Mutually Agreed Norms for Internet Intermediary (MANII)

Alternative Dispute Resolution for Copyright Infringement

Kenny Huang, Ph.D. 黃勝雄博士

Chairman and CEO

Taiwan Network Information Center

Taiwan Computer Emergency Response Team/Coordination Center

huangk@twnic.tw

Dec 2019

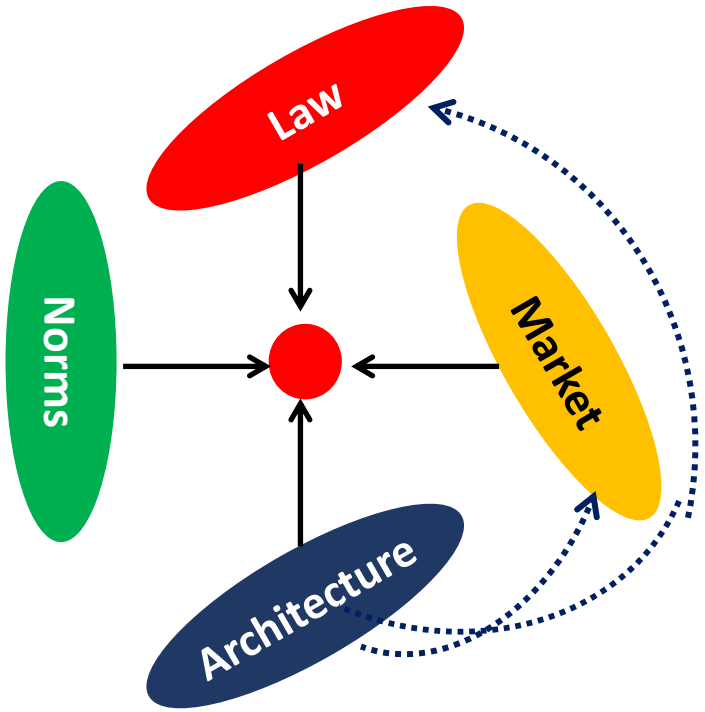
Public Goods Governance Models

	Governance Capability & Capacity for Public Goods		
Non-state Actors	X	O	O
Governments	O	O	X
Governance Model	State Regulation (Neoliberalism)	Cooperation (Knill, 2002)	***Private Self Regulation*** ICANN APNIC IETF (Knill, 2002)
		Co-Regulation (Tanja Borzel, 2007)	
		Delegation (Tanja, Borzel, 2007)	

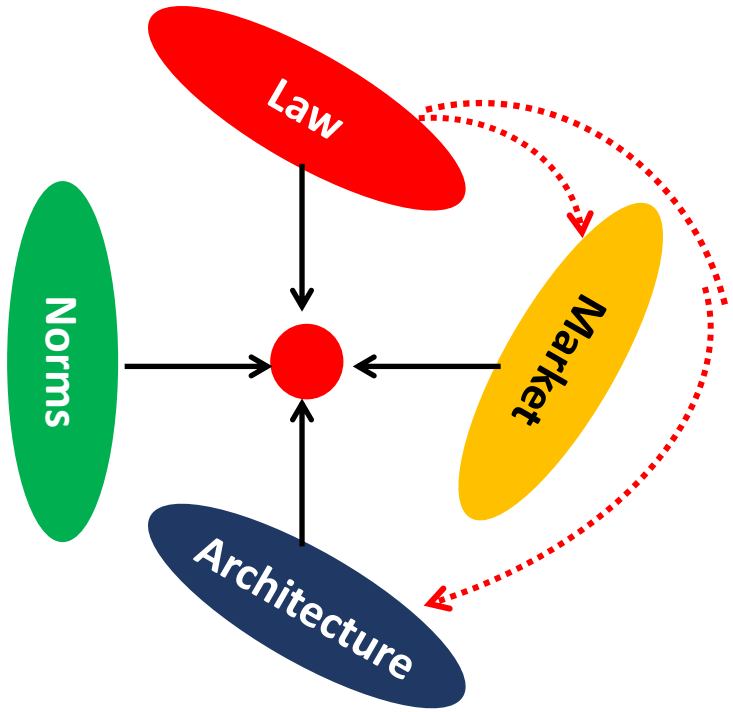
Source: Dr. Kenny Huang

New Chicago School Theory (How is Cyberspace Regulated)

