3 POLICY PROGRAMS

DATA & JURISDICTION PROGRAM

CONTENT & JURISDICTION PROGRAM

**DOMAINS** & JURISDICTION PROGRAM

Cross-border access to **electronic evidence**

Cross-border **content moderation** & **restrictions**

Cross-border **DNS-level action** to address abuses

INTERNET &
JURISDICTION
POLICY NETWORK

- A great diversity of types of abuses

- A transnational problem

- Complexity - need to understand the functioning of the internet

- Lack of tools, competences, and resources

- A problem for all actors: governments, businesses, users
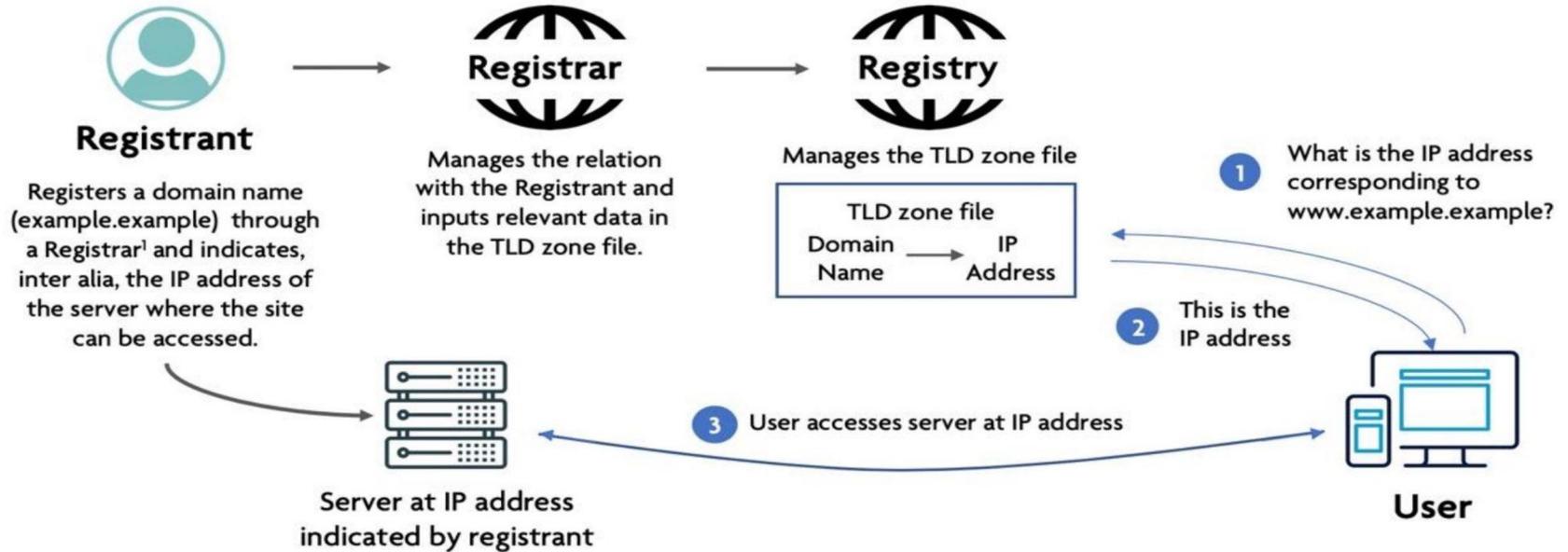
**Source**: I&JPN EFFECTS OF ACTIONS AT THE DNS LEVEL

