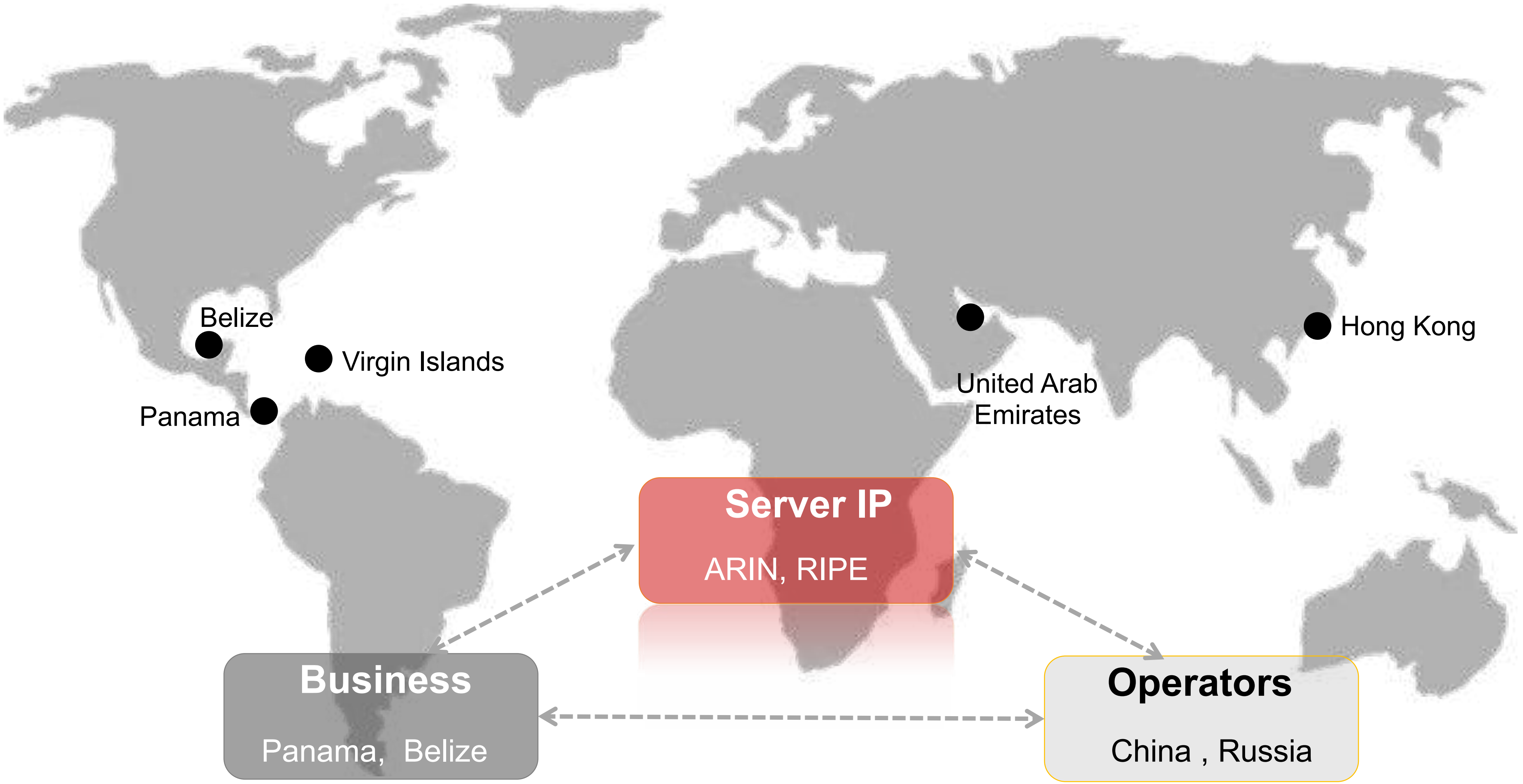
98.5% cases are beyond the jurisdiction.



0.03% of cases are ruled by law.

Source: TWNIC (CIB, MJIB, High Prosecutors Office, Court)