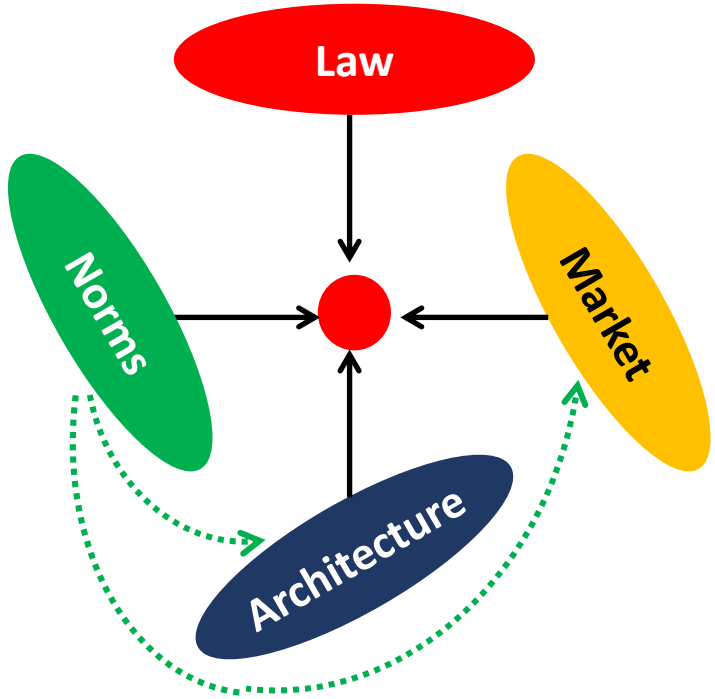
Code is Law



Law is Code



Cyber Norms



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

Safe Harbors ISP Liability

Provision	TPP	USMCA	CETA	RCEP (JPN)	China-Korea FTA
Parties "shall" include secondary liability for ISPs	X	X			
FTA has language pertaining to, but does not require, secondary liability for ISPs			X	X	X
Parties required to include safe harbors for secondary ISP liability		X	X		
Safe harbor explicitly covers transmitting, routing, providing connections, storage	X	X			
Safe harbor explicitly covers hosting	X		X		
Safe harbor explicitly covers caching	X	X	X		

Source: Infojustice (2018 Dec)

