DOMAINS & JURISDICTION PROGRAM

TOOLKIT

DNS LEVEL ACTION TO ADDRESS ABUSES

MARCH 2021
I&JPN REF: 21-105
www.internetjurisdiction.net/domains/toolkit

INTERNET & JURISDICTION POLICY NETWORK

The Internet & Jurisdiction Policy Network is the multistakeholder organization fostering legal interoperability in cyberspace. Its stakeholders work together to preserve the cross-border nature of the internet, protect human rights, fight abuses, and enable the global digital economy. Since 2012, the Internet & Jurisdiction Policy Network has engaged more than 400 key entities from six stakeholder groups around the world including: governments, the world's largest internet companies, the technical community, civil society groups, leading universities and international organizations.

DESIGN & LAYOUT
João Pascoal Studio
www.joaopascoal.com

CITATION
Internet & Jurisdicion Policy Network Toolkit
DNS Level Action to Address Abuses (2021)

TABLE OF CONTENTS

1. ISSUE FRAMING

Cross-border requests for domain name suspensions are increasingly sent to Domain Name System (DNS) Operators in relation to alleged abusive content or activity on underlying websites.

Yet, the DNS, as an addressing system, is a neutral technical layer vital for the proper functioning of the internet. This level is neither a fully effective way - nor should be considered as the natural tool - to address abusive content. Protection of the core of the internet is and should be a key priority.

Acting at the DNS level should only be considered when it can be reliably determined that a domain is used with a clear intent of significant abusive conduct. Furthermore, because a domain suspension has by definition a global impact, the concept of proportionality dictates that only a particularly high level of abuse and/or harm could potentially justify resorting to such a measure. It is also important that the actual impact of specific actions at the DNS level is well understood by all actors.

This important issue is generally recognized as outside of the Internet Corporation for Assigned Names and Numbers (ICANN) mandate. Moreover, the fundamental distinction between generic and country-code Top Level Domains (gTLDs and ccTLDs) in terms of relations with, respectively, ICANN and national laws or authorities, leads to very different approaches and constraints.

All actors are nonetheless confronted with a common challenge: defining when it is appropriate to act at the DNS level in relation to the content or behavior under a domain address, and what role courts and so-called "notifiers" should or could respectively play in that regard.

The Domain Name System (DNS), as the "phonebook of the internet", saves internet users the burden of memorizing Internet Protocol (IP) addresses. Thanks to the DNS, information can more easily be accessed online through domain names, for example: nytimes.com or lemonde.fr.

Importantly, the DNS exists and operates independently from the underlying websites or services where or through which abuses happen. Addressing abuses on the internet should not have negative impacts on the integrity and reliability of this essential infrastructure layer upon which internet use relies.

In that regard, it is critical to distinguish two categories:

1.) **Technical abuse** (*e.g.* phishing, malware distribution, etc.), which is closely related to the security and stability of the technical layer of the internet; and
2.) **Website content abuse** (*e.g.* child sexual abuse imagery, intellectual property violations, etc.) which occur at the level of the website.

Accordingly, what is often labelled as "addressing DNS abuse", should rather be understood as: "DNS level action to address abuses online".

DNS Level Action to Address Abuses

DNS Operators (registries and registrars - the entities that manage domain names) have limited technical options at their disposal to address abuses, which do not include the capacity of removing specific slices of content from websites. Moreover, when a DNS Operator takes action to disable a domain name, the underlying website and its content remain available through the website's IP address. These technical limitations coupled with the complex interplay of competing legal systems in varying jurisdictions often differ as to whether particular forms of content are legal or illegal. Therefore caution should be taken when tasking DNS Operators with acting as the arbiters of permissible content on the internet.

Registries and Registrars are very diverse in terms of size, activities and governance structures. Moreover, the fundamental distinction between generic and country-code Top Level Domains (gTLDs and ccTLDs) in terms of relation with national laws and authorities, leads to very different approaches and constraints when receiving direct requests or orders for action at the DNS level regarding abuses online, particularly when they originate across borders. In the absence of a generally accepted framework regarding how to deal with abuse, DNS Operators' practices vary considerably.

Therefore, defining when it is appropriate to act at the DNS level to address abuses requires communication between all stakeholders to help them understand each other's situation, concerns and intentions; agreed norms of behavior to foster informal or structured coordination; and processes to develop practical cooperation mechanisms.

The Domains & Jurisdiction Program Contact Group, consisting of experts from governments, internet companies, technical operators, civil society, leading universities and international organizations has, over the years, identified the key issues that could structure new models of transnational cross-border action to address DNS abuses.

A common objective of the different actors should be the definition of high substantive and procedural standards regarding:

- Under what strict conditions might interruption of a domain name without consent of the registrant be envisaged/acceptable;
- What actions should/would domain name operators be willing and able to exercise;
- What rules and procedures could help establish or enhance the credibility of notifiers' notifications (for information or action); and
- What possible mechanisms can help improve transparency in such processes?

2. I&JPN METHODOLOGY

The Internet & Jurisdiction Policy Network fosters a new approach to transnational policy-making. Its innovative methodology identifies relevant stakeholders to define common problems and produce solutions to pressing and complex policy challenges. The neutral and replicable approach, structures interactions among diverse policy actors who would normally not have the opportunity to work together on practical and concrete outcomes.

Since 2016 in regular iterations, the Domains & Jurisdiction Program Contact Group engages a selected set of these global policy actors while trying to ensure balanced geographical representation from governments, internet companies, technical operators, civil society, leading universities and international organizations. Using the I&JPN Methodology, Contact Groups have iteratively developed concrete outcomes pertaining to specific facets of DNS-level action to address abuses. Based on this methodology, future Contact Groups will continue to develop specific policy outcomes on focused issues while also addressing emerging challenges.

Meet the Members of the Domains and Jurisdiction Contact Group from 2018 - 2020 here.

The Internet & Jurisdiction Policy Network fosters a new approach to transnational policy-making. Its innovative methodology identifies relevant stakeholders to define common problems and produce solutions to pressing and complex policy challenges.

FRAMING COMMON PROBLEMS

Issues can best be addressed when formulated as problems that stakeholders have in common rather than with one another. As a first step, stakeholders are consulted to develop a shared framing of the issue at hand and build a shared vernacular. This helps develop a common understanding of the policy problem and helps identify key areas for cooperation where stakeholders can work collaboratively to develop practical and operational solutions.

How can the neutrality of the internet's technical layer be preserved when national laws are applied to the Domain Name System?

I&JPN Domains & Jurisdiction Framing Paper (2017)[i]

SETTING COMMON OBJECTIVES

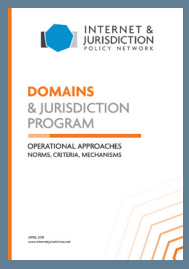
Based on these areas of cooperation, a dedicated Contact Group, guided by a neutral and independent coordinator, identifies key structuring questions that guide discussions among stakeholders and provide a framework within which concrete policy solutions can be developed. These discussions documented as Policy Options define common objectives to ensure better policy coherence and structure further work.

This document aims at providing, in a forward-looking approach, guiding elements to structure further discussion on possible frameworks regarding cross-border DNS-level action to address abuses. It explores the due process dimensions of voluntary regimes envisaged by some DNS operators to deal with domain takedown requests and the potential role of so-called "notifiers".

I&JPN Domains & Jurisdiction Policy Options (2018)[ii]

DEVELOPING COMMON APPROACHES

Based on the objectives identified, intense work in the Contact Group aims to develop scalable, interoperable policy solutions. These can take the form of Operational Norms – to help actors organize their own behavior and mutual interactions; Operational Criteria – to guide actors who develop, evaluate & implement solutions; and Operational Mechanisms – which offer concrete avenues for cooperation.



The work of the dedicated Contact Group of the Internet & Jurisdiction Policy Network aims to contribute to policy discussion by addressing key elements of cross-border DNS-level action to address abuses.

I&JPN Domains & Jurisdiction Operational Approaches (2019)[iii]

FOSTERING LEGAL INTEROPERABILITY

Further work is conducted to evangelize, communicate and aid the implementation of these policy solutions. This may take the form of Toolkits compiling thematic Outcomes developed by the Contact Group. This helps further legal interoperability in two dimensions:

- **Interoperability between actors**: to enable automation of the technical workflow among public authorities and private actors across borders to ensure due process at scale.
- **Interoperability between norms**: to reduce the potential of conflicts in rule-setting, implementation and enforcement among different regimes.

i. https://www.internetjurisdiction.net/uploads/pdfs/Papers/Domains-Jurisdiction-Program-Paper.pdf
ii. https://www.internetjurisdiction.net/uploads/pdfs/Papers/Domains-Jurisdiction-Policy-Options-Document.pdf
iii. https://www.internetjurisdiction.net/uploads/pdfs/Papers/Domains-Jurisdiction-Program-Operational-Approaches.pdf

The DNS Level Action to Address Abuses Toolkit frames approaches towards defining thresholds of when action at the DNS level is appropriate and builds a common understanding of the requisite processes that can ensure due process. This resource can be useful for DNS Operators in the design of their DNS Abuse related activities, and for Notifiers in the detection and reporting of problematic activity within the DNS. It can also help legislators and policymakers determine procedures for dealing with different types of DNS Abuse. This Toolkit provides tools that seek to help improve the interactions between the different actors to act on DNS Abuse while also strengthening corresponding procedures and mechanisms to guarantee proportionate remedies and due process for registrants. The Domains & Jurisdiction Contact Group will continue to engage on the topics addressed in the Toolkit with the objective of refining them and developing new tools.

The subsequent components of this Toolkit are a joint contribution by some of the most engaged experts in this field to advance the ongoing debate on the complex issues of cross-border domain name suspensions. They should not be however understood as the result of a formal negotiation validated by these Members' organizations. They are a best effort by the Members of the Program's Contact Group to address the important cross-border issues pertaining to addressing abuses at the DNS level that have been curated by the I&JPN Secretariat into the framework of this Toolkit.