The TLD zone file is edited to assign a different IP address to the domain name

REDIRECT

TLD zone file

Domain Name ✗ → IP Address
↳ → **IP Address 2**

Registrant

Server at IP address 2

1. What is the IP address corresponding to www.example.example?

2. This is the **IP address 2**

3. User is directed to server at IP Address 2

User
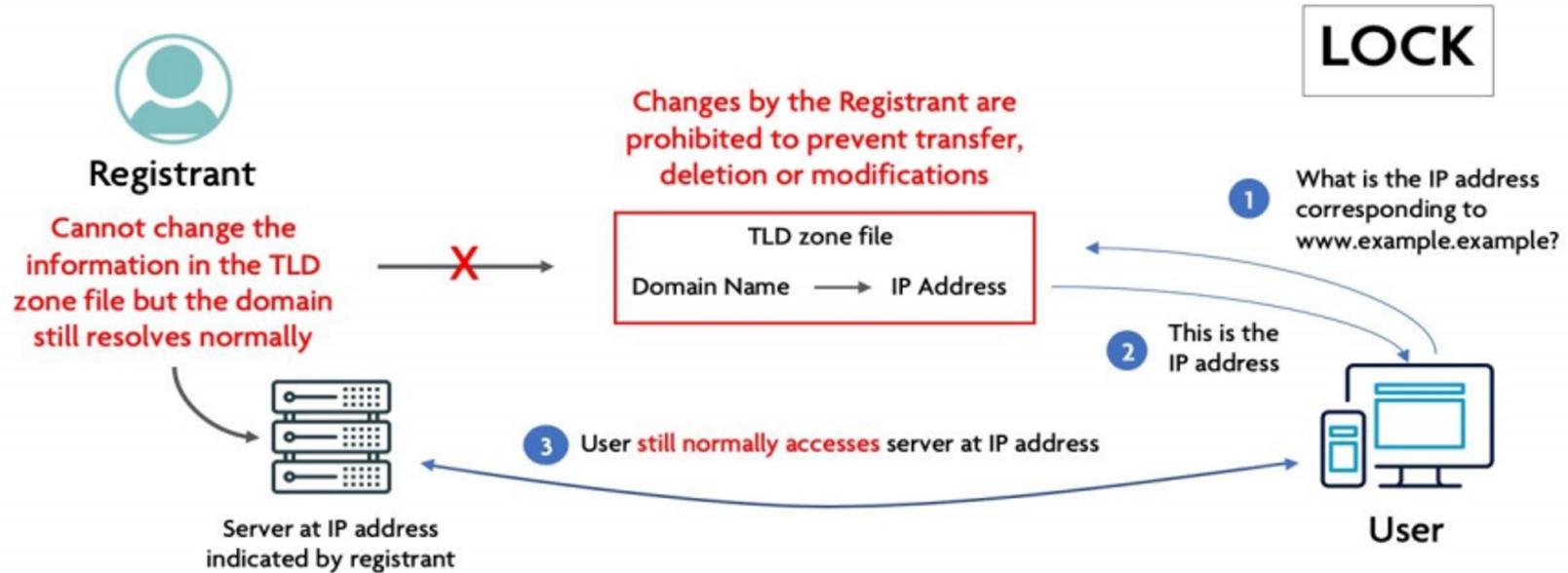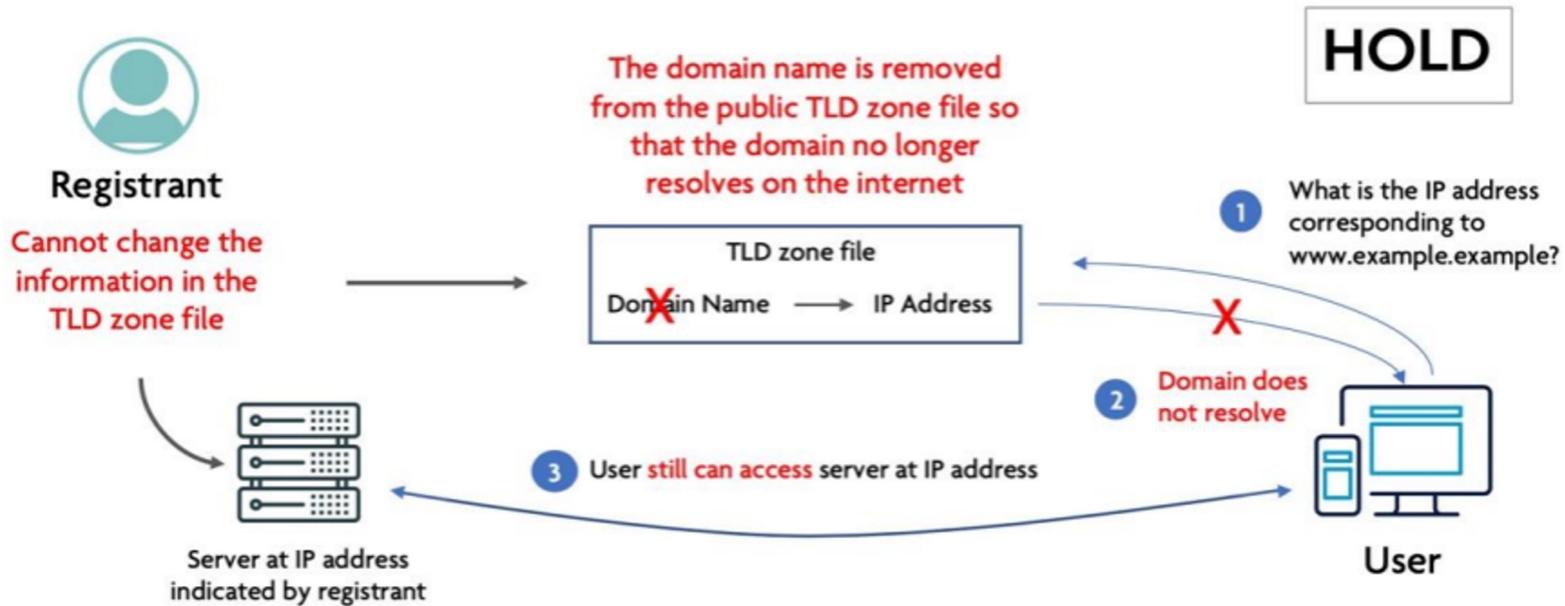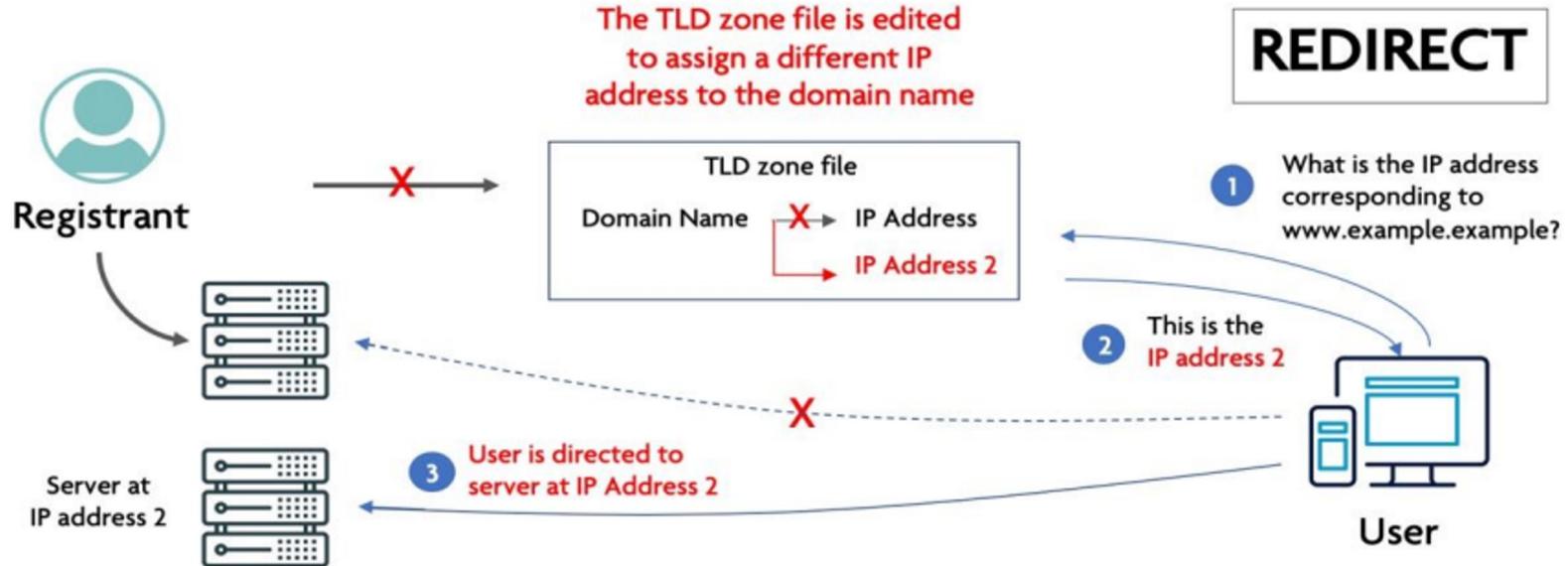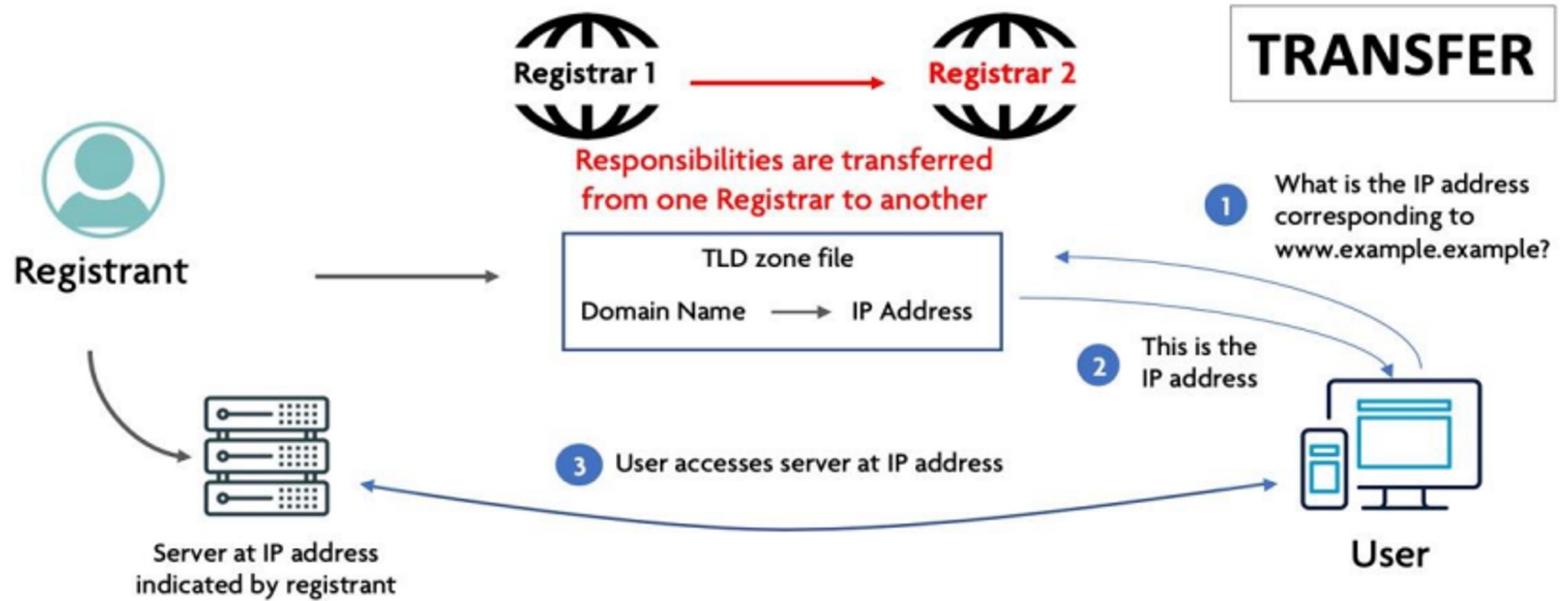
- A blunt instrument with collateral effects