Cybercrime global operation



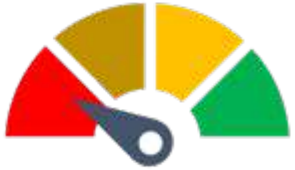
Current solutions

Borderless Internet

National laws confined to territorial limits

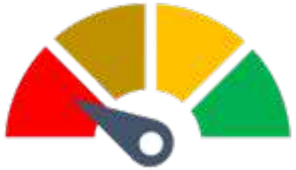
MLAT

- Slow and complicated



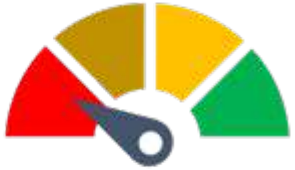
Budapest Convention

- Extremely slow and complicated
- Not scalable



Legal Cooperation

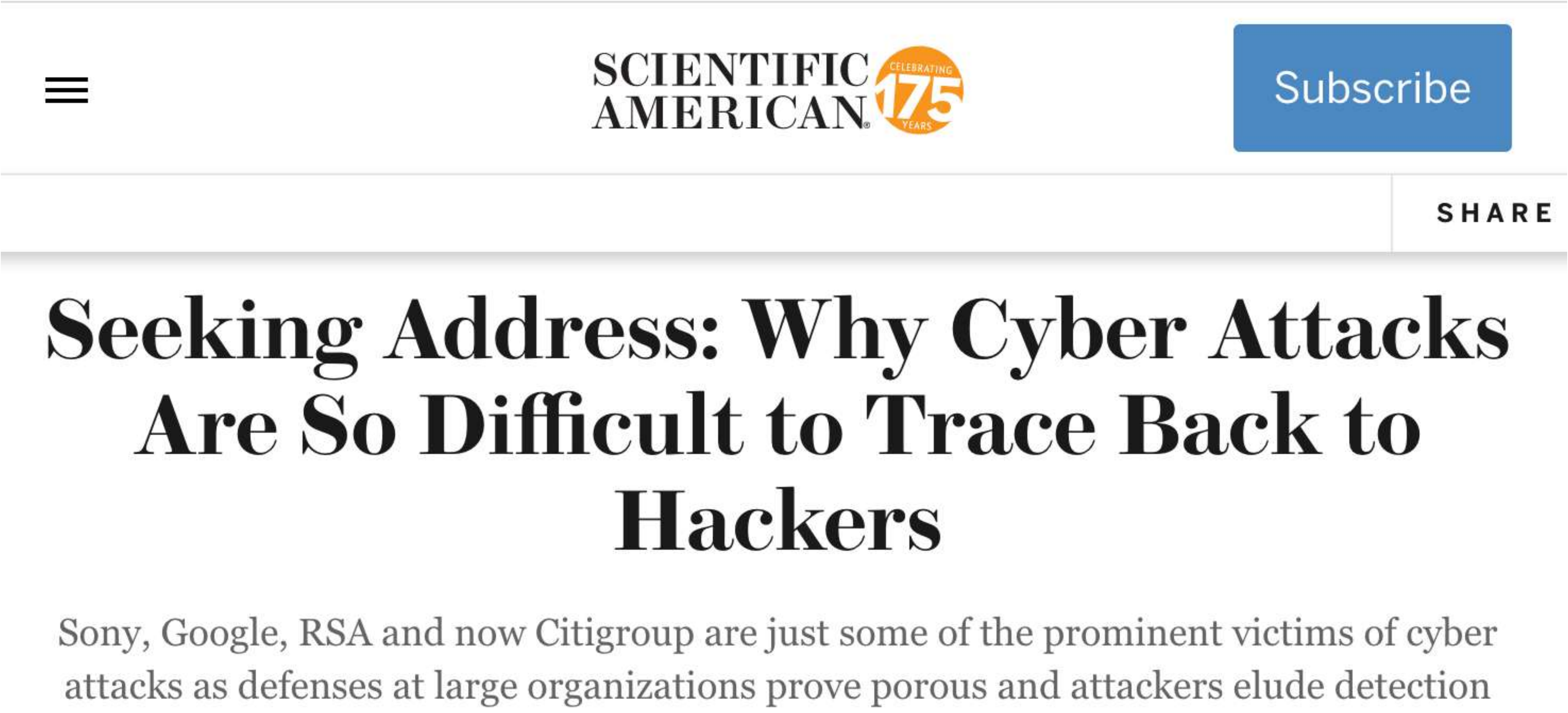
- Lack of transparency
- Evidence admissibility
- Conflicts of law



Public policy governance model

	Governance Capacity and Capability		
Private sector	👎	👍	👍
Public sector	👍	👍	👎
Governance Model	State regulation (Neoliberalism)	Cooperation (Knill, 2002) Co-regulation (Tanja Borzel, 2007) Delegation (Tanja, Borzel, 2007)	Self regulation (Knill, 2002)

Principles
Norms
Rules



Seeking Address: Why Cyber Attacks Are So Difficult to Trace Back to Hackers

Sony, Google, RSA and now Citigroup are just some of the prominent victims of cyber attacks as defenses at large organizations prove porous and attackers elude detection

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

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

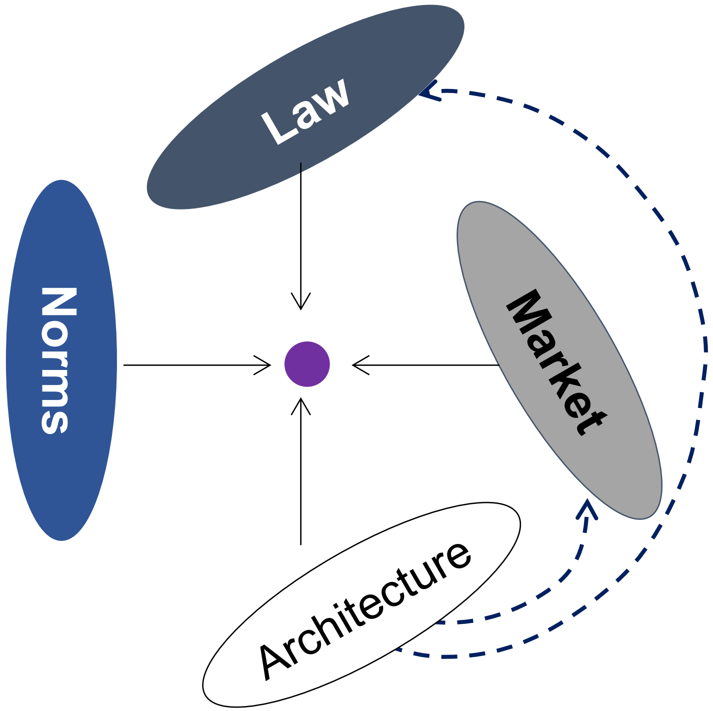
characteristics	ICANN	ITU	IGF	APNIC	TWNIC	IETF	NATO
multistakeholder	x		x	x	x		
bottom-up model of governance	x		x	x	x	x	
standard setting	x	x		x	x	x	
operates based on contractual compliance	x			x	x		
governmental		x					x
sets internationally enforceable obligations for states		x					x