This Toolkit provides resources that seek to help improve the interactions between the different actors to act on DNS Abuse while also strengthening corresponding procedures and mechanisms to guarantee proportionate remedies and due process for registrants.

3.
TOOLKIT
DNS LEVEL ACTION TO ADDRESS ABUSES

STRUCTURE

ADDRESSING ABUSE AT DNS LEVEL (GENERAL)

ADDRESSING TECHNICAL ABUSE

STRUCTURE

The following Toolkit curates tools that practitioners can use in their everyday work to determine when - and how - it is appropriate to act at the DNS level to address abuses. These tools have been developed by the multistakeholder Domains & Jurisdiction Program Contact Group throughout 2019-20 and also draw on the Operational Approaches document published by the Contact Group in April 2019.

This Toolkit has a twofold structure, each organized along the four stage framework of: identification, evaluation, choice of action, and recourse. The first section 'Addressing Abuse At DNS Level' provides a set of generic tools that shape actors' overall understanding of the types of abuses for which operators receive requests to act on, and actions available to DNS Operators, as well as the effects and implications of such actions. The second section 'Addressing Technical Abuse' contains practical tools specifically targeting technical abuse. This section also contains a Procedural Workflow outlining the process and specific points of interaction between actors in addressing phishing and malware abuse.

ADDRESSING ABUSE AT DNS LEVEL (GENERAL)

IDENTIFICATION

- TYPES OF ABUSES
- DUE DILIGENCE BY NOTIFIERS
- NOTIFICATION TO REGISTRANTS

EVALUATION

- THRESHOLDS

CHOICE OF ACTION

- TYPES OF ACTIONS
- EFFECTS OF ACTION AT THE DNS LEVEL

RECOURSE

- RECOURSE FOR REGISTRANTS
- TRANSPARENCY

ADDRESSING TECHNICAL ABUSE

IDENTIFICATION AND NOTIFICATION OF TECHNICAL ABUSE

- CHANNELS/SOURCES/TYPOLOGY OF TECHNICAL ABUSE NOTIFIERS
- DNS-LEVEL ACTION TO ADDRESS TECHNICAL ABUSES: DUE-DILIGENCE GUIDE FOR NOTIFIERS
- MINIMUM COMPONENTS FOR TECHNICAL ABUSE NOTICES

EVALUATION OF TECHNICAL ABUSE

- DNS OPERATORS' DECISION-MAKING GUIDE TO ADDRESS TECHNICAL ABUSE

ACTING ON TECHNICAL ABUSE

- DNS TECHNICAL ABUSE: CHOICE OF ACTION

PROCEDURAL WORKFLOW

- ADDRESSING PHISHING AND MALWARE

ADDRESSING ABUSE AT THE DNS LEVEL (GENERAL)

IDENTIFICATION AND NOTIFICATION

EVALUATION

CHOICE OF ACTION

RECOURSE

IDENTIFICATION AND NOTIFICATION

Addressing DNS Abuse begins with the identification of abuse that meets a sufficient threshold to justify action at the DNS level. The tools in this section respectively address:

- The types of abuses for which DNS Operators receive requests to act upon.
- The requisite due diligence by Notifiers in the identification of such abuse.
- The modalities of notification to Registrants when it is deemed appropriate to act on specific domains engaged in abuse.

I&JPN Ref. 19-126

TYPES OF ABUSES

DNS Operators receive cross-border requests to take action against domain names allegedly associated with technical abuse or problematic content. Listed below are descriptions of different types of technical abuses, as well as website content abuse, for which Registries and Registrars often receive such requests.[1]

1. Technical abuses

Domain names can be misused to propagate different types of technical abuse, including but not limited to the following:

a. **Malware** is malicious software, installed on a device without the user's consent, which disrupts the device's operations, gathers sensitive information, and/or gains access to private computer systems. Malware includes viruses, spyware, ransomware, and other unwanted software.[2]

b. **Phishing** occurs when an attacker tricks a victim into revealing sensitive personal, corporate, or financial information (e.g. account numbers, login IDs, passwords), whether through sending fraudulent or "look-alike" emails, or luring end users to copycat websites. Some phishing campaigns aim to persuade the user to install software, which is in fact malware.

c. **Pharming** is the redirection of unknowing users to fraudulent sites or services, typically through DNS hijacking or poisoning. DNS hijacking occurs when attackers use malware to redirect victims to their own site instead of the one initially requested. DNS poisoning causes a DNS server to respond with a false IP address bearing malicious code.[3] Phishing differs from pharming in that the latter involves modifying DNS entries, while the former tricks users into entering personal information.

d. **Botnets** are collections of internet-connected computers that have been infected with malware and commanded to perform activities under the control of a remote administrator.[4]

e. **Fast-flux** hosting is used to disguise the location of websites or other internet services, or to avoid detection and mitigation efforts, or to host illegal activities. Fast-flux techniques use the DNS to frequently change the location on the internet to which the domain name of an internet host or name server resolves.[5]

---

1. These lists are illustrative and not intended to be exhaustive.
2. See M3AAWG & London Action Plan, Operation Safety-Net: best practices to Address Online Mobile and Telephony Threats (2015) ("Operation Safety-Net"), at https://www.m3aawg.org/system/files/M3AAWG_LAP-79652_IC_Operation_Safety-Net_Brochure-web2-2015-06.pdf; "Malware" page at the U.S. Federal Trade Commission website, at https://www.consumer.ftc.gov/articles/0011-malware
3. See the Public Interest Registry's Domain Name Anti-Abuse Policy, at https://thenew.org/org-people/about-pir/policies/org-idn-policies/anti-abuse-policy-org-idn/; entries for DNS hijacking and DNS poisoning in the Kaspersky Lab Encyclopedia, at https://encyclopedia.kaspersky.com/glossary/dns-hijacking/
4. See "A Glossary of Common Cybersecurity Terminology," National Initiative for Cybersecurity Careers and Studies, at: https://niccs.us-cert.gov/about-niccs/glossary#B
5. See the Public Interest Registry's Domain Name Anti-Abuse Policy, at https://thenew.org/org-people/about-pir/policies/org-idn-policies/anti-abuse-policy-org-idn/

f. **Spam** is unsolicited bulk email, where the recipient has not granted permission for the message to be sent, and where the message was sent as part of a larger collection of messages, all having substantively identical content.[6] Spam is included here to address when it is used as a delivery mechanism for technical abuse.

2. Website content abuses

Most DNS Operators treat requests to deal with problematic website content differently from technical abuses. Since Registries and Registrars (when not also serving as the hosting provider) cannot remove offending pieces of content from a website, more often than not, acting at the DNS level is not appropriate. Remediation for problematic content should occur at the registrant or hosting provider level.

The descriptions below are derived from various sources, including input from I&JPN Contact Group members. They are neither offered nor intended to be interpreted as normative descriptions. Some types of problematic content find a higher degree of shared agreement across jurisdictions than others.

a. **Child abuse material** consists of photos or videos taken by an offender, documenting the sexual abuse of a child.[7]

b. **Controlled substances and Regulated goods** for sale or trade, include illegal drugs, the illegal sale of legal drugs, illegal services, stolen goods, and illegal firearms or other weapons. The legality of a given substance or good will vary across jurisdictions.

c. **Violent extremist content** includes content that depicts graphic violence, encourages violent action, endorses a terrorist organization or its acts, or encourages people to join such groups.

d. **Hate speech** includes advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence.[8]

e. **Intellectual property** related domain name suspension requests in response to website content (not relating to the domain name itself) have been issued on the basis of alleged trademark (e.g. sale of counterfeit goods), patent or trade secret infringement, or piracy of copyrighted works. As with all categories above, laws regarding intellectual property differ across jurisdictions.

6. See "The Definition of Spam" by The Spamhaus Project, at https://www.spamhaus.org/consumer/definition/
7. Interpol, "Online child abuse material: Q & A" (January 2017). https://www.interpol.int/Media/Files/Crime-areas/Crimes- against-children/Online-Child-Abuse-%E2%80%93-Questions-and-Answers
8. International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS171 (ICCPR), Art. 20(2), at https://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx

I&JPN REF. 19-130

DUE DILIGENCE BY NOTIFIERS

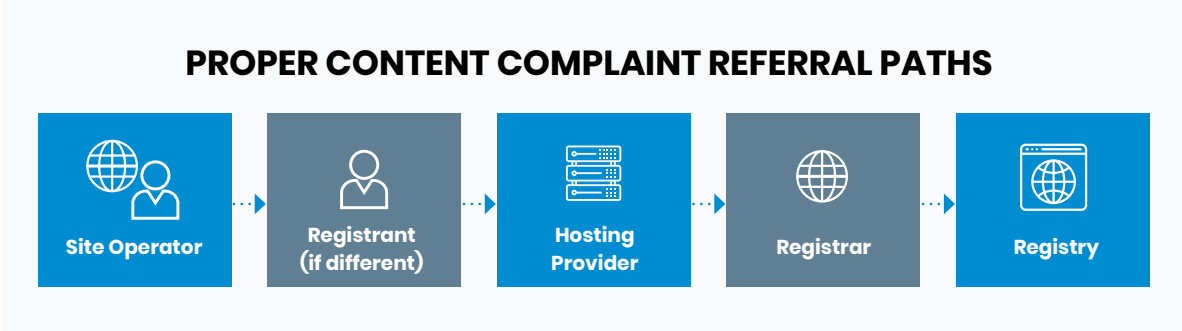
1. General principle

Persons or entities that file complaints or make abuse notices (notifiers) to domain name Registrars and Registries should ensure that they have conducted proper due diligence (both substantive and procedural) prior to alleging a domain name is engaged in abuse, either DNS/technical abuse (security and stability abuses) or in the context of content complaints (website content abuses).