- Global impact

- Partly efficient (still access through IP address)

- Part of a larger ecosystem of actors (escalation path)

- Limited obligations in operators' accreditation agreements

INTERNET &
JURISDICTION
POLICY NETWORK

- Numerous sessions for several years around **"DNS Abuse"**

- Mutual criticism between constituencies and tensions within them

- Lingering sense of frustration

No good answer to a bad question => Reframe

INTERNET & JURISDICTION
POLICY NETWORK

The real question:

When is it appropriate to act at the DNS level to address abuses online?

Defining DNS Abuse:

Malware

Botnets

Phishing

Pharming

Spam (as delivery tool)

I&JPN Operational
Approaches

**DOMAINS
& JURISDICTION
PROGRAM**

OPERATIONAL APPROACHES
NORMS, CRITERIA, MECHANISMS

04/
2019

Framework
to address Abuse

Framework to Address Abuse

12/
2019

SSAC Report

**SAC 115**

03/
2021

≠ **From content-related abuse**
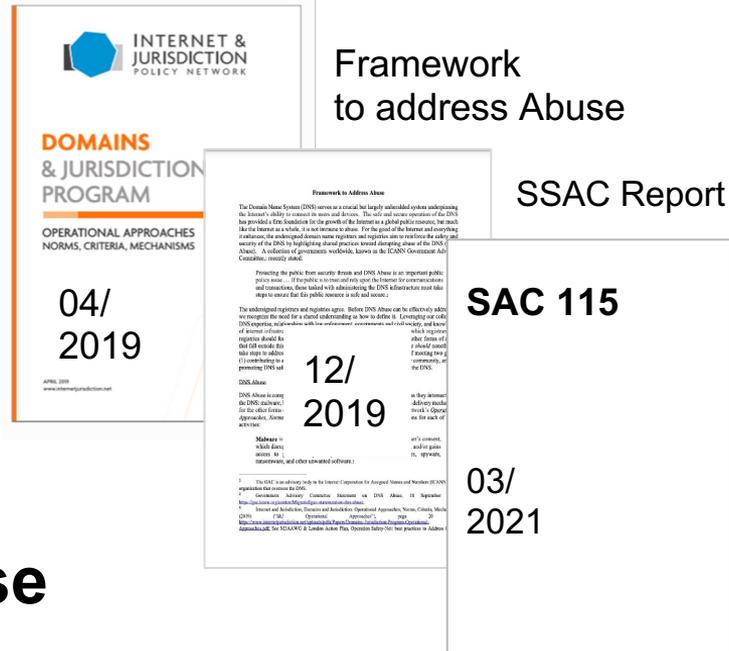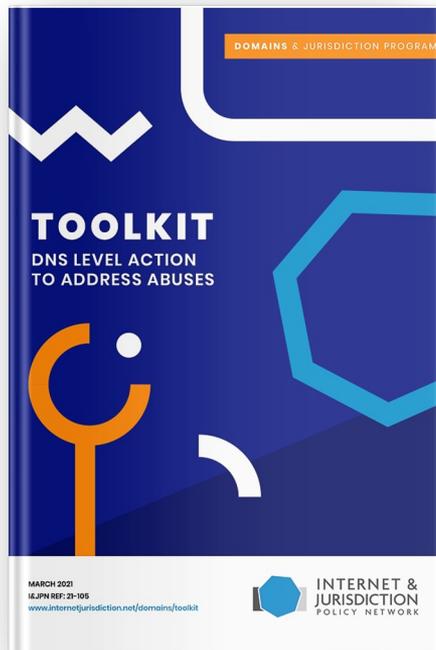
HELPING

