

INTERNET &
JURISDICTION
POLICY NETWORK

ACTION AT THE DNS LEVEL TO ADDRESS ABUSES: IS IT APPROPRIATE?

Bertrand de LA CHAPELLE
Executive Director, I&JPN



EURALO presentation
February 23rd, 2021

Action at the **DNS** level to address **abuses** - is it **appropriate**?

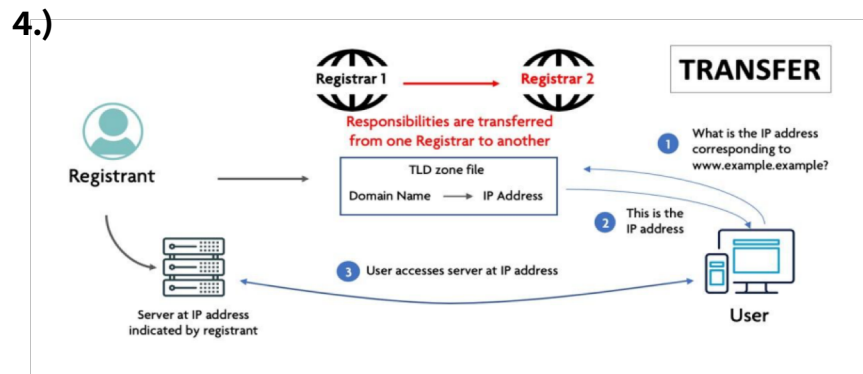
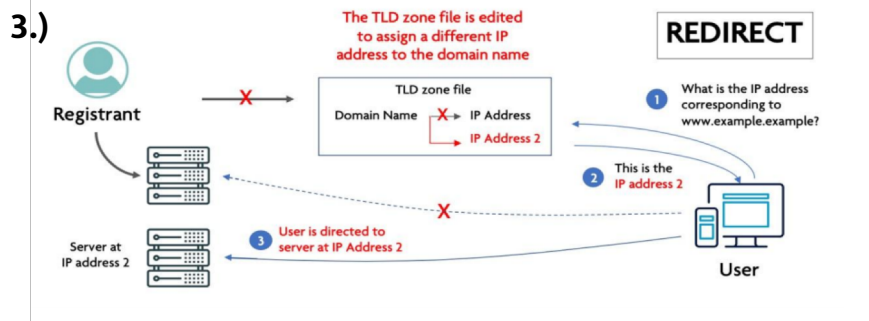
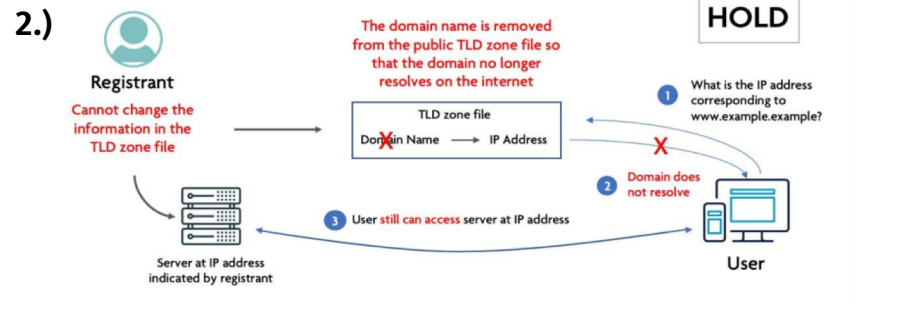
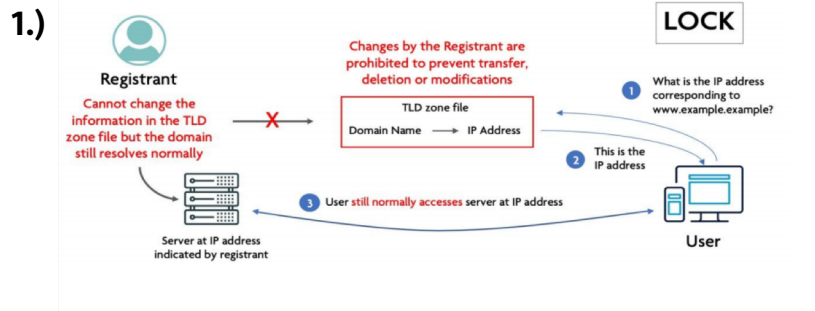
- The **DNS** is a technical infrastructure (address book)
- **Abuses** online: the internet is not a Garden of Eden (mirror of behaviors in human society – real harm)
- **Appropriateness**: a polarized debate (magic switchboard vs. « not my problem »)