2. Operational considerations

a. Substantive due diligence
Substantive due diligence involves ensuring that any claim against the content of any domain is properly investigated, substantiated and documented (e.g. screen shots, listing on any blacklists, evidence of ownership in claims of infringement). A notifier should ensure that it has undertaken proper substantive due diligence before making a referral.

b. Procedural due diligence
Procedural due diligence involves a hierarchy (see Proper Content Complaint Referral Paths below) of where the notice should be made. For technical abuse, notices directly to the Registrar and Registry are appropriate. In instances of content complaints, mitigation at the DNS level is an imperfect remedy. Accordingly, notices should be made in the following order:



Currently, some notifiers for content complaints make their referrals directly to the Registry or Registrar. This can lead to problems with proportionality.

i. Using the example of a file sharing site, if a Registrar or Registry suspends the entire domain because of an allegation regarding a limited number of infringing or offensive content, then potentially thousands of other pieces of legitimate content are rendered inaccessible by not just the registrant, but end users.

ii. The website operator, registrant or hosting provider, however, can all affect and likely remove the limited instances of abusive content while leaving the remaining content (as well as the domain name) unaffected.

Accordingly, for content complaints, a notifier should first attempt to work with the website operator, the registrant and the hosting provider to have the specific pieces of content removed. If none of those actors ultimately act or remove the content, the notifier may wish to escalate to the Registrar or Registry (such referral would still be subject to applicability of any Acceptable Use or similar policy).

I&JPN REF. 19-133

NOTIFICATION TO REGISTRANTS

1. General principle

Registrants should generally be provided with notifications of alleged abuse before a Registrar or Registry acts against a domain name. There are, however, some allegations of abuse where this is not practical, advisable, or even permissible, and in those instances, notification after the fact should be provided, unless legally forbidden.

2. Operational considerations

a. Registrant notification before action

If a Registry or Registrar receives allegations of copyright infringement, allegations of defamation, instances where content may be inferred to be illegal or fraudulent but cannot be proven without further investigation[9] (generally, "content complaints"), notification to the registrant should occur prior to a DNS Operator taking action on the domain.

b. Registrant notification after action

If a Registry or Registrar receives allegations of DNS technical abuse ("technical abuse"), court orders from competent jurisdiction(s) directing action or as set forth in applicable Registrar or Registry policies or procedures, notification to the registrant can occur after the fact.[10]

c. Who provides the notification?

Between the Registrar and Registry, Registrars are the preferred operator to provide notifications to registrants. Registrars usually have a closer contractual and business relationship with the registrant, and the Registrar collects the registrant's information. Many ccTLD Registries have direct contractual or business relationships with the registrant and may be similarly positioned to provide notifications.

gTLD Registries typically (but not always) provide notifications to Registrars who are asked to work with the registrant to remediate the alleged abuse. In non-court-mandated situations, abuse notifications are usually sent to the Registrar who is then requested to work with the registrant in a limited time frame (e.g. 48 hours) to remediate the alleged abuse.

d. Content of the notice

In most cases, only information necessary to inform the registrant's investigation and remediation of the alleged abuse should be provided in a notification. In some instances, the entire referral may be transmitted (e.g. in instances of alleged copyright infringement if that is in scope of the relevant parties' terms).

---

9. This assumes the various categories of content fall within the scope of the Registry or Registrar's Terms of Service, Anti-Abuse or Acceptable Use Policies or other governing terms. If the content falls outside the scope of such terms, no Notification will be typically provided and the domain will not be actioned.

10. There are also instances when a DNS Operator cannot provide Notification at all (such as when a court order requires confidential handling, or after weighing relevant law enforcement considerations).

EVALUATION

Once potential abuse has been identified in connection with a specific domain name, the next step is an in-depth evaluation towards making a decision on whether the abuse meets a sufficient threshold justifying taking action at the DNS level. This part of the Toolkit sets out the criteria that should be considered.

I&JPN REF. 19-127

THRESHOLDS

1. Technical 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.

2. Abusive content

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*:

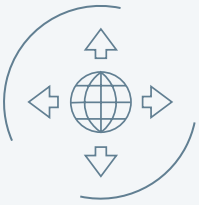
a. The degree of global normative coherence[11] regarding the alleged abuse: i.e. whether the content at issue is considered illegal across a sufficient number of jurisdictions;

b. The proportion of the site effectively dedicated to the infringing content;

c. The manifest intended purpose or bad faith of the registrant, and

d. The lack of available alternative measures to remediate the situation.

11. See International Normative Coherence in I&J Policy Brief on the Geographic Scope of Content Restrictions: https://www.internetjurisdiction.net/uploads/pdfs/Internet-Jurisdiction-Policy-Network-20-102-Geographic-Scope-Content-Restrictions.pdf



CHOICE OF ACTION

Once a decision to act on a domain name has been made, Operators need to determine the specific action which can be most effective and appropriate to address the abuse. The following section sets out the tools that are available to DNS Operators and their practical effect, to guide the determination of the right course of action:

- A non-exhaustive list of the different types of actions at the disposal of Operators.
- An explanation of the technical effects of such actions.

I&JPN REF. 19-131

TYPES OF ACTIONS

Protection of the core of the internet is and should be a key priority. The DNS - part of the core of the internet - is an addressing system. It is a neutral, technical layer that is vital for the proper functioning of the internet. Action at the DNS level is neither a fully effective way - nor should be considered as the natural tool - to address technical abuses or problematic content.

Acting at the DNS level should only be considered when it can be reliably determined that the domain itself is used with a clear intent of significant abusive conduct. Furthermore, because the suspension of a domain has by definition a global impact, proportionality requires that only a particularly high level of abuse and/or harm could potentially justify resorting to such a measure. It is important that the impact of a specific action at DNS level is well understood.

Requests for domain name suspension should be directed in the first instance to those parties that are closest to the abusive activity, including by contractual relationship (see Proper Content Complaint Referral Paths under 'Due Diligence by Notifiers' for more detail). For example, notifiers should first attempt to contact the domain name registrant, and then the hosting provider (either or both of which may be the wrongdoer), as these parties have the most direct relationship to the website content.[12] Direct action by registrants or hosting providers minimizes potential impact on the functioning of the DNS. If these attempts are unsuccessful, notifiers should consider the below options. Listed below are different types of actions that Registries and Registrars may take, as appropriate, in response to cross-border suspension requests.[13]

Note that the availability of any given action below may vary across providers.

1. For Registries: **Refer the suspension request to the Registrar**, which has the contractual relationship with the Registrant of the domain name.
2. **Hold** the domain name so it does not resolve. This removes the domain name from the TLD zone file, so the domain name will no longer resolve on the public Internet. In the event that the request was made in error, this action may be reversed.
3. **Lock** the domain name so it cannot be changed. A locked domain cannot be transferred, deleted or have its details modified, but will still resolve.
4. **Redirect** name services for the domain name. A Registry has the technical ability to change a domain name's nameservers. By changing the nameservers for the domain name, services associated with the domain name can be redirected for "sink-holing" (logging traffic) to identify victims for the purposes of remediation.
5. **Transfer** of the domain name to a suitably-qualified Registrar may prevent exploitation, whilst allowing for management of lifecycle, EPP status codes, and expiration.
6. **Delete** the domain name. Deletion is an extreme action and not generally recommended without careful due diligence and direction from the appropriate authorities. Restoring a domain name, if the deletion is found to be inappropriate, may involve additional burdens that are not manifest when placing a domain name on hold. Deletion is generally not as effective at mitigating abuses as suspension, as a registrant is free to re-register the domain name after it is purged from the zone.

---

12. See CENTR, Domain name registries and online content (Jan 30, 2019), available at: https://centr.org/library/library/policy-document/domain-name-registries-and-online-content.html (describing the relationships between various actors involved with a website featuring abusive content).

13 . These actions are adapted from ICANN's Framework for Registry Operator to Respond to Security Threats, at https://www.icann.org/resources/pages/framework-registry-operator-respond-security-threats-2017-10-20-en (Internal citations omitted).