- **DNS Operators** in the design of their DNS Abuse related activities.

- **Notifiers** in the detection and reporting of problematic activity.

- **Legislators** and law enforcement to determine procedures for dealing with different types of abuse.

GENERAL WORKFLOW

INTERNET &
JURISDICTION
POLICY NETWORK

IDENTIFICATION
> TYPES OF ABUSES
> DUE DILIGENCE BY NOTIFIERS
> NOTIFICATION OF REGISTRANTS

EVALUATION
> THRESHOLD CRITERIA

CHOICE OF ACTION
> TYPES OF ACTION
> EFFECTS OF ACTION AT THE DNS LEVEL

RECOURSE
> RECOURSE FOR REGISTRANTS
> TRANSPARENCY

DNS ABUSE – GUIDANCES

Notice Components

Typology of Notifiers

Due Diligence Guide for Notifiers

Trusted Notifiers Framework

Fighting Botnets (AGDs)

Phishing/Malware Workflow

DNS ABUSE

Acting at the DNS level is **generally justified** in situations of technical abuse in order to protect the stability and security of the global infrastructure of the internet. Specific additional measures are nonetheless justified to assist the registrant if the domain is obviously compromised by third parties without his/her knowledge.

CONTENT-RELATED ABUSE

On the other hand, given the geographically global impact of an action at the DNS level, doing so regarding abusive content can **only be justified if** a particularly high threshold of abuse/harm is met, regarding inter alia:

1. The degree of **global normative consistency** regarding the alleged abuse: i.e. whether the content at issue is considered illegal across a sufficient number of jurisdictions;
2. The **proportion of the site** effectively dedicated to the infringing content;
3. The manifest **intended purpose or bad faith** of the registrant, and
4. The lack of available alternative measures to remediate the situation.

- **Escalation path** via other actors first: site operator, registrant, hosting provider;

- Triggering **threshold criteria** for exceptions;

- **Reachability** (to site operator, to registrant, or hosting provider)

- Trusted Notifiers **Agreements**

=> Shared Responsibility (tbd)

All I&JPN Domains Program Outcomes:

https://www.internetjurisdiction.net/news/domains-jurisdiction-program-outcomes

Effects of Action at the DNS Level:

https://www.internetjurisdiction.net/uploads/pdfs/Internet-Jurisdiction-Policy-Network-20-101-Effects-Action-DNS.pdf

I&JPN Operational Approaches - Domains Program:

https://www.internetjurisdiction.net/uploads/pdfs/Papers/Domains-Jurisdiction-Program-Operational-Approaches.pdf

SSAC Report 115:

https://www.icann.org/en/system/files/files/sac-115-en.pdf

Framework to address Abuse:

https://www.dnsabuseframework.org/media/files/2020-05-29_DNSAbuseFramework.pdf

DNS Abuse Institute:

https://dnsabuseinstitute.org/

NetBeacon:

https://netbeacon.org
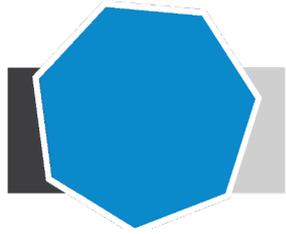
INTERNET &
JURISDICTION
POLICY NETWORK

DOMAINS &
JURISDICTION
PROGRAM

THANK YOU

Bertrand de LA CHAPELLE - Executive Director
bdelachapelle@internetjurisdiction.net

Ajith FRANCIS - Policy Programs Director
francis@internetjurisdiction.net