ISP Safe harbors 免責要件

1 未主動連線傳輸
2 未選擇資訊接收者
3 未變更傳輸內容

即使 ISP 符合免責要件，並不排除權利人可要求ISP阻止侵權行為可能性

歐盟法院

ISP 居於終結侵權行為最佳位置，在不影響其他救濟可能下，應給予權利人向 ISP 提出緊急處份可能性。此要求未侵害ISP之企業自由

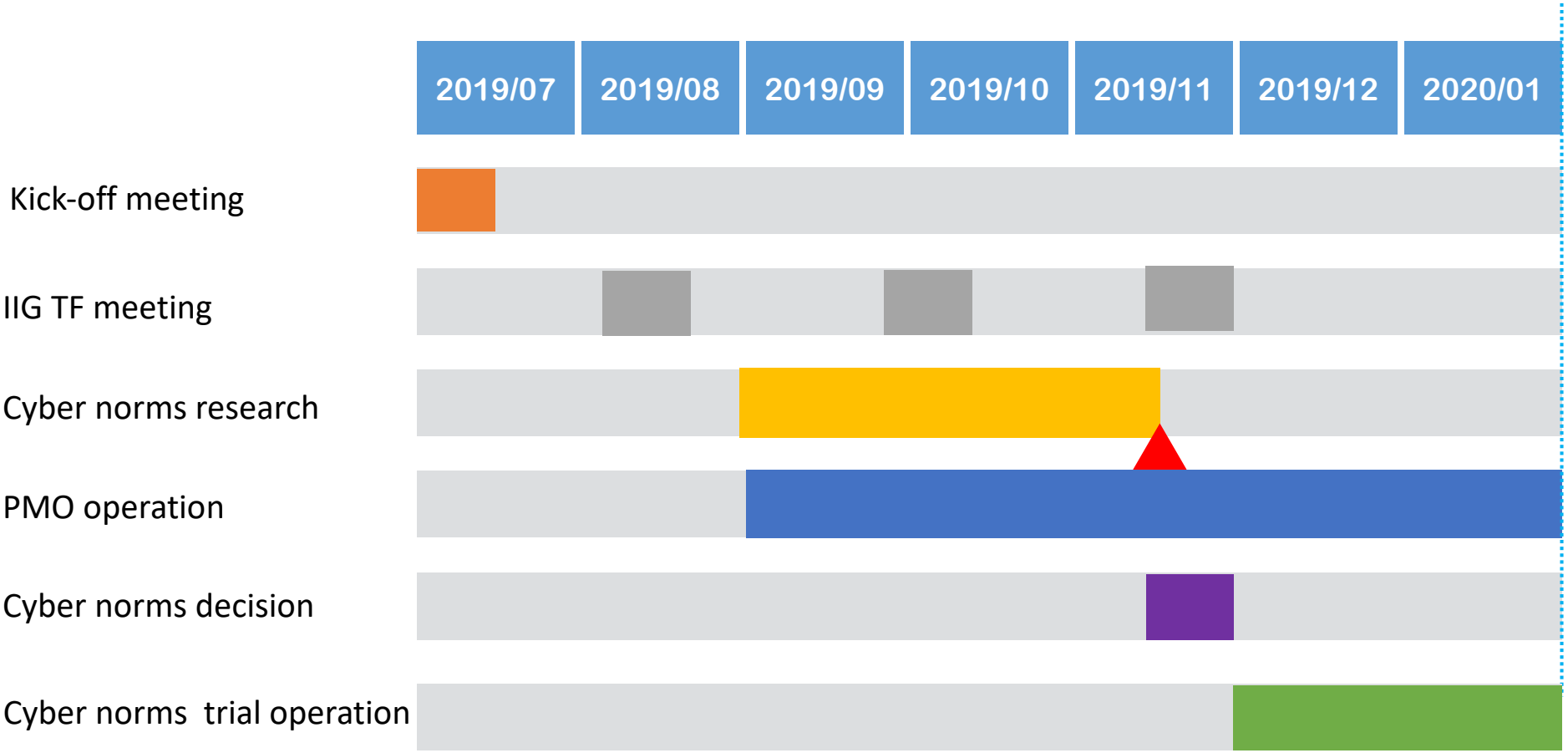
ISP 所採取的措施必須充分有效，足以阻止利用人接取侵害著作權資訊

著作權法90-5條

連線服務提供者對其使用者侵害他人著作權之行為，不負賠償責任

不負賠償責任，不代表免除防止義務

Schedule for Internet Intermediary Governance Taskforce



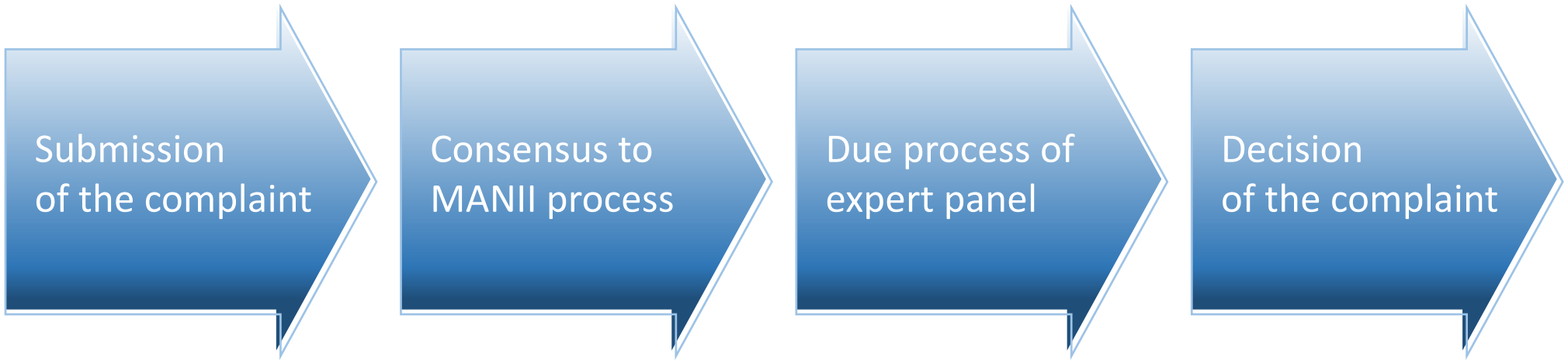
Source: Dr. Kenny Huang (2019 July)