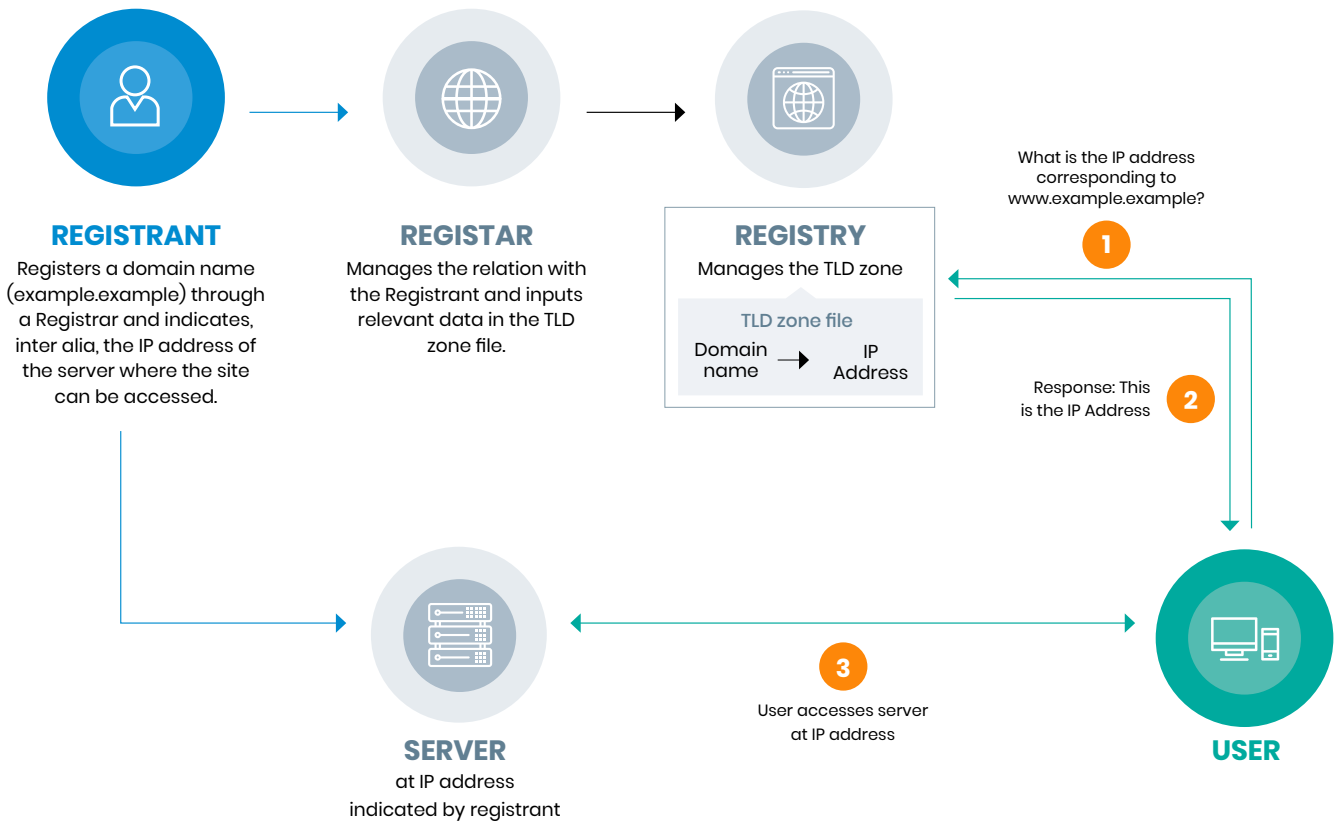
I&JPN REF. 20-101

EFFECTS OF ACTIONS AT THE DNS LEVEL

Action at the DNS level is neither a fully effective way - nor should be considered as the natural tool - to address technical abuses or problematic content. Acting at the DNS level should only be considered when it can be reliably determined that the domain itself is used with a clear intent of significant abusive conduct. Furthermore, because the suspension of a domain has by definition a global impact, proportionality requires that only a particularly high level of abuse and/or harm can potentially justify resorting to such a measure.

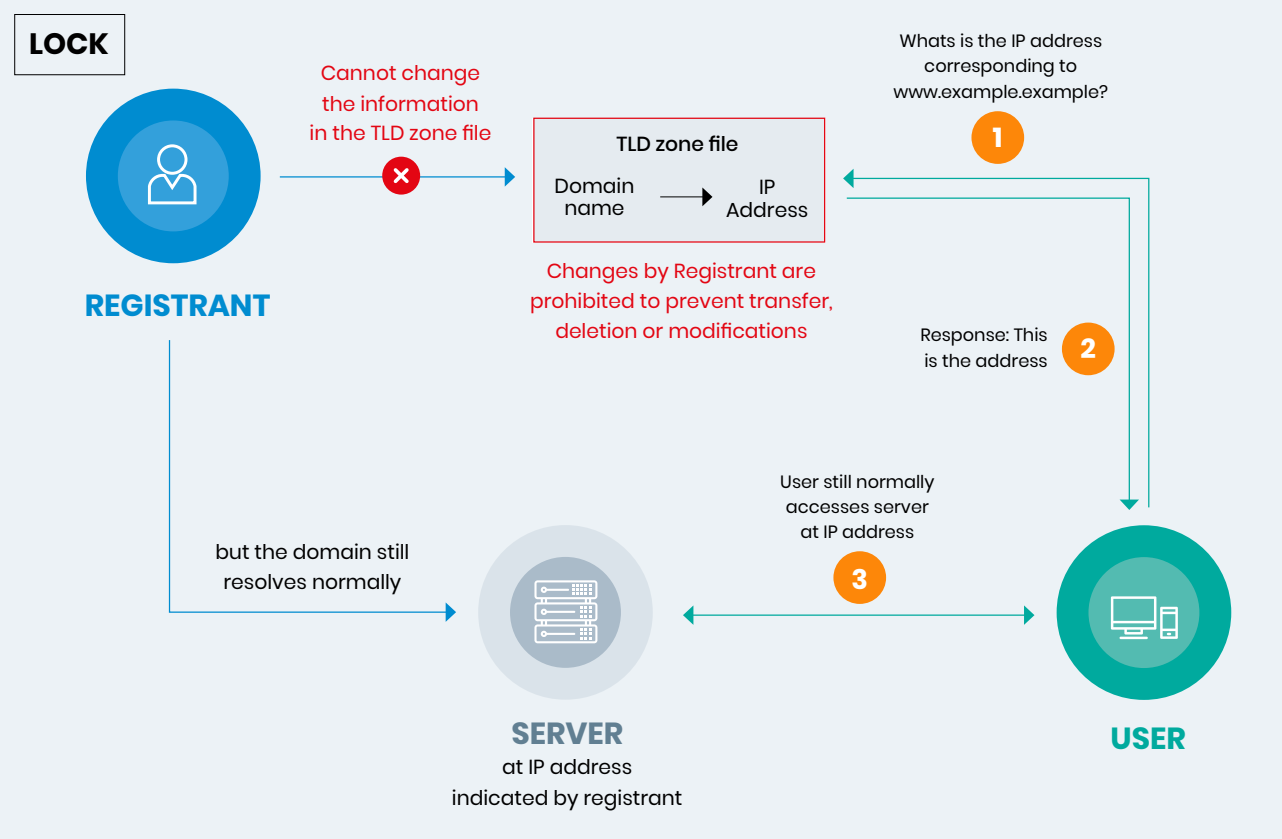
In any case, requests for action should be directed first to parties that are closest to the abusive activity, including by contractual relationship, in order to minimize impact on the functioning of the DNS. If attempts to reach the registrant or the hosting provider are unsuccessful, notifiers should consider the different types of actions listed below that Registries (who manage the Top Level Domains ("TLDs")) and Registrars may take, as appropriate, in response to cross-border suspension requests. It is important that the functioning of the DNS and the impact of each specific action at DNS level are well understood.