New Chicago School Theory

How to regulate cyberspace

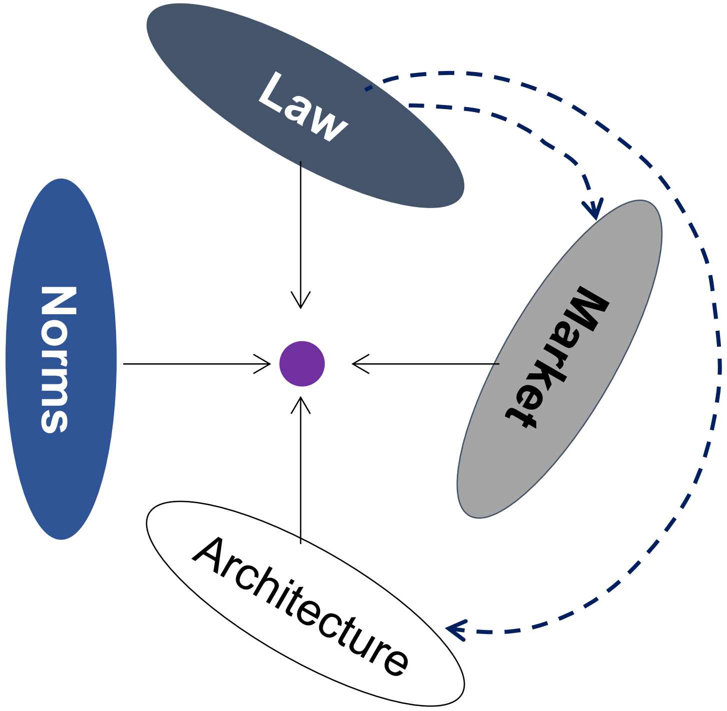
Code is Law

I E T F



Law is Code

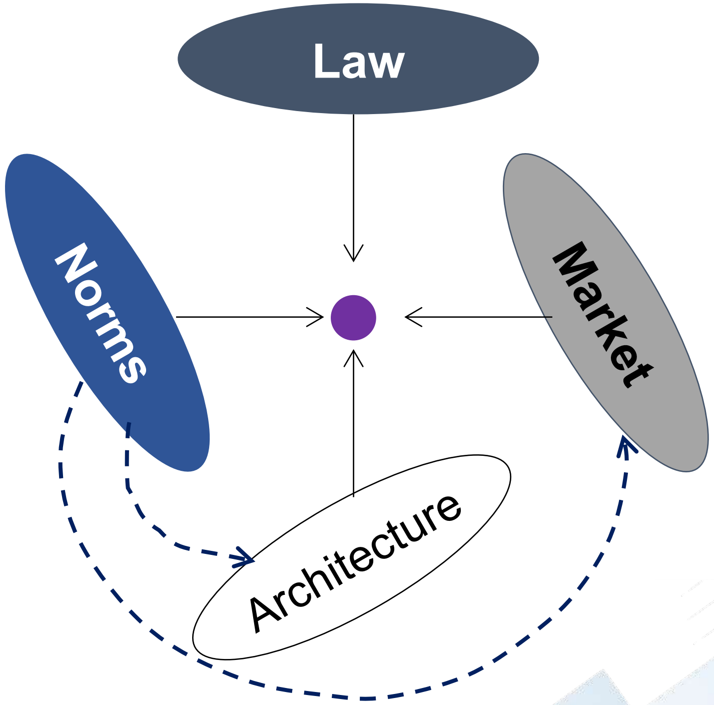
GDPR



Norm is Law

GLOBAL COMMISSION ON THE STABILITY OF CYBERSPACE

IGF GENEVA 2017



Norm: shared expectations of appropriate behavior

Multistakeholder coordination 1/2

hate speech

deepfake

scam

	Effective	Quick	Simple	Precise	Proportional	Cost-Effective
ISP	✓	✗	✗	?	✗	✗
CDN	?	?	?	?	✗	✗
Hosting	✓	✗	✗	✗	✗	✗
Platform	✓	✓	✓	✓	✓	✓
Registrar	✓	✓	✓	✗	✗	✗
Registry	✓	✓	✓	✗	✗	✗