Alternative Dispute Resolution : Proposed Mechanism for MANII

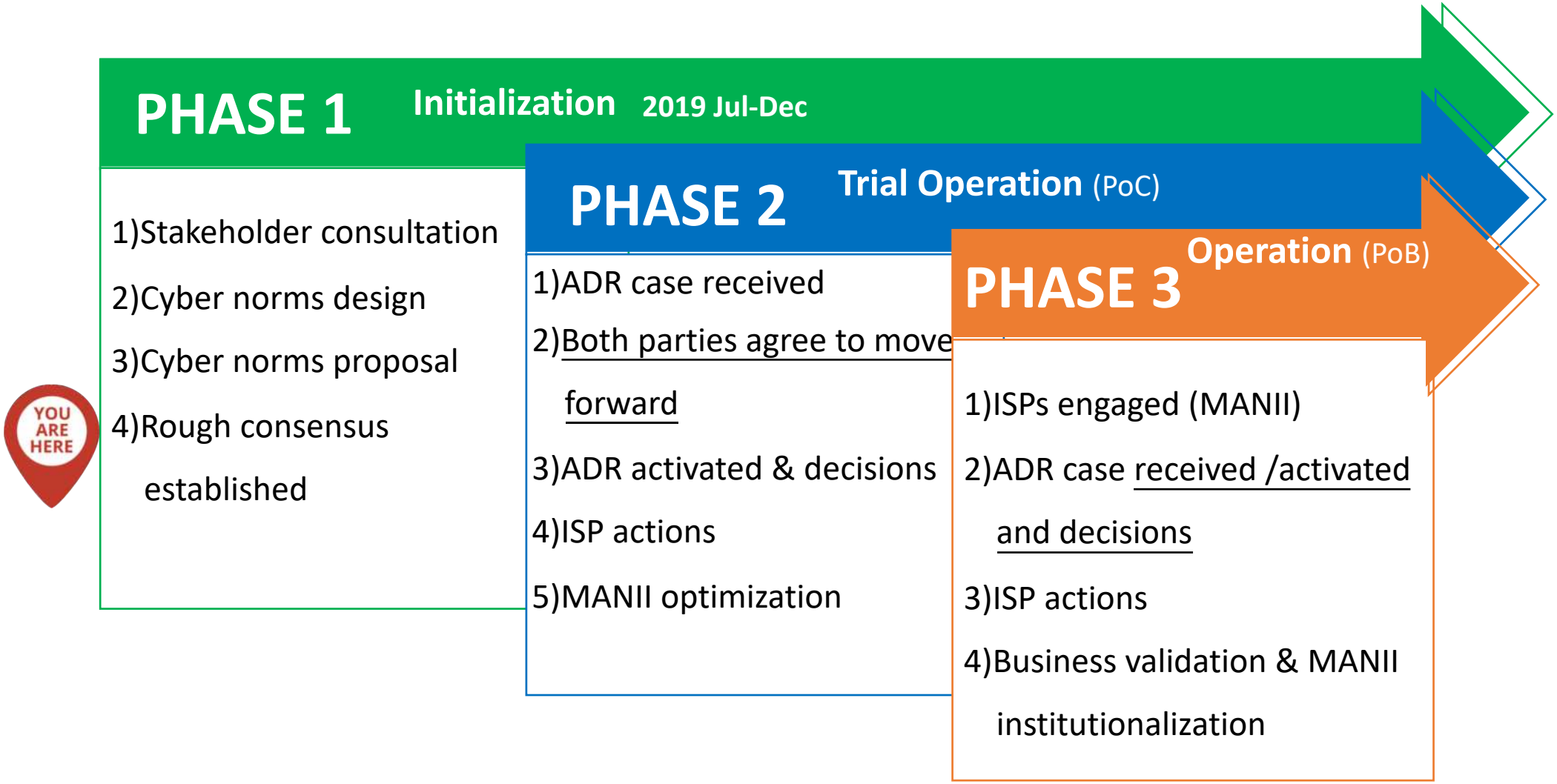
Alternative Dispute Resolution (ADR) is a collective term for processes such as mediation, arbitration, and expert determination. These processes enable parties to resolve their disputes without the need for litigation.

