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

SOME BASIC POINTS

Action at the DNS level to adress 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 »)

SOME NUANCE TO FRAME THE DEBATE

- 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)?

APPROPRIATENESS

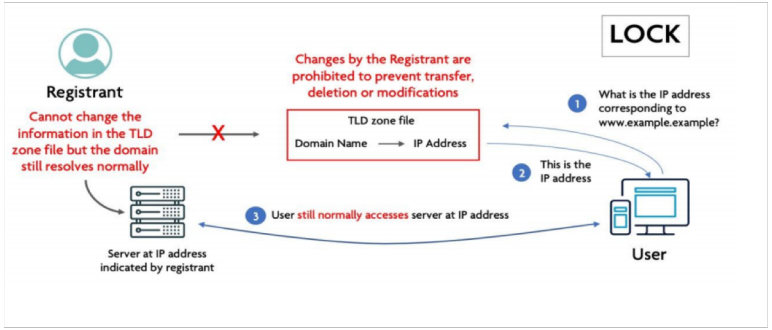
Appropriate means both:

- Effective:
  - blunt tools (global, collateral effects)
  - often only partial solution (lack of awareness by actors of the actual results of DNS-level actions)

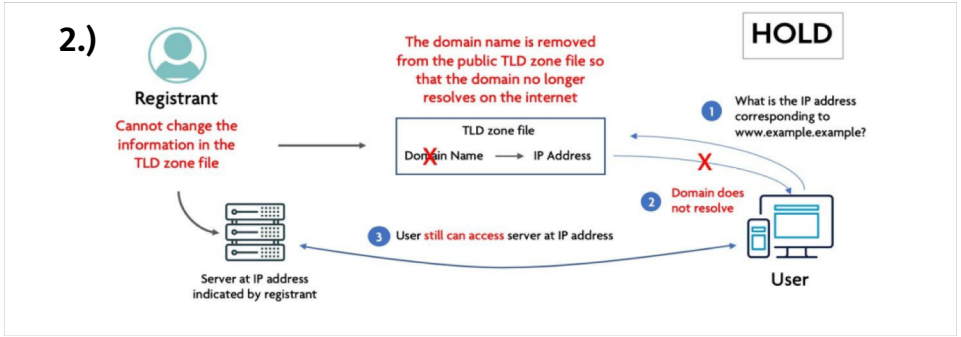
- Legitimate:
  - thresholds to justify such global action (different for technical abuses and content-related ones)

EFFECTS OF ACTION AT THE DNS LEVEL

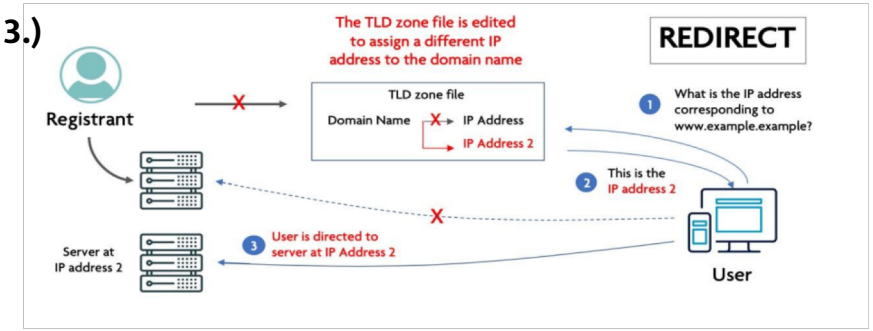
1.)



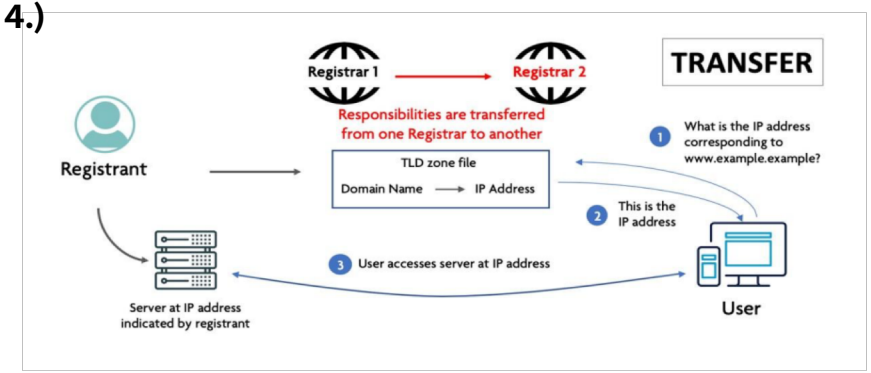
2.)