Multistakeholder coordination 2/2

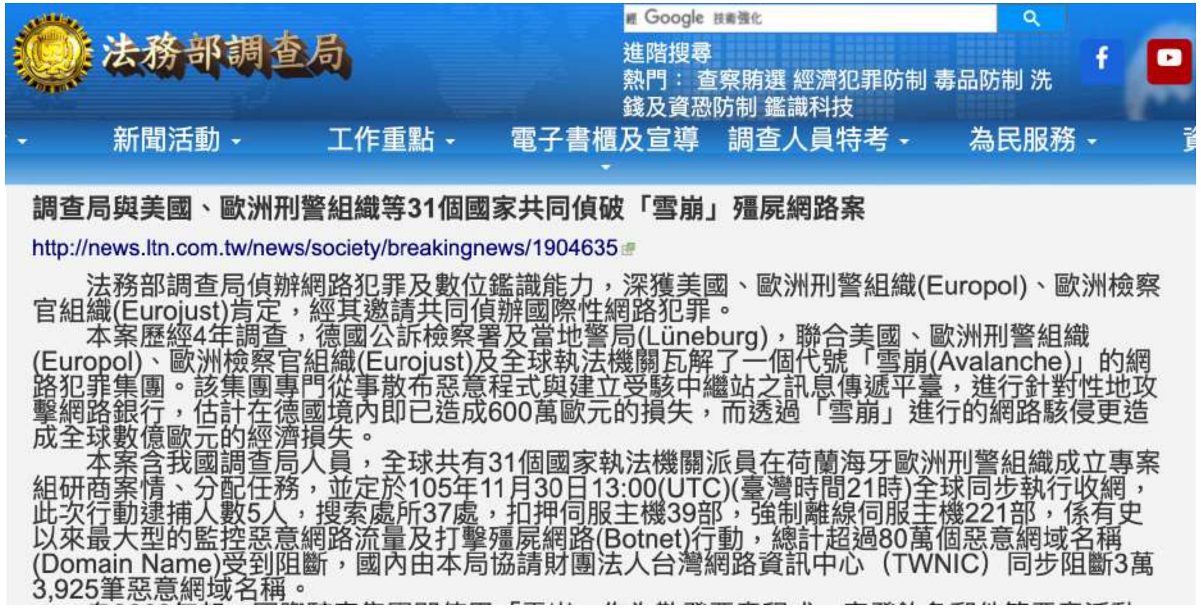
SCENARIO

C2 server

botnet

pirate site

	Effective	Quick	Simple	Precise	Proportional	Cost-Effective
ISP	✗	✗	✗	?	✓	✗
CDN	✗	?	?	?	✓	?
Hosting	✗	?	✓	✓	✓	✓
Platform	?	?	?	?	?	?
Registrar	✓	✓	✓	✓	✓	✗
Registry	✓	✓	✓	✓	✓	✓