The basic functioning of the Domain Name System

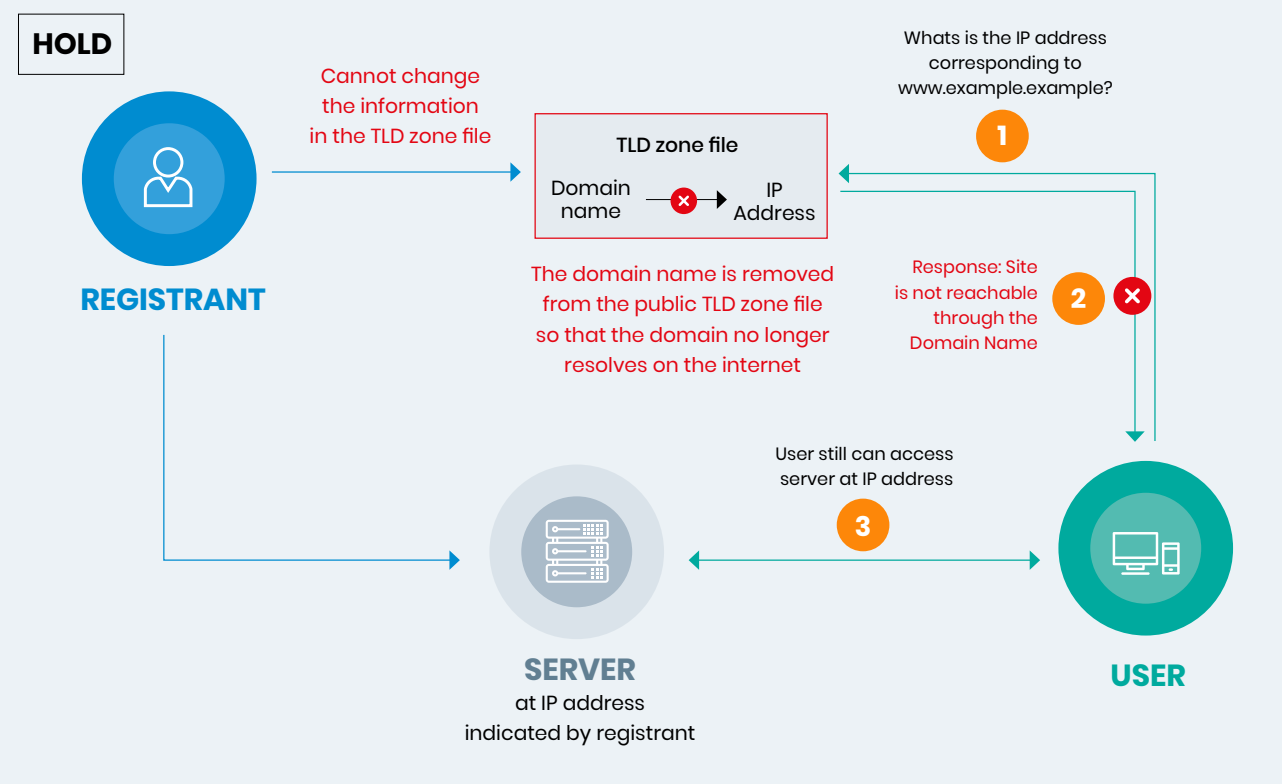


ACTIONS

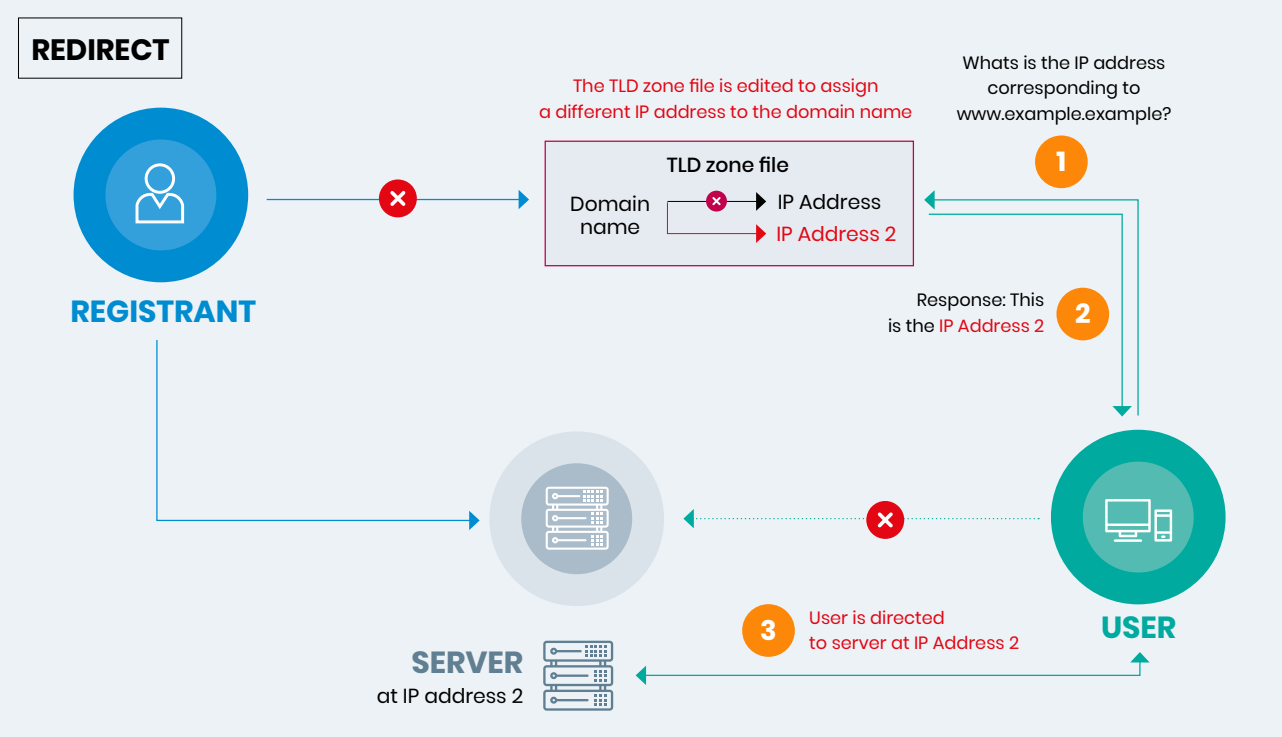
ACTION 1: LOCK A locked domain cannot be transferred, deleted or have its details modified, but still resolves.



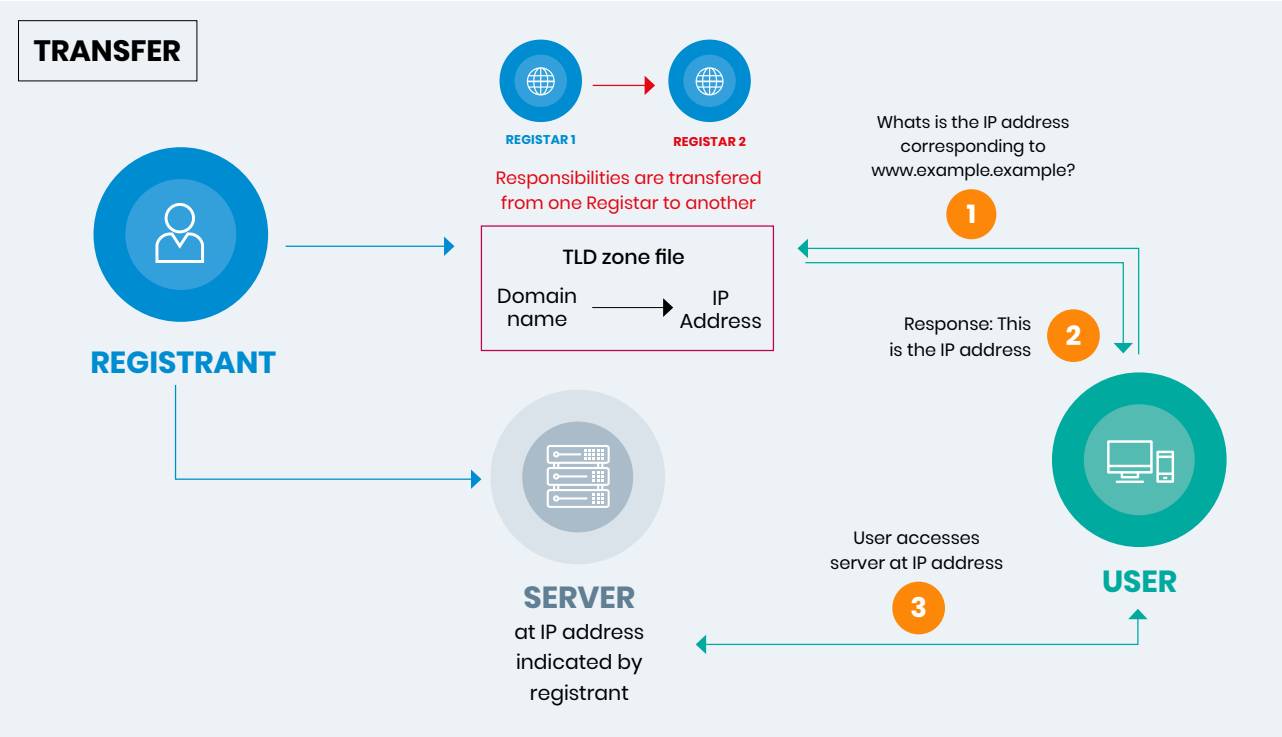
ACTION 2: HOLD This action removes the domain name from the TLD zone file, so the domain name will no longer resolve on the public Internet. In the event that the request was made in error, this action may be reversed. Importantly, the site still remains accessible through the IP address.



ACTION 3: REDIRECT By changing the nameservers for the domain name, associated services can be redirected without consent of the registrant, for instance for "sink-holing" (logging traffic) to identify victims for the purposes of remediation. This measure is usually done in conjunction with 'Lock', and the registrant is typically not informed of the action in advance.



ACTION 4: TRANSFER Transfer of the domain name to a qualified Registrar may prevent exploitation, whilst allowing for management of lifecycle, EPP status codes, and expiration.



ACTION 5: DELETION Deleting a domain name is an extreme action and **not generally recommended** without careful due diligence. Restoring the domain name would involve additional burdens absent when placing a domain name on hold. More importantly, **registrants are free to re-register the domain** name after it is purged from the zone.

RECOURSE

Recourse is an essential part of due process. It is independent from the evaluation conducted ahead of the action being taken by Operators on a domain name and must provide avenues for registrants to challenge such action and obtain redress. This section outlines the following tools:

- Principles to structure mechanisms for registrant recourse.
- A two-dimensional approach to foster transparency.

I&JPN REF. 19-134

RECOURSE FOR REGISTRANTS

1. General principles

Registrars and Registries should maintain a publicly available process (even an informal one) for allowing a registrant to contest or appeal an action against a domain name for technical abuse or for a content complaint. Any appeal must include independently verifiable evidence that does not require (or at least minimizes the need for) the DNS Operator to interpret the law, which is generally outside the DNS Operator's expertise.

2. Operational considerations

a. Process

Registries and Registrars should note in their Anti-Abuse Policy/Acceptable Use Policy how such an appeal can be lodged.

i. This will typically be something along the lines of "For inquiries regarding actions taken pursuant to this policy, please contact [abuse@example.example or review@example.example]"

This process will be available for actions except those carried out pursuant to a court order from the DNS Operator's jurisdiction. If action was taken pursuant to an order from a court with jurisdiction over the DNS Operator, no internal DNS Operator process can overrule such an order. The DNS Operator should conduct proper and thorough due diligence before action on the domain is effectuated. This should obviate the need for much back-and-forth with the registrant on appeal.

b. Evidence submitted

Registries and Registrars are not courts of competent jurisdiction, nor are they experts in interpreting various applicable laws. Accordingly, any evidence submitted by a registrant/appellant must be independently verifiable and not require (or at least minimize the necessity for) the DNS Operator to interpret the law. For a DNS Operator to reverse its decision in such an appeal, the evidence must be overwhelming and objective. It is important to have such a mechanism in case, for instance, of DNS Operator error or overwhelming evidence provided against the notifier's complaint.

c. Overturning action regarding technical abuse

There is less "wiggle room" in evaluating technical abuse than in evaluating abusive content. If a domain was engaged in phishing or distribution of malware and identified as such, only evidence clearing a high threshold should allow for reversal of a suspension, unless the domain has been compromised.

i. If a registrant is able to show the domain was compromised without his/her knowledge, the DNS Operator may wish to consider such evidence.

ii. Another instance for a DNS Operator to reverse a decision for technical abuse would be for DNS Operator error, such as suspending the wrong domain name (example1.example instead of example11.example), or if a domain was removed from a blocklist that was relied upon prior to suspension.

d. Overturning action regarding website content abuse

There is more room for interpretation here by a DNS Operator for content complaints, but any evidence submitted must be independently verifiable and not require, or at least minimize the necessity for, the DNS Operator to interpret the law.

If a registrant appeals an action a DNS Operator took due to reliance on work with a third party (such as a specialized notifier), the DNS Operator and notifier should have a process in place whereby the notifier can independently assess the countervailing evidence and be willing to reverse its recommendation.

I&JPN REF. 19-132

TRANSPARENCY

A two-dimensional approach can help to improve transparency:

1. Statistics

Beyond metrics currently used for performance measurement, DNS Operators are encouraged to develop metrics for collecting and reporting, in exportable, and accessible formats, coherent statistics pertaining to abuse notifications and implemented actions. Public authorities and specialized notifiers should likewise develop corresponding mechanisms to ensure traceability of their notices.

2. Decision-making

DNS Operators document and make available to the public the criteria determining when action at the DNS level is appropriate, the types of abusive content they are willing to take action on, and their abuse point(s) of contact. They also document and publicize their internal criteria for decision-making and the channels for appeals/recourse. Specialized notifiers likewise document and make available to the public their criteria for evaluation of abuses, as well as their due diligence rules and procedural guarantees.

ADDRESSING TECHNICAL ABUSE

IDENTIFICATION AND NOTIFICATION OF TECHNICAL ABUSE

This section of the Toolkit lays out practical tools that can help different third-parties (Notifiers) in their identification and notification of technical abuse, including:

- A typology of the sources that provide notifications on technical abuses to DNS Operators, referred to herein as “Notifiers”;
- The requisite due-diligence expected from such Notifiers in the notification of technical abuse; and
- The minimum notice components that must be included in the notification of such technical abuse.