Court action can often take considerable time, so finding a solution using ADR may be more efficient for both parties.

Simplified MANII (ADR) Process



Phased Approach



Source: Dr. Kenny Huang (2019 Dec 06)

Mutually Agreed Norms for Internet Intermediary

MANII provides baseline recommendations in the form of actions

- Distilled from common behaviors – BCPs, optimized for low cost and low risk of deployment for mitigating copyright infringement
- With high potential of becoming norms for mitigating copyright infringement

MANII builds a visible community of accountable operators in anti-piracy

- Social acceptance and peer pressure

MANII for Network Operators (Phase 2)

Participate

Joint initial review of submitted compliant

ISPs participate MANII process: When applicant submit a compliant, ISPs can join initial review and determine further engagement of the dispute resolution

Select

Select Expert Panel for dispute resolution

When ISP join a complaint, ISP has the right to select one of preferred expert from an expert list.

Deliberate

Deliberate decision from expert panel

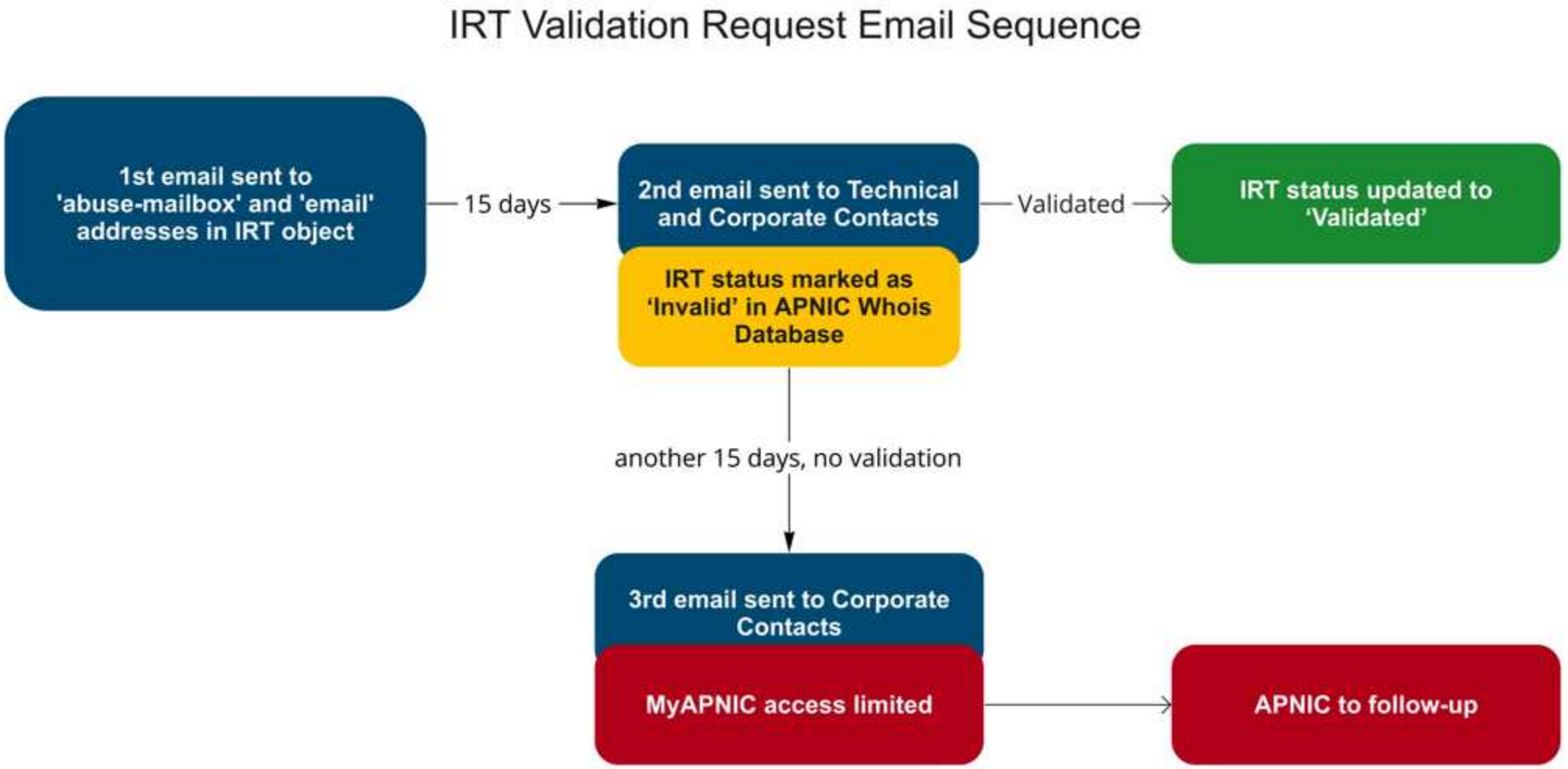
When a decision was made by the expert panel. ISP remains the right for review and deliberate the decision.