調查局與美國、歐洲刑警組織等31個國家共同偵破「雪崩」殭屍網路案

http://news.ltn.com.tw/news/society/breakingnews/1904635

法務部調查局偵辦網路犯罪及數位鑑識能力，深獲美國、歐洲刑警組織(Europol)、歐洲檢察官組織(Eurojust)肯定，經其邀請共同偵辦國際性網路犯罪。

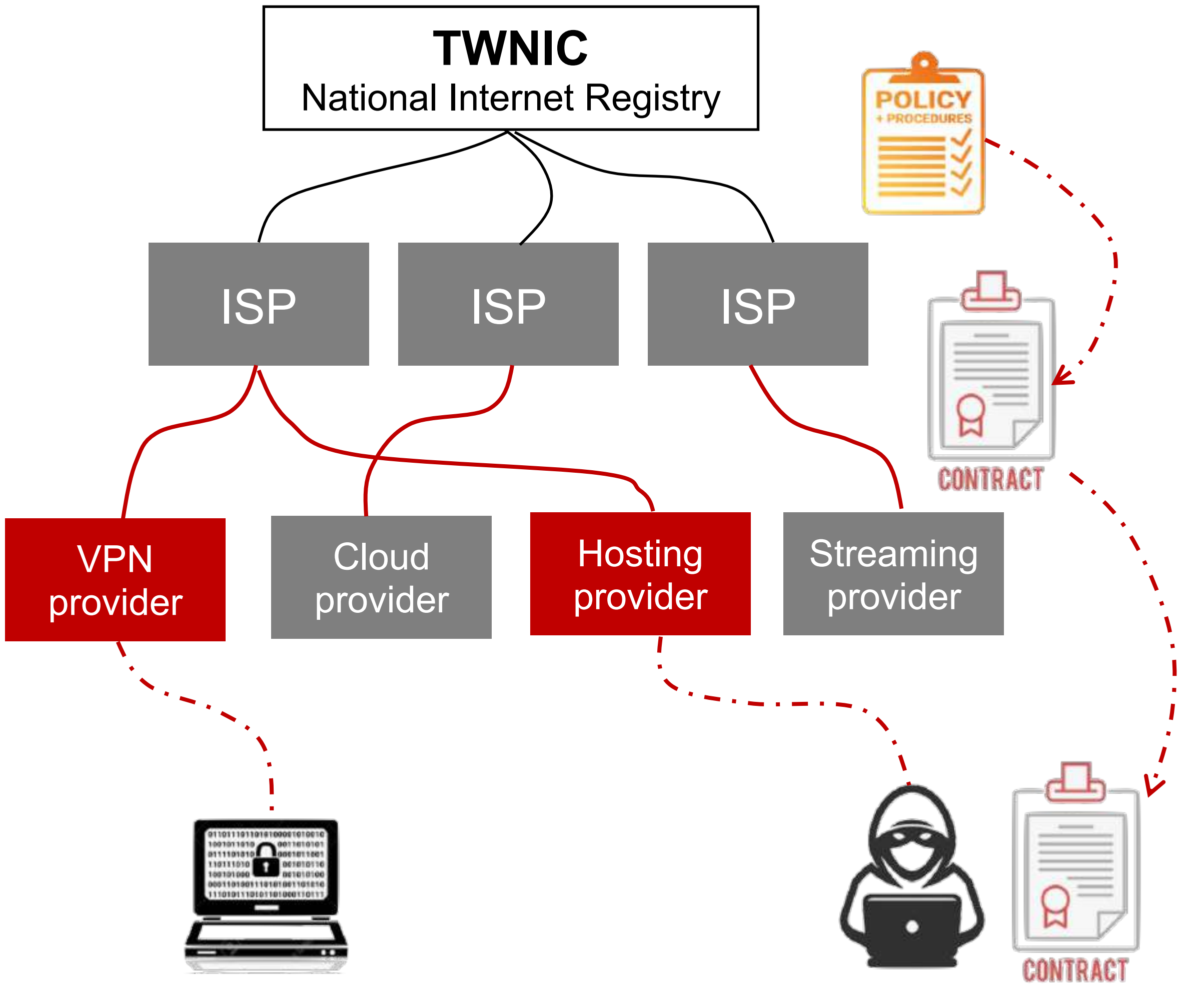
本案歷經4年調查，德國公訴檢察署及當地警局(Lüneburg)，聯合美國、歐洲刑警組織(Europol)、歐洲檢察官組織(Eurojust)及全球執法機關瓦解了一個代號「雪崩(Avalanche)」的網路犯罪集團。該集團專門從事散布惡意程式與建立受駭中繼站之訊息傳遞平臺，進行針對性地攻擊網路銀行，估計在德國境內即已造成600萬歐元的損失，而透過「雪崩」進行的網路駭侵更造成全球數億歐元的經濟損失。

本案含我國調查局人員，全球共有31個國家執法機關派員在荷蘭海牙歐洲刑警組織成立專案組研商案情、分配任務，並定於105年11月30日13:00(UTC)(臺灣時間21時)全球同步執行收網，此次行動逮捕人數5人，搜索處所37處，扣押伺服主機39部，強制離線伺服主機221部，係有史以來最大型的監控惡意網路流量及打擊殭屍網路(Botnet)行動，總計超過80萬個惡意網域名稱(Domain Name)受到阻斷，國內由本局協請財團法人台灣網路資訊中心（TWNIC）同步阻斷3萬3,925筆惡意網域名稱。

台灣微軟攜手法務部調查局攻破非法IP位址 成功遏止殭屍網路肆虐

April 21, 2020

IP Address Policy



TWNIC

National Internet Registry

ISP

ISP

ISP

VPN provider

Cloud provider

Hosting provider

Streaming provider

Cybercrime Mitigation Strategy

TIG Norms

- Information disclosure : address holder should be registered in WHOIS database if allocation > /30
- Abuse contact validation every 6 months