- Different types of abuses (simplified distinction: **technical and content-related abuses**)
- « **DNS abuse** » is a misleading expression
- What matters is:
 - when is it appropriate to **act at the DNS level?**
 - **who** should make the decision and **how** (roles and responsibilities)?

Appropriate means both:

- **Effective:**
 - blunt tools (global, collateral effects)
 - often only partial solution (lack of awareness by actors of the actual results of DNS-level actions)
- **Legitimate:**
 - thresholds to justify such global action (different for technical abuses and content-related ones)

EFFECTS OF ACTION AT THE DNS LEVEL



5.) **DELETE**

Access here: <https://www.internetjurisdiction.net/news/i-j-educational-resource-raises-awareness-of-the-effects-of-actions-at-the-dns-level>

- **Technical abuses:**
 - if manifest, with special care for compromised sites
- **Content-related abuses** - very high threshold regarding:
 - degree of international normative consistency
 - proportion of site effectively dedicated to the infringing content
 - registrant's manifest intended purpose or bad faith
 - lack of available alternative measures

- **There are indeed situations** where action at the DNS level is both efficient and legitimate
- More frequent for **technical abuse** (objective criteria, connection to the stability and security of the system)
- Harder for **content-related issues** (normative diversity, subjective appreciation) => rather hosting providers

- **Multiplicity and diversity** of DNS operators (ccTLDs vs. gTLDs, Ry vs Rr) with very different attitudes and willingness or ability (size, resources) to act
- **ICANN** (mandate, PDP, lack of consensus)
- Complex **ecosystem** (LEAs, notifiers, registries, registrars)
- 4 key stages in the **workflow**:
 - identification, evaluation, choice of action, recourse

Enable stakeholders to **collaboratively address**
the transnational policy challenges
of the digital 21st century.

Concretely, provide **a safe space** for willing actors to
identify how to improve their interactions
in the respect of due process.

3 POLICY PROGRAMS



DATA & JURISDICTION PROGRAM

Cross-border access
to **electronic evidence**



CONTENT & JURISDICTION PROGRAM

Cross-border **content
moderation & restrictions**

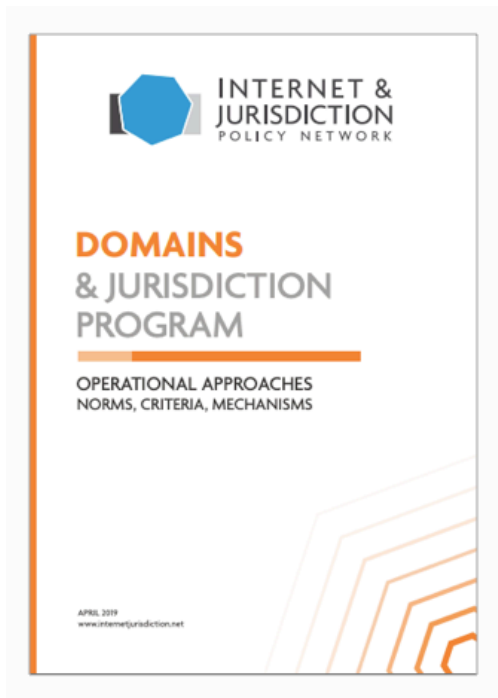


DOMAINS & JURISDICTION PROGRAM

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

Allowing stakeholders to develop **voluntary policy standards**

DOMAINS & JURISDICTION PROGRAM



- **Contact Group** since 2017 (Coordinator)
- **Operational Approaches** in 2019 (norms, criteria and mechanism)
- This year, **6 very concrete outcomes**, with a focus on technical abuse
- To be packaged in a **Toolkit** (launched on March 18)