I&JPN REF: 20-110

CHANNELS / SOURCES / TYPOLOGY OF TECHNICAL ABUSE NOTIFIERS

DNS Operators receive technical abuse complaints ("Notices") from a variety of sources representing different types of stakeholders in the DNS ecosystem ("Notifiers"). Whether and how DNS Operators take action in response to Notices depends on many factors, including, but not limited to whether the Notice contains information required for evaluation and possible action by the Operator, whether the Operator has a pre-existing relationship (contractual or otherwise) with the Notifier concerning detection and remediation of the type of abuse alleged[14], the Operator's contractual obligations to third parties (e.g. ICANN), the Operator's Terms of Service and the local jurisdictional framework. In all cases, Notifiers should exercise careful due diligence before requesting Operators to take action at the DNS Level to address alleged abuses.

The table below provides an overview of the types of notifiers, as well as examples of entities or persons that fall within each given type. Such examples are not meant to be exhaustive nor prescriptive. Some categories of notifiers may fall within more than one type: for example, a Reputation Block List Provider may be a non-commercial entity. Likewise, a DNS Infrastructure Provider may be a commercial or non-commercial entity.

TYPES	NOTIFIERS
Individuals	DNS users acting in their personal capacity
Governments (Domestic, Regional, Foreign)	Court orders
	Public Administration Bodies (e.g. Regulators, Public Safety Administrators, CSIRTs)
	Law enforcement
DNS Infrastructure Providers	Registries Registrars and resellers Back-end service providers Technical solutions and security providers ICANN
Commercial Entities	Reputation blocklist providers CERTs Businesses and consultants
Non-commercial entities	Mission-based organizations that are dedicated to furthering the public interest
Machine	Artificial Intelligence

14. Operators may enter into contractual obligations with different notifying entities. According to the terms of such agreements, the DNS Operator can determine the level of evaluation that it may undertake.

I&JPN REF: 20-113

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

All notifiers have a duty to conduct due diligence before making notifications of alleged technical abuse[15] to DNS Operators and requesting action at the DNS level to remedy such abuse. While action at the DNS level may be appropriate to address certain types of technical abuse, DNS-level action has a major impact not only on the domain name, itself, but potentially on other activities linked to the domain name, such as email, name servers, databases and other services which are linked to the domain. DNS-level action to address alleged technical abuses must be therefore not only effective, but efficient and proportionate to the harm(s) alleged. By employing *procedural and substantive*[16] due diligence measures before making notifications to the DNS Operator, notifiers can increase the efficiency and effectiveness with which the Operator evaluates and addresses notifications of alleged abuse.

This document lists a series of questions notifiers should ask themselves in order to determine that making notices to operators is appropriate. This guide is structured around three parts: Identification; Evaluation; and Notification. The Identification and Evaluation sections list the *substantive* due diligence a notifier is encouraged to perform to determine that abuse is present and whether action at the DNS level is appropriate to address it. The Notification section indicates the level of *procedural* due diligence that notifiers are encouraged to conduct in order to ensure that the notice is addressed efficiently and effectively.

IDENTIFICATION

The following questions will help notifiers when identifying potential abuse:

- What triggered the Notifier's attention to this abuse and does the Notifier have first-hand knowledge of the alleged abuse?
- What is the type of technical abuse at stake? Does this appear to be something that can and should be mitigated at the DNS level?
- What is the evidence for the existence of such alleged abuse?
- Is it likely that the domain has been compromised, i.e. the infringing action has been done without the knowledge or intent of the registrant/site operator?

EVALUATION

When making a referral to a DNS Operator or Infrastructure Provider, notifiers should make the referral to the entity closest to the abuse and most likely to be able to evaluate the specific problem and remediate it with the least collateral damage. The questions below can help a Notifier determine which Operator is best positioned to help:

---

15. For scope of technical abuse, refer to 'Types of Abuses' in the Addressing Abuse at DNS Level (General) part of this toolkit.

16. Refer to Criteria E2: Due Diligence by Notifiers in Domains & Jurisdiction Operational Approaches

- Where is the abuse taking place (e.g. sublevel domain, specific URL, etc.)?
- Is action at the DNS[17] level appropriate or are there other means to address the abuse?
- If there is a more appropriate actor than a DNS Operator to address the abuse (e.g. hosting provider or site operator), has there been an attempt to address the abuse at that level?
- Would action at the DNS level create collateral damage disproportionate to the harm caused by the alleged abuse?
- What could be the appropriate choice of action at the DNS level to address the abuse?
- Who are the relevant registry and registrar and how do their respective terms of service address such type of abuse?
- Is there a way to assess (including through interaction with relevant authorities) if there is an ongoing investigation that a DNS-level action could jeopardize?

NOTIFICATION

When making notification to DNS Operators, Notifiers should consider the following questions to improve the efficiency and efficacy of their notices:

- When action at the DNS level is appropriate, to whom should notification be made: Registrar, Registry, both?
- Does the notifier have an existing contractual relationship with the Operator and have the terms of such a contract been met?
- What is the DNS Operator's preferred channel for notification of abuse?
- Does the DNS Operator have a prescribed reporting format?
- Does the notice contain all the required components for a good/effective notice[18]?
- Should the notice be designated confidential, e.g. in cases where there is a risk of jeopardizing an investigation?

17. Refer to I&J Educational Resource on Effects of Action at the DNS Level

18. Refer to Domains & Jurisdiction Program Outcome Minimum Notice Components for Technical Abuse

I&JPN REF: 20-106

MINIMUM COMPONENTS FOR TECHNICAL ABUSE NOTICES

DNS Operators frequently receive complaints of technical abuse "Notices" in a broad diversity of formats that often do not contain sufficient information for investigation and action. The following table, based on Criteria C of the Internet & Jurisdiction Policy Network Domains & Jurisdiction Operational Approaches document, therefore proposes a list of components that support actionable Notices for reporting technical abuse.[19] While the table indicates a subset of components that are necessary to make a given Notice actionable, as well as those components which significantly assist the operator in addressing the alleged abuse, *all* components listed are important contributions to robust and effective Notices. In general, more detailed Notices are better in assisting the operator's evaluation and response. Additionally, where the notifier submits evidence of alleged technical abuse in the form of attachments (*e.g.* screenshots of alleged phishing), operators may reasonably employ an added layer of security review to ensure that attachments are not infected. This may increase the timeframe for the operator's review of the Notice, depending upon the operator's internal security capabilities.

Elements marked with a red asterix(*) are components without which Notice is not actionable. Those highlighted in blue can significantly help the operator deal with the Notice.

IDENTIFICATION		Components without which notice is not actionable (A)
Time*	Date and time corresponding to the issuance of the request.	A
Type of Notifier	Refer to Typology of Notifiers (court, law enforcement, private notifier, legal representative of a complainant, Anonymous)	
Issuing Entity[20]*	Identification of the requester	A
Request ID number	Reference provided by the issuer of the request (if applicable).	
Registrar (if Notice is addressed to the Registry)	Name and Abuse Point Of Contact of the Registrar managing the registration.	
Registry (if the Notice is addressed to the Registrar)	Registry managing the corresponding TLD extension. If not known, indicate the TLD.	
CASE – In case of court order from court of applicable jurisdiction		
Type of abuse*	Indication of the type of abuse alleged (from taxonomy list)	A
Legal basis*	A copy of the court order	A

19. The criteria for notifications for Website Content Abuse are considered separately, not in this document.

20. While the identity of the person or entity making the Notice is generally required for operator's to fully evaluate a given Notice, there are circumstances where operators may accept and evaluate Notices that are submitted anonymously, particularly where the subject matter of the alleged abuse is especially sensitive, such as those involving allegations of Child Sexual Abuse Imagery ("CSAM").

DUE DILIGENCE[21] – In case of no court order from court of applicable jurisdiction		
Evaluation	Steps undertaken by the notifier - prior to notification of the DNS Operator - to establish the existence, and extent of the abuse in conformance with the Operators' applicable policies	
Supporting evidence	Factual documentation of the alleged abuse and evaluation. This may be in the form of listings on reputation block lists (RBLs) the operator relies upon or through direct evidence (like screenshots in the case of phishing).	
Foreign Public Authority*	An official notice, documenting the elements above, including, where necessary, effort to domesticate foreign court order, if any.	A
Proportionality	Justification that the alleged abuse meets a sufficient threshold for action at the DNS Level, and also factoring potential collateral damage and the effectiveness of action at the DNS level.	
REQUESTED ACTION		
Targeted domain(s)*	Specific domain name(s) upon which action is requested, including URL.	A
Action sought*	Indication of the specific action requested (see Types of Action under 'Choice of Action')	A (in case of court order from applicable jurisdiction)
TIMING		
Deadline	When the action(s) should be executed (important in particular in case of concerted actions or emergency)	
Time range	Duration of the requested action (if applicable, if action sought is not 'transfer/delete')	
Emergency	Is this action justified by a particular emergency (nature of emergency)	
Rationale emergency*	Explanation of how the requested action will avert or mitigate the emergency	A(If confidentiality is requested)
CONFIDENTIALITY		
Confidentiality	Request not to notify the registrant prior to action or potentially even ex post for a period of time (if applicable)	
Confidentiality timeline*	Requested duration of confidentiality	A(If confidentiality is requested)
Rationale for confidentiality*	Proper justification for confidentiality request and timeline (can be included in the Court Orders)	
AUTHORITY		
Authentication	Information allowing verification of the identity of the Notifier and the authenticity of its Notice	
Certification	Written self-certification by the Notifier of its competence, performance of prior due diligence and accuracy of its statements and that there is no improper motivation or illegitimate purpose for requesting the suspension/cancellation.	
CONTACTS		
Issuing entity	Contact details of the Notifier, to which notification of action (or non-action) should be sent	
SIGNATURE		

21. For technical abuse, all requests made to ccTLD Operators by notifiers other than a court of applicable jurisdiction can be acted upon on a voluntary basis according to Operators' terms of service and national legislation, when applicable.