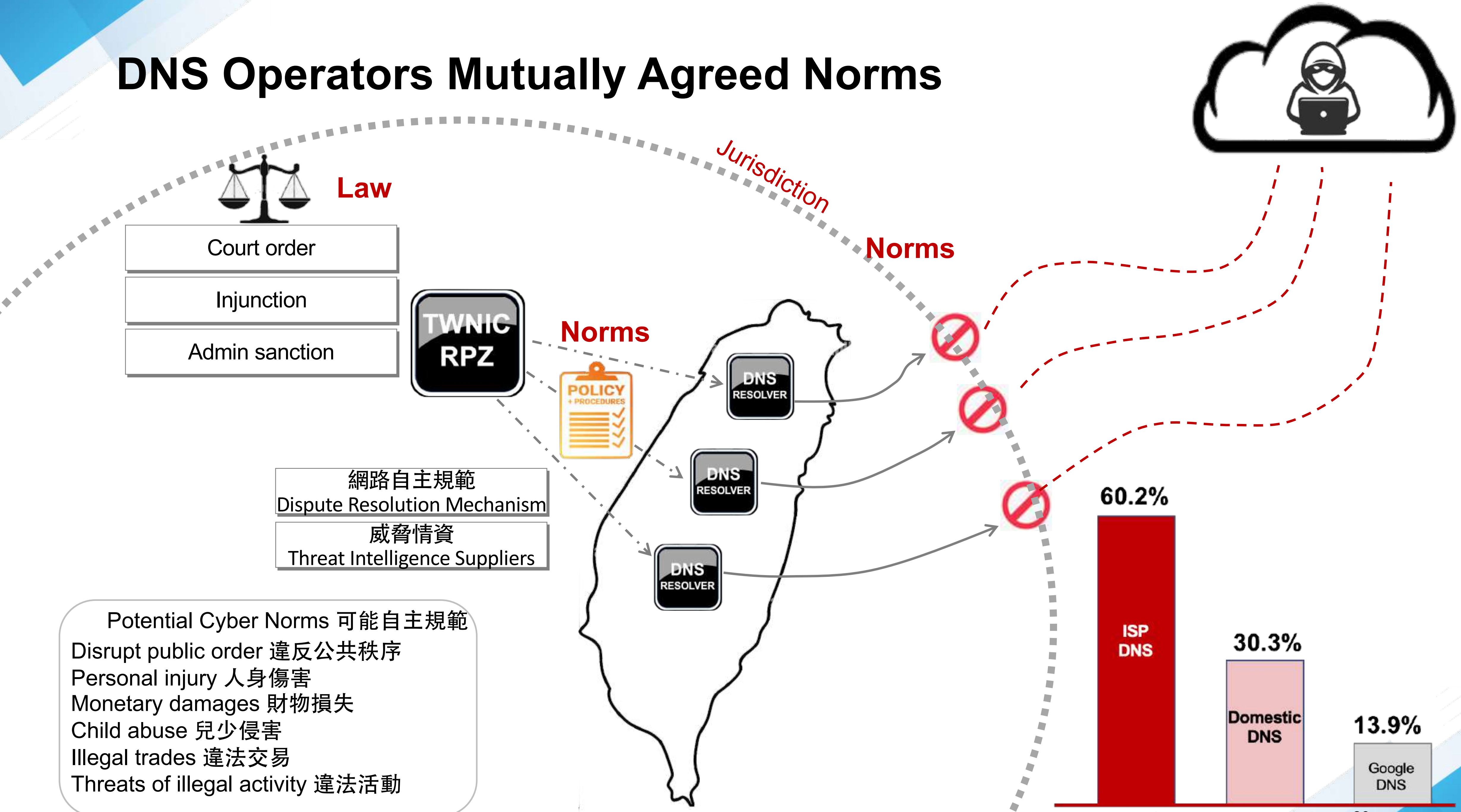
Contractual Compliance

- Inform address holder’s responsibility conducting cybersecurity clearance
- deploy required measures to against cyber threats.
- transparency and accountability mechanism.

Norm Enforcement

- Q/A methodology : official notice and timely response until issue resolved.
- Address holder’s resources can be frozen if it fail to fulfill contractual obligations.

DNS Operators Mutually Agreed Norms



Court order

Injunction

Admin sanction

網路自主規範
Dispute Resolution Mechanism

威脅情資
Threat Intelligence Suppliers

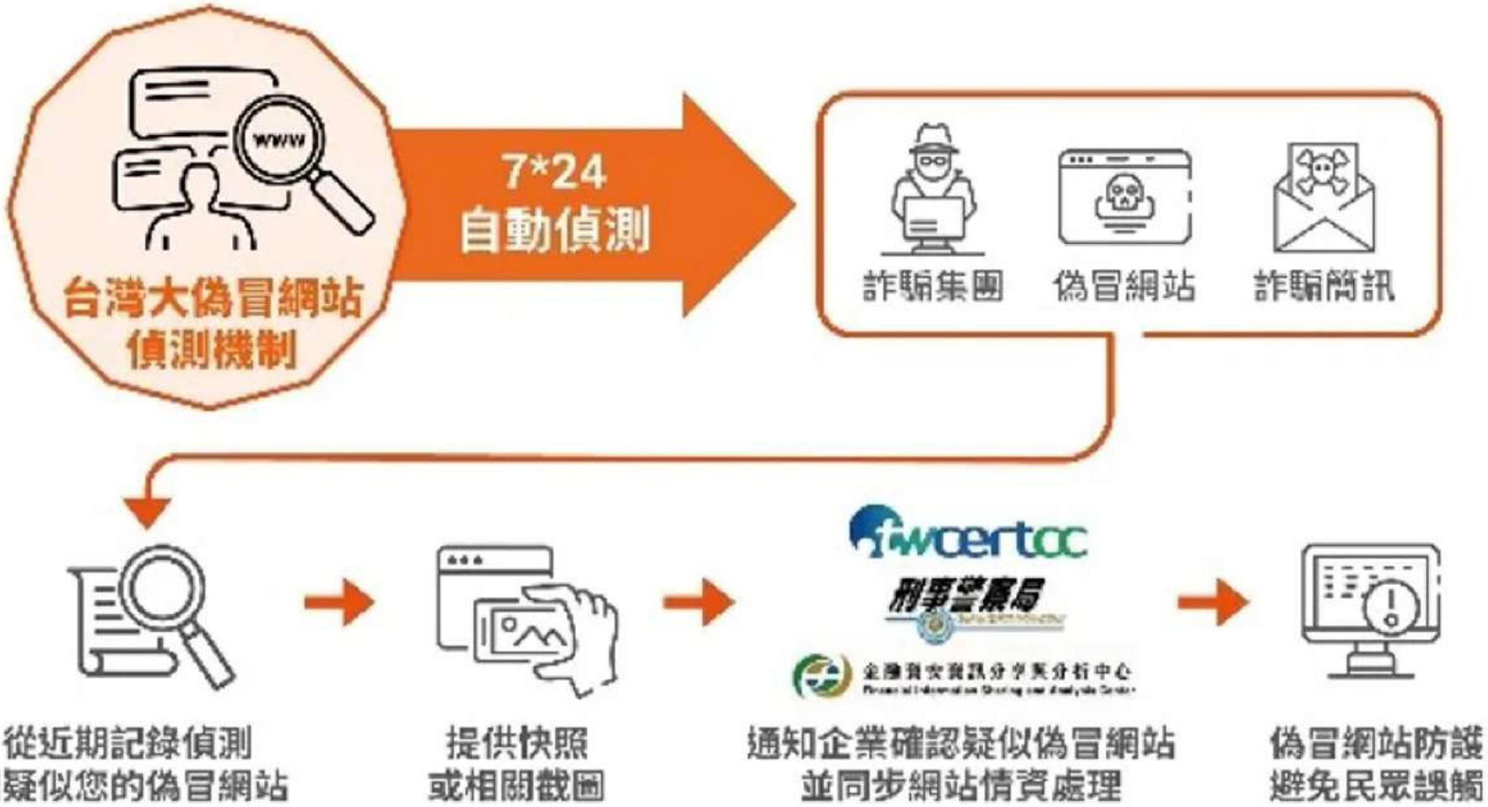
Potential Cyber Norms 可能自主規範
Disrupt public order 違反公共秩序
Personal injury 人身傷害
Monetary damages 財物損失
Child abuse 兒少侵害
Illegal trades 違法交易
Threats of illegal activity 違法活動