Action

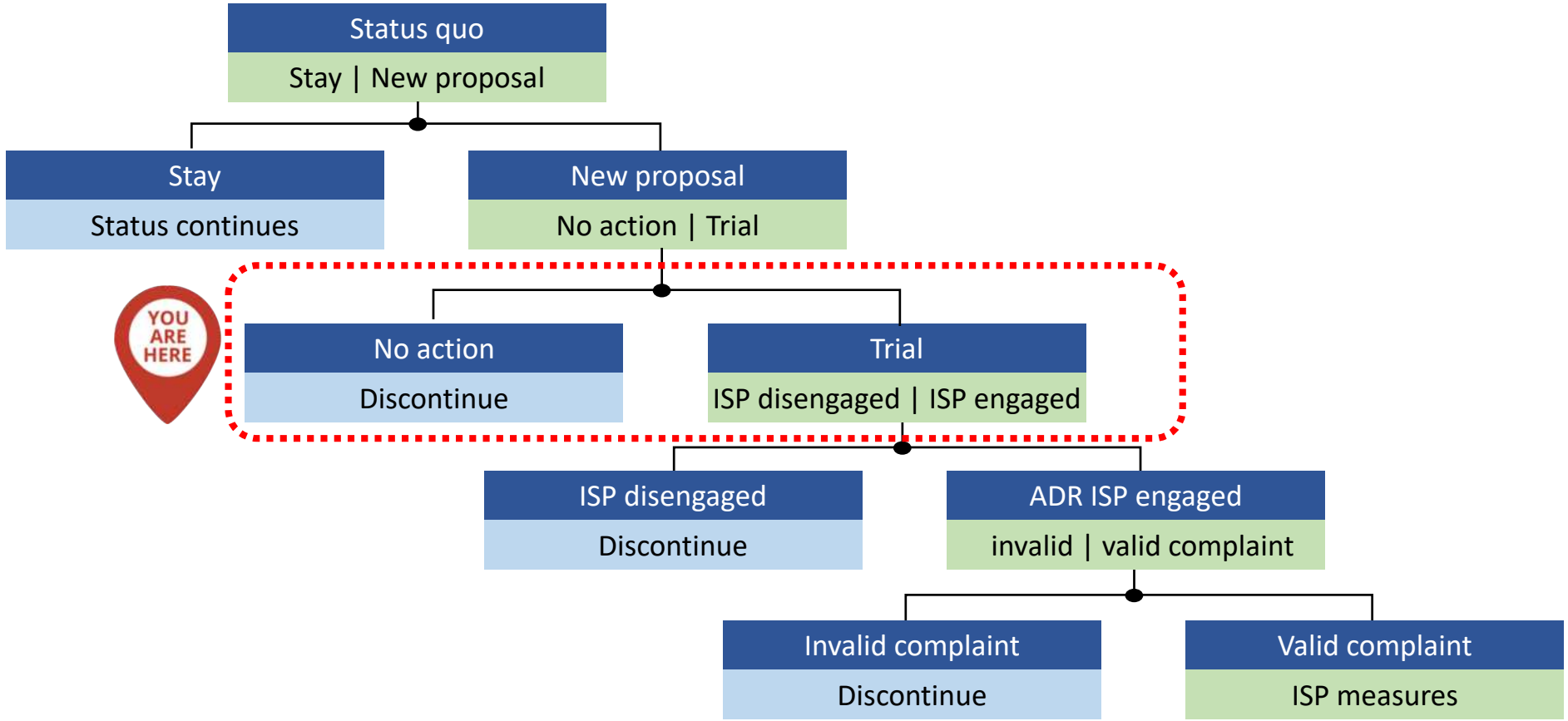
Implement decision from expert panel

When a decision conclude a valid copyright infringement from the identified IP/DN. ISP should take required actions of site blocking.