SIX 2020 PROGRAM OUTCOMES

DNS OPERATOR DECISION-MAKING GUIDE TO ADDRESS TECHNICAL ABUSE

INTERNET & JURISDICTION POLICY NETWORK

REF ID: A10-1001 | 10/2020

This guide is intended to provide a systematic, structured decision-making process to assist the ability and security of the global infrastructure of the Internet. DNS operators use a variety of policies and technical measures to identify, respond and prevent unwanted abuse. This document provides a framework for a decision-making process to assist operators in making a decision on how to respond to unwanted abuse. It is not intended to be a substitute for the policies and procedures of the operator.

A general approach to addressing technical abuse can be broken down into the following steps:

- Identification of whether the alleged technical abuse poses the identified risk
- Identification of the policy or policies that apply to the alleged technical abuse
- Technical actions to more effectively and efficiently address the abuse

The guide includes a set of decision questions for DNS operators to use in each step to determine a course of action to address technical abuse in a variety of ways.

IDENTIFICATION AND NOTIFICATION	EVALUATION OF ABUSE
<p>IDENTIFICATION AND NOTIFICATION</p> <ul style="list-style-type: none"> • Is the abuse within the DNS Operator's control? • Does the abuse impact Internet access? • Does the abuse consist of a necessary component for identifying abuse and taking action, or is it necessary to identify abuse and take action? • Does the abuse consist of a necessary component for identifying abuse and take action? • Does the abuse consist of a necessary component for identifying abuse and take action? 	<p>EVALUATION OF ABUSE</p> <ul style="list-style-type: none"> • Is the abuse a violation of the DNS Operator's policy? • Does the abuse pose a risk to the DNS Operator's ability to provide Internet access? • Does the abuse pose a risk to the DNS Operator's ability to provide Internet access? • Does the abuse pose a risk to the DNS Operator's ability to provide Internet access? • Does the abuse pose a risk to the DNS Operator's ability to provide Internet access?

INTERNET & JURISDICTION PROGRAM | WWW.INTERNETANDJURISDICTION.NET/OUTCOMES

DNS Operator Decision-making Guide to Address Technical Abuse

CHANNELS/SOURCES/TYPOLGY OF TECHNICAL ABUSE NOTIFIERS

INTERNET & JURISDICTION POLICY NETWORK

REF ID: A10-1002 | 10/2020

DNS Operators receive technical abuse notifications. There are a variety of sources, channels, and typologies of technical abuse. This document provides a typology of technical abuse notifiers. It is intended to assist operators in identifying technical abuse notifiers and possible actions to be taken. The document also provides a typology of technical abuse notifiers and possible actions to be taken. The document also provides a typology of technical abuse notifiers and possible actions to be taken.

TYPOLGY	SOURCES
Government, Regional, Provider	<ul style="list-style-type: none"> • Law enforcement • Law enforcement • Law enforcement • Law enforcement • Law enforcement
DNS Infrastructure Provider	<ul style="list-style-type: none"> • Registrar and registrar • Registrar and registrar • Registrar and registrar • Registrar and registrar • Registrar and registrar
Government Bodies	<ul style="list-style-type: none"> • Registrar and registrar • Registrar and registrar • Registrar and registrar • Registrar and registrar • Registrar and registrar
Non-government entities	<ul style="list-style-type: none"> • Registrar and registrar • Registrar and registrar • Registrar and registrar • Registrar and registrar • Registrar and registrar
Media	<ul style="list-style-type: none"> • Registrar and registrar • Registrar and registrar • Registrar and registrar • Registrar and registrar • Registrar and registrar

INTERNET & JURISDICTION PROGRAM | WWW.INTERNETANDJURISDICTION.NET/OUTCOMES

Channels / Sources/ Typology of Technical Abuse Notifiers

DNS TECHNICAL ABUSE: CHOICE OF ACTION

INTERNET & JURISDICTION POLICY NETWORK

REF ID: A10-1003 | 10/2020

This document provides a choice of action to address technical abuse. It is intended to assist operators in identifying technical abuse and taking action. The document also provides a choice of action to address technical abuse and taking action. The document also provides a choice of action to address technical abuse and taking action.