Taiwan DNS Resolver Market Share

TWNIC DNS RPZ

RPZ1.0	RPZ1.5	Trusted Notifiers
Court Oders	**Disinformation during election**	**High Prosecutor’s Office**
Injunctions	**Critical Financial Crime**	**Ministry of Justice**
Sanctions	**Government Phishing Website**	**Crime Investigation Bureau**
	Scam Website	**Ministry of Digital Affairs**

偽冒網站偵測服務：服務架構



台灣大偽冒網站偵測機制

7*24
自動偵測

詐騙集團

偽冒網站

詐騙簡訊

從近期記錄偵測
到疑似您的偽冒網站

提供快照
或相關截圖

twcertcc

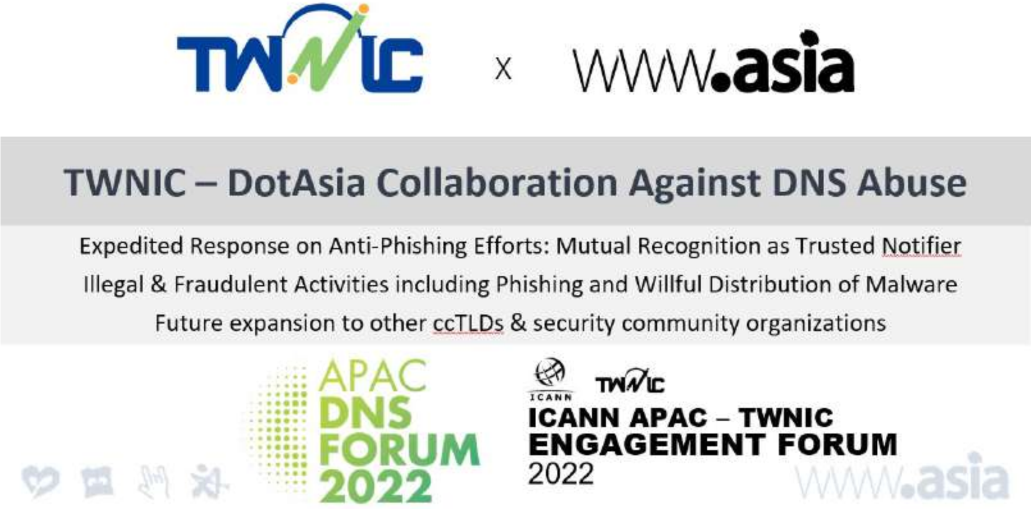
刑事警察局

金融資安資訊分享與分析中心
Financial Information Sharing and Analysis Center

通知企業確認疑似偽冒網站
並同步網站情資處理

偽冒網站防護
避免民眾誤觸

Multistakeholder Model Best Practice



TWNIC x www.asia

TWNIC – DotAsia Collaboration Against DNS Abuse

Expedited Response on Anti-Phishing Efforts: Mutual Recognition as Trusted Notifier

Illegal & Fraudulent Activities including Phishing and Willful Distribution of Malware

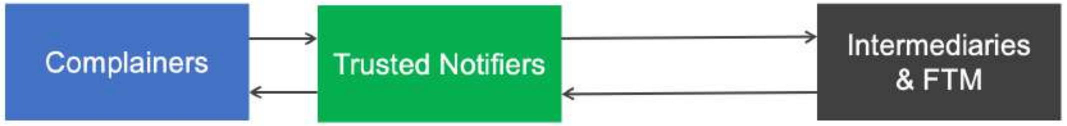
Future expansion to other ccTLDs & security community organizations

APAC DNS FORUM 2022

ICANN APAC – TWNIC ENGAGEMENT FORUM 2022

Value to intermediary :