3.)



4.)



5.) **DELETE**

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

INTERNET & JURISDICTION POLICY NETWORK

THRESHOLDS

- Technical abuses:
  - if manifest, with special care for compromized 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

Source: I&JPN – Operational Approaches (2019)

BOTTOM LINE

- 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

ROLES AND RESPONSIBILITIES

- 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

I&J VISION

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.

INTERNET & JURISDICTION POLICY NETWORK

ADVANCE SOLUTIONS

3 POLICY PROGRAMS

DATA & JURISDICTION PROGRAM

Cross-border access to electronic evidence

CONTENT & JURISDICTION PROGRAM

Cross-border content moderation & restrictions

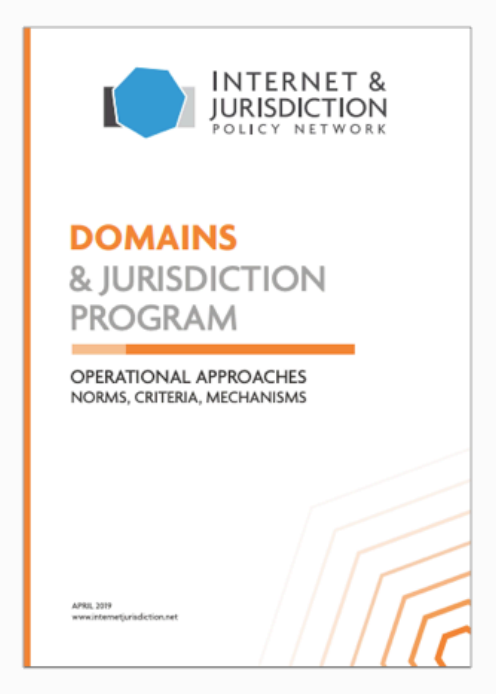
DOMAINS & JURISDICTION PROGRAM

Cross-border DNS-level action to address abuses

Allowing stakeholders to develop voluntary policy standards

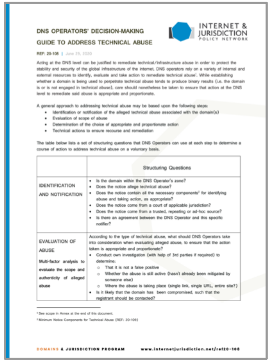
INTERNET & JURISDICTION POLICY NETWORK

DOMAINS & JURISDICTION PROGRAM

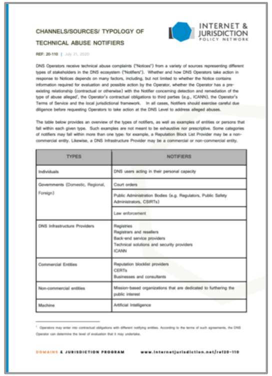


- Contact Group since 2017 (Coordinator)
- Operational Approaches in 2019 (norms, criteria and mechanism)
- This year, 6 very concrete outcomes, with a focus on technical abuse
- To be packaged in a Toolkit (launched on March 18)

SIX 2020 PROGRAM OUTCOMES


DNS OPERATORS' DECISION-MAKING GUIDE TO ADDRESS TECHNICAL ABUSE

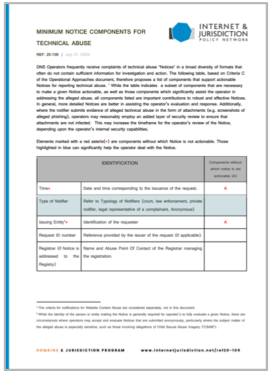
DNS Operator Decision-making Guide to Address Technical Abuse


CHANNELS/SOURCES/ TYPOLOGY OF TECHNICAL ABUSE NOTIFIERS

Channels / Sources/ Typology of Technical of Technical Abuse Notifiers


DNS TECHNICAL ABUSE : CHOICE OF ACTION

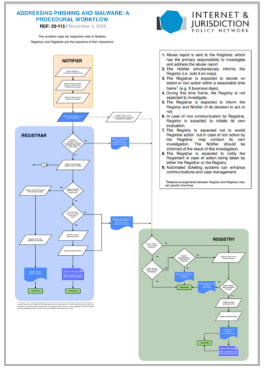
DNS Technical Abuse: Choice of Action


MINIMUM NOTICE COMPONENTS FOR TECHNICAL ABUSE

Minimum Notice Components for Technical Abuse


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

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



Addressing Phishing and Malware: A Procedural Workflow

INTERNET & JURISDICTION POLICY NETWORK

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