When evaluating a technical abuse that is identified through a notification, the operator should consider the following factors:

- The nature of the abuse
- The impact of the abuse
- The operator's ability to address the abuse
- The operator's ability to address the abuse
- The operator's ability to address the abuse

The choice between a choice of action to address technical abuse and taking action is based on the operator's ability to address the abuse and taking action. The choice between a choice of action to address technical abuse and taking action is based on the operator's ability to address the abuse and taking action.

INTERNET & JURISDICTION PROGRAM | WWW.INTERNETANDJURISDICTION.NET/OUTCOMES

DNS Technical Abuse: Choice of Action

MINIMUM NOTICE COMPONENTS FOR TECHNICAL ABUSE

INTERNET & JURISDICTION POLICY NETWORK

REF ID: A10-1004 | 10/2020

This document provides a minimum notice components for technical abuse. It is intended to assist operators in identifying technical abuse and taking action. The document also provides a minimum notice components for technical abuse and taking action. The document also provides a minimum notice components for technical abuse and taking action.

IDENTIFICATION	NOTIFICATION
<p>IDENTIFICATION</p> <ul style="list-style-type: none"> • Is the abuse within the DNS Operator's control? • Does the abuse impact Internet access? • Does the abuse consist of a necessary component for identifying abuse and taking action, or is it necessary to identify abuse and take action? • Does the abuse consist of a necessary component for identifying abuse and take action? • Does the abuse consist of a necessary component for identifying abuse and take action? 	<p>NOTIFICATION</p> <ul style="list-style-type: none"> • Is the operator's ability to address the abuse? • Is the operator's ability to address the abuse? • Is the operator's ability to address the abuse? • Is the operator's ability to address the abuse? • Is the operator's ability to address the abuse?

INTERNET & JURISDICTION PROGRAM | WWW.INTERNETANDJURISDICTION.NET/OUTCOMES

Minimum Notice Components for Technical Abuse

DNS LEVEL ACTION TO ADDRESS TECHNICAL ABUSE: DUE DILIGENCE GUIDE FOR NOTIFIERS

INTERNET & JURISDICTION POLICY NETWORK

REF ID: A10-1005 | 10/2020

This document provides a due diligence guide for notifiers. It is intended to assist operators in identifying technical abuse and taking action. The document also provides a due diligence guide for notifiers and taking action. The document also provides a due diligence guide for notifiers and taking action.

The following questions will help notifiers identify potential abuse:

- What is the nature of the abuse?
- What is the impact of the abuse?
- What is the operator's ability to address the abuse?
- What is the operator's ability to address the abuse?
- What is the operator's ability to address the abuse?

INTERNET & JURISDICTION PROGRAM | WWW.INTERNETANDJURISDICTION.NET/OUTCOMES

DNS Level Action to Address Technical Abuse: Due Diligence Guide for Notifiers

ADDRESSING PHISHING AND MALWARE: A PROCEDURAL WORKFLOW

INTERNET & JURISDICTION POLICY NETWORK

REF ID: A10-1006 | 10/2020

This document provides a procedural workflow for addressing phishing and malware. It is intended to assist operators in identifying technical abuse and taking action. The document also provides a procedural workflow for addressing phishing and malware and taking action. The document also provides a procedural workflow for addressing phishing and malware and taking action.

INTERNET & JURISDICTION PROGRAM | WWW.INTERNETANDJURISDICTION.NET/OUTCOMES

Addressing Phishing and Malware: A Procedural Workflow

THANK YOU

Contact us if you are interested by the launch of the toolkits

Elizabeth BEHSUDI is the Domains Program Director

<https://www.internetjurisdiction.net/work/domains-jurisdiction>