- Risk reduction : better evidenced
- Cost reduction : transfer evaluation cost to TNs
- Firm value : consumer trust



Complainers

Trusted Notifiers

Intermediaries & FTM

Value to trusted notifier:

- Efficiency : faster
- Effectiveness : enforceability

TWNIC DNS Abuse Framework

Technical Regime

.TW DNS query : 1.7T queries =>1.2T abuse queries

TWCERT : 100K cases / month

Law Regime

Disinformation cases

notice>10000, report 2953, investigate 589, prosecutor office 93

Gap assessment

From intermediary liability to intermediary responsibility

DNS Abuse Framework

Technical abuse

1 malware
2 botnet
3 ransomware
4 phishing
5 spam

Cyber norms

1 TWNIC RPZ Norms
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 orders
2 injunctions
3 sanctions

Cyber Jurisdiction

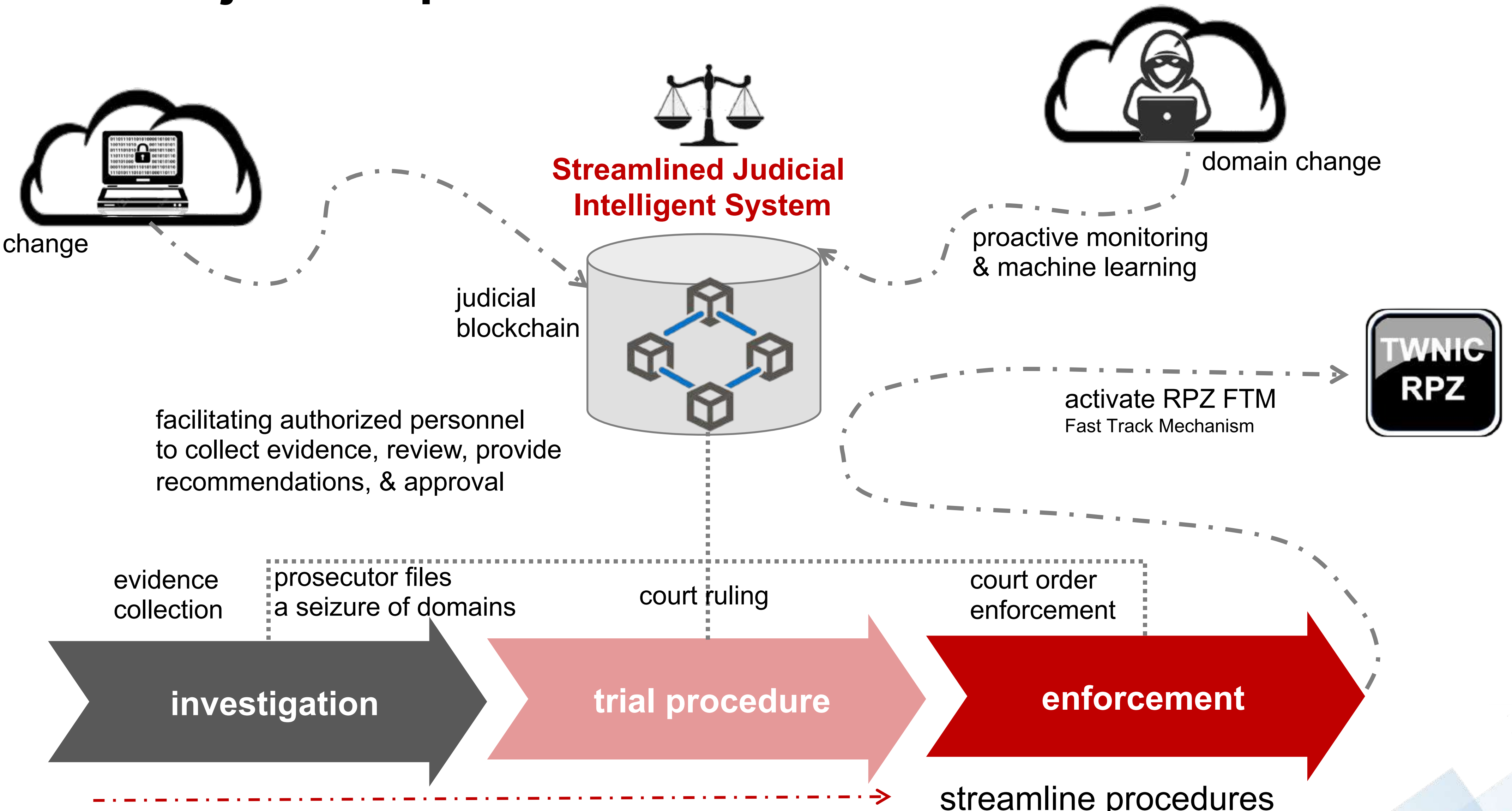
Current solutions

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

Streamline judicial procedures



domain change

Streamlined Judicial Intelligent System

judicial blockchain

domain change

proactive monitoring & machine learning

activate RPZ FTM

Fast Track Mechanism

facilitating authorized personnel to collect evidence, review, provide recommendations, & approval

evidence collection

prosecutor files a seizure of domains

court ruling

court order enforcement

investigation

trial procedure

enforcement

streamline procedures

Q
A