EVALUATION OF TECHNICAL ABUSE

Once alleged technical DNS abuse has been notified to DNS Operators, they must make a determination on whether to act on it or not. Towards this, the following section provides Operators guidance for their internal evaluation processes.

I&JPN REF: 20-108

DNS OPERATORS' DECISION-MAKING GUIDE TO ADDRESS TECHNICAL ABUSE

Acting at the DNS level can be justified to remediate technical/infrastructure abuse in order to protect the stability and security of the global infrastructure of the internet. DNS operators rely on a variety of internal and external resources to identify, evaluate and take action to remediate technical abuse[22]. While establishing whether a domain is being used to perpetrate technical abuse tends to produce binary results (i.e. the domain is or is not engaged in technical abuse), care should nonetheless be taken to ensure that action at the DNS level to remediate said abuse is appropriate and proportionate.

A general approach to addressing technical abuse may be based upon the following steps:

- Identification or notification of the alleged technical abuse associated with the domain(s)
- Evaluation of scope of abuse
- Determination of the choice of appropriate and proportionate action
- Technical actions to ensure recourse and remediation

The table below lists a set of structuring questions that DNS Operators can use at each step to determine a course of action to address technical abuse on a voluntary basis.

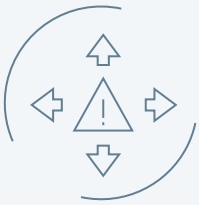
	STRUCTURING QUESTIONS
IDENTIFICATION AND NOTIFICATION	• Is the domain within the DNS Operator's zone? • Does the notice allege technical abuse? • Does the notice contain all the necessary components[23] for identifying abuse and taking action, as appropriate? • Does the notice come from a court of applicable jurisdiction? • Does the notice come from a trusted, repeating or ad-hoc source? • Is there an agreement between the DNS Operator and this specific notifier?
EVALUATION OF ABUSE Multi-factor analysis to evaluate the scope and authenticity of alleged abuse	According to the type of technical abuse, what should DNS Operators take into consideration when evaluating alleged abuse, to ensure that the action taken is appropriate and proportionate? • Conduct own investigation (with help of 3rd parties if required) to determine: - That it is not a false positive - Whether the abuse is still active (hasn't already been mitigated by someone else) - Where the abuse is taking place (single link, single URL, entire site?) • Is it likely that the domain has been compromised, such that the registrant should be contacted? • Is the alleged abuse related to a sublevel or third level domain? • Should action be taken?

22. See 'Types of Abuses' in 'Addressing Abuse At DNS Level' section of this Toolkit

23. Refer to Domains & Jurisdiction Minimum Notice Components for Technical Abuse

CHOICE OF ACTION Choice of the measure used to address the abuse	According to the type and level of technical abuse, what determines the choice of action? • Should the DNS Operator act or should other actors act[24] (e.g. hosting provider)? • If ordered by a court of applicable jurisdiction, is the specified action technically implementable? • What type of action[25] should be taken? • Should the registrant be notified[26]?
RECOURSE AND REMEDIATION Recourse Mechanisms available to registrants	According to each type of technical abuse and type of notice: • When is there notification to the registrant (when applicable)? • What recourse mechanisms[27] are available to the registrant?

24. Refer to Criteria E/2B - Procedural Due Diligence in the Domains & Jurisdiction Operational Approaches
25. Refer to Criteria F - Types of Action in the Domains & Jurisdiction Operational Approaches
26. Refer to Criteria H - Notification to Registrants in the Domains & Jurisdiction Operational Approaches
27. Refer to Criteria I - Recourse for Registrants in the Domains & Jurisdiction Operational Approaches



ACTING ON TECHNICAL ABUSE

This section of the Toolkit provides actors with an understanding of the technical effects of the diverse actions available to DNS Operators and their suitability and effectiveness against specific types of technical abuses.

I&JPN REF: 20-114

DNS TECHNICAL ABUSE: CHOICE OF ACTION

Once technical abuse[28] has been identified, evaluated and confirmed, DNS Operators must decide whether and how to act to address the abuse. While action at the DNS level may be appropriate to address certain types of technical abuse, DNS-level action has a major impact not only on the domain name, itself, but potentially on other activities linked to the domain name, such as email, name servers, databases and other services which are linked to the domain. DNS-level action to address alleged technical abuses must be therefore not only effective, but efficient and proportionate to the harm(s) alleged.

Malware and Phishing are technical abuses that can be delivered through websites or via email (in the form of spam). In such cases, acting on the attendant domain can be used to stop or interrupt its activity within the DNS.

Conversely, pharming, while a form of technical abuse, cannot be remedied through DNS-level action by DNS Operators. Pharming involves the redirection of unknowing users to fraudulent sites or services, typically through DNS hijacking or poisoning. DNS hijacking occurs when attackers use malware to redirect victims to the attacker's site instead of the one initially requested. DNS poisoning causes a DNS server [or resolver] to respond with a false IP address bearing malicious code. These activities do not involve the use of domain name(s) to propagate abuse. Therefore, action at the DNS level is ineffective to address pharming. Signing domains with DNSSEC and enabling validation on resolvers is a systemic approach that can be effective in preventing pharming.

As noted below, the LOCK and HOLD commands are most often used in tandem to address malware and phishing, as, respectively, these commands appropriately prevent the resale or transfer of domains engaged in abuse and remove the domain name from the TLD zone file, thereby preventing the domain from resolving on the public internet. Conversely, as explained below, the Transfer, Redirect and Create commands are of limited use in stopping DNS abuse and are usually implemented by DNS operators only pursuant to formal requests from law enforcement or courts.

The charts below are based on Criteria F 'Types of Action' of the Operational Approaches[29] document and address respectively:

- HOLD and LOCK, most often indicated to remediate technical abuse.
- REDIRECT and TRANSFER, generally used as additional measures upon specific requests.
- DELETE and CREATE, exceptional actions mainly used in the case of botnets and Domain Generation Algorithms (DGA's).

28. For scope of technical abuse, Refer to Annex in Domains & Jurisdiction Program Outcome on DNS Operators' Decision-making Guide To Address Technical Abuse

29. See 'Types of Action' in Addressing Abuse At DNS Level section of this Toolkit

TYPE OF ACTION	APPLICABLE AGAINST	EFFECT OF ACTION
LOCK	Malware, Phishing, Botnets, Fast Flux Hosting, Spam (as a delivery mechanism)	Locking a domain name preserves the *status quo* in terms of ownership, contact information and server configuration. This can assist investigators and fact-finders (*e.g.* courts) in investigating alleged abuse. The *Lock* command also prevents the resale or transfer of domains involved in abuse to unsuspecting third parties. A locked domain cannot be transferred, deleted or have its details modified, but will still resolve through the DNS (i.e. enabling access to the attendant website(s) via the domain name).
HOLD/ SUSPENSION	Malware, Phishing, Botnets, Fast Flux Hosting, Spam (as a delivery mechanism)	The *Hold or Suspension* command removes the domain name from the TLD zone file and prevents it from resolving on the public internet (i.e. enabling access to the attendant website(s) or other services including emails or 3rd party domains linked via nameservers via the domain name). This helps prevent distribution of malware and exposure to phishing including its distribution via email. The *Hold or Suspension action* is the strongest action applicable to a domain name and can be used to address most technical abuse. It is important to note however, that the attendant website will still remain reachable, albeit only through its IP address.

The actions *Redirect* and *Transfer* ***do not stop or impede ongoing technical abuse***. DNS Operators generally apply these commands only when compelled to do so by a formal request from law enforcement, a court order or other compulsory instruments.

TYPE OF ACTION	APPLICABLE AGAINST	EFFECT OF ACTION
REDIRECT	Malware, Phishing, Botnets	A DNS Operator has the technical ability to change a domain name's nameservers. By changing the nameservers for the domain name, services associated with the domain name can be redirected upon request for "sink-holing" (logging traffic), for instance to identify victims for the purposes of remediation.
TRANSFER	Malware, Phishing, Botnets, Fast Flux Hosting, Spam (as a delivery mechanism)	DNS Operators may be compelled to *Transfer* domain names without the registrant's consent in certain limited circumstances, for instance in order to prevent further abuse. This command effects a change in control (administration and ownership rights) of a domain to a third party to prevent exploitation, whilst allowing for management of lifecycle, EPP status codes, and expiration.

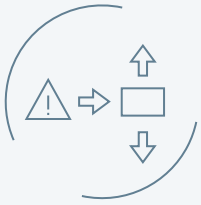
When a domain is deleted, it is removed from the TLD (Top Level Domain) zone file. As a result however, the domain becomes available again to be registered on a first-come, first-served basis.

This may potentially be done by the very registrant[30] who was using the domain to commit abuse. For this reason, the Delete command is generally not widely used to address abuse. The Create command may be also sparingly used for specific forms of technical abuse, such as botnets, but the use of this command raises very important and specific issues[31].

30. In some instances, DNS Operators are required (by court order) to place deleted domain names "on reserve" so that they cannot be re-registered by the perpetrator(s) of abuse. However, DNS Operators who operate pursuant to contractual agreements with ICANN are generally contractually prohibited from placing domains on reserve, except in limited circumstances outside of abuse operators mitigation efforts. Likewise, certain ccTLD (country code Top Level Domains) operators may also be subject to restrictions or prohibition when placing domains on reserve.

31. Criteria F 'Types of Action' in the Domains & Jurisdiction Operational Approaches does not include 'Create', but is included here due to its relevance to the topic. Create has however two important consequences in the ICANN environment: 1) It requires a contractual waiver for DNS Operators and 2) The newly created domains may entail the payment of a recurring fee.