APNIC/TWNIC IRT validation policy



Decision Tree



Technology Overview

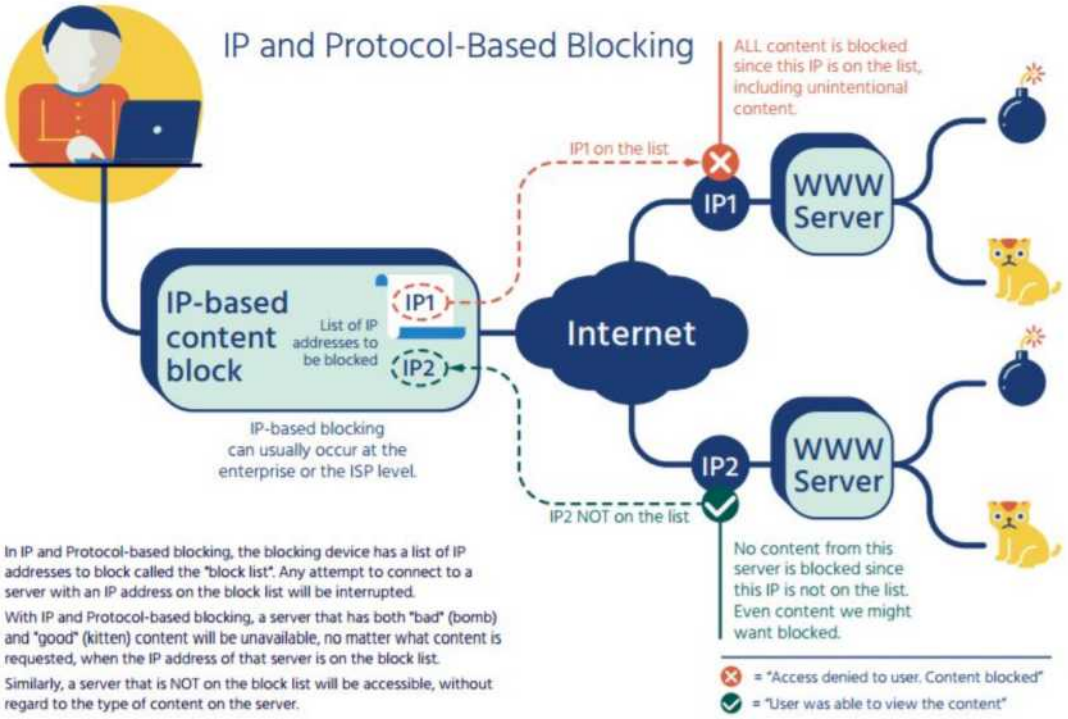
	IP-based Blocking	DNS-based Blocking	DPI-based Blocking (URL)
Overview	A device is inserted in the network that blocks based on IP address and application	At ISP level, DNS traffic is funneled to a modified DNS server that can block lookups of certain domain names	A device is inserted in the network that blocks based on content (e.g., URL)
Is it effective?	IP addresses are easily changed, this technique works poorly	It is effective when significant amount of content should be blocked. Over-blocking makes it an ineffective technique.	It works well when blocking access to entire categories of information. The technique is very ineffective in the face of encryption.
Collateral damage	Any targeting of larger servers has a huge false positive rate	Any targeting of domain names used by larger servers has a huge false positive rate	URL blocking can be quite specific
Common ways to evade it	Change IP addresses, CDN, VPN	Application encryption effectively evade this type of blocking	Avoid DNS lookups, e.g., VPN, Apps, STB

Source: Internet Society; edited by Dr. Kenny Huang

IP-based Blocking

Architecture

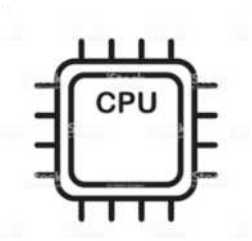
IP route 101.101.101.101/32 Null0



Increased Resource Consumption

0.0% per IP address

Memory

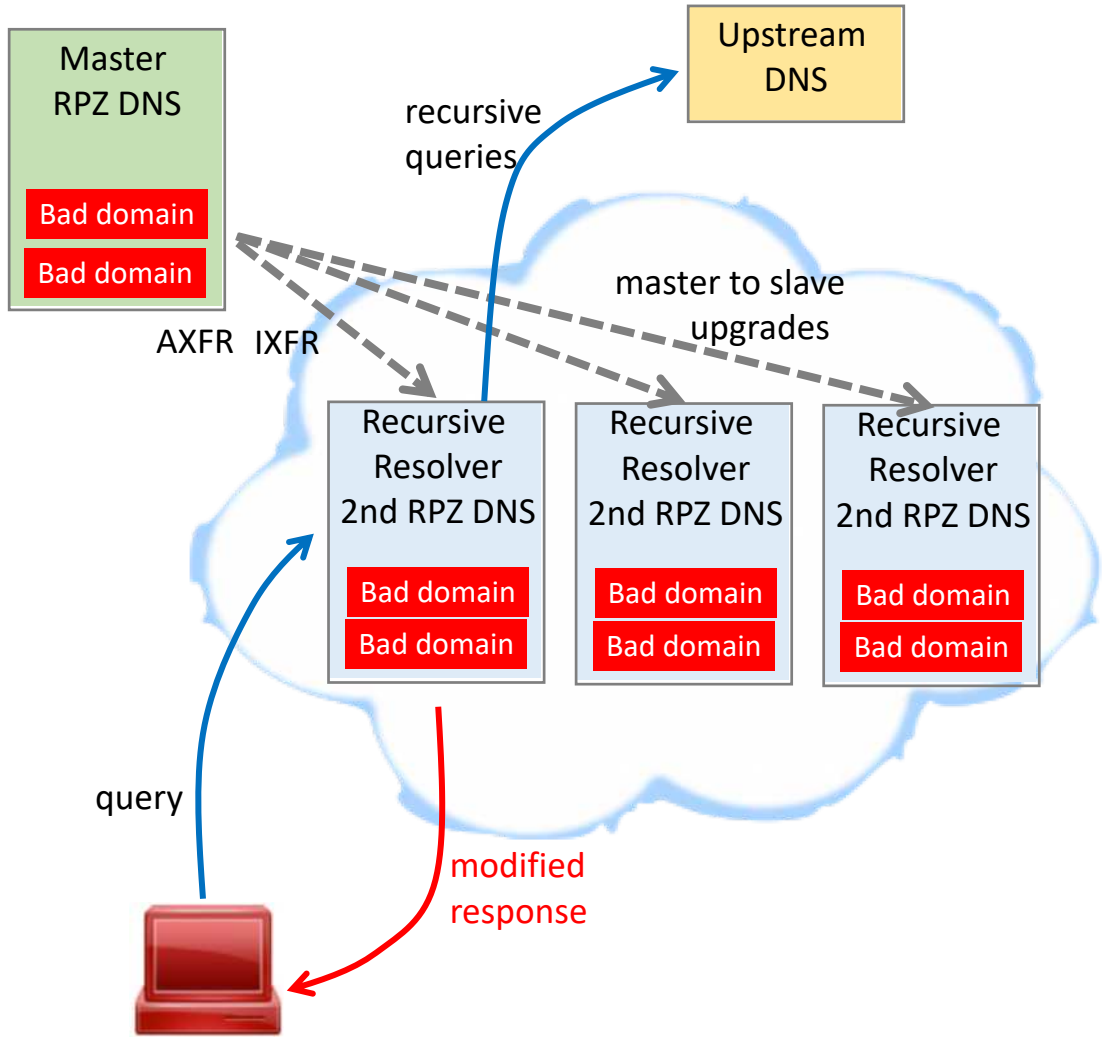


0.0% per IP address

CPU

DNS-based Blocking

Architecture

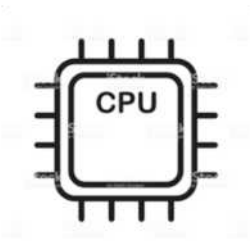


Increased Resource Consumption

Memory

0.0%

1,000 domains



CPU

0.0%

1,000 domains


Q
A