TYPE OF ACTION	APPLICABLE AGAINST	EFFECT OF ACTION
DELETE	Botnets	Deleting a domain name is an extreme action and not generally recommended without careful due diligence and direction from the appropriate authorities. The Delete command may assist in interrupting a Botnet by interrupting the command and control path set by the Botnet's controllers. Deletion has a dramatic effect on the domain name holder and related services and cannot be undone in the circumstances when this choice of action is erroneously implemented. However, as noted above, the *Delete* command generally is not as effective at mitigating abuses as other actions such as Hold because the domain(s) can be quickly re-registered by a bad actor.
CREATE	Botnets, Domain Generation Algorithms	DNS Operators are sometimes asked to create and then redirect/ sinkhole domains that are part of a predictive sequence of a Domain Generation Algorithm ("DGA"). DGAs are algorithms seen in various families of malware used to periodically generate a large number of domain names to be used as rendezvous points with their command and control servers. Once created, the actions *Hold, Redirect or Delete* might be used to interfere with the domain names pointing to the servers that form the botnet. In some cases, this may effectively hinder a botnet, as the infected machines require the path provided by the control domain names in order to "call home".



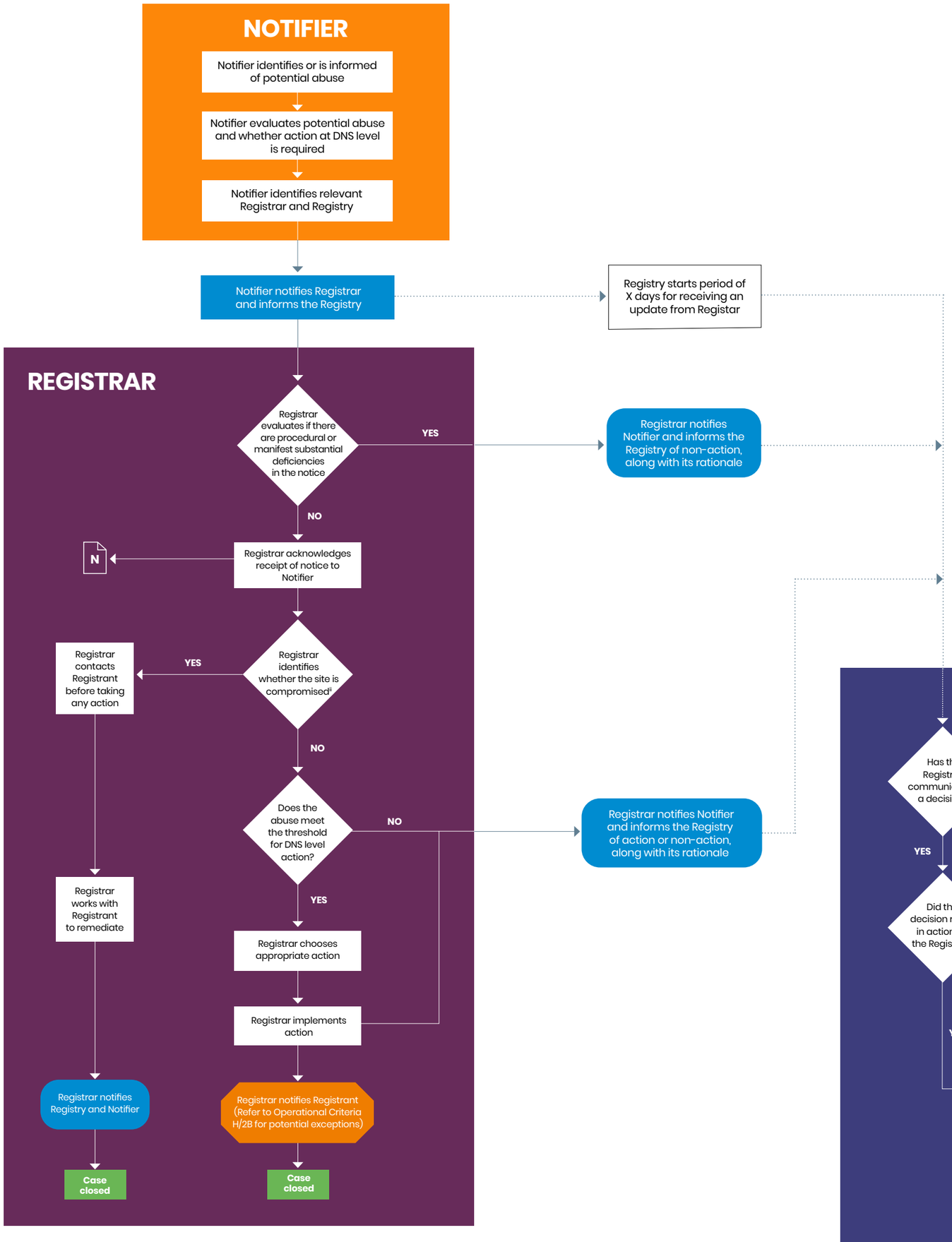
PROCEDURAL WORKFLOW

This section of the Toolkit provides a graphical representation of the procedural workflow for addressing phishing and malware distribution. It visualizes the steps mentioned in the previous stages of this section and provides all actors with a framework to manage their expectations regarding the distribution of responsibilities between actors and the sequence of notifications along the process.

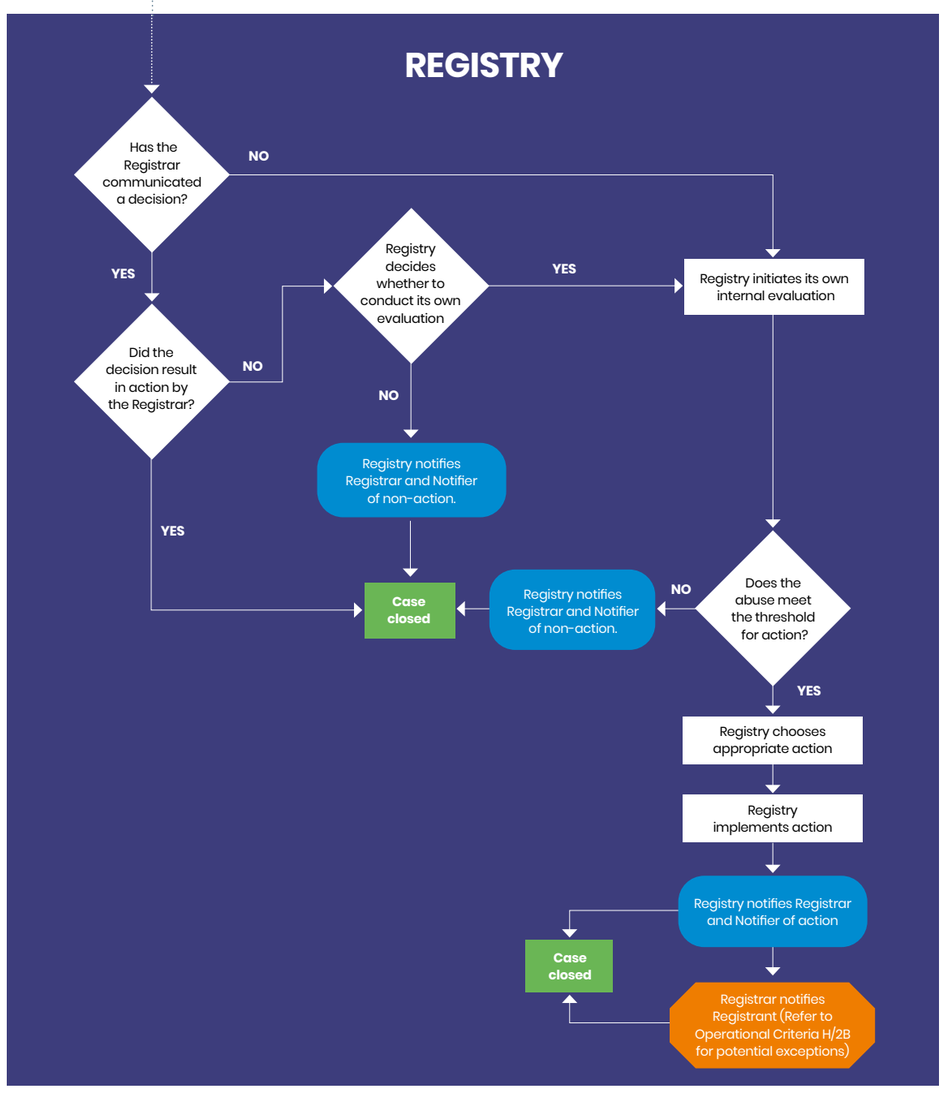
ADDRESSING PHISHING AND MALWARE: A PROCEDURAL WORKFLOW

I&JPN REF: 20-115

This workflow maps the respective roles of Notifiers, Registrars and Registries and the sequence of their interactions.



ii. A domain can be considered compromised not only when the control of the domain is seized by a third party (i.e. someone other than the registrant) and used maliciously to spread malware or conduct phishing, but may also occur in instances where the domain remains under the registrant's control but one or more subpages or URLs are likewise used to propagate phishing or malware without the registrant's knowledge and consent.



1. Abuse report is sent to the Registrar, which has the primary responsibility to investigate and address the abuse report.
2. The Notifier simultaneously informs the Registry (i.e. puts it on copy).
3. The Registrar is expected to decide on action or non-action within a reasonable time frame[i] (e.g. X business days).
4. During this time frame, the Registry is not expected to investigate.
5. The Registrar is expected to inform the Registry and Notifier of its decision to act or not.
6. In case of non communication by Registrar, Registry is expected to initiate its own evaluation.
7. The Registry is expected not to revisit Registrar action but in case of non-action by the Registrar, may conduct its own investigation. The Notifier should be informed of the result of this investigation.
8. The Registrar is expected to notify the Registrant in case of action being taken by either the Registrar or the Registry.
9. Automated ticketing systems can enhance communications and case management.

i. Bilateral arrangements between Registry and Registrar may set specific time lines.

4. INTERNET & JURISDICTION POLICY NETWORK

> **Managing the way that a large number of separate legal frameworks apply to the internet is one of the biggest policy challenges of our time – more complex than building the internet itself.**
>
> **Vint Cerf Co-inventor of the internet, writing in the Financial Times ahead of the 2nd Global Conference of the Internet & Jurisdiction Policy Network in 2018**

The Internet & Jurisdiction Policy Network is the multistakeholder organization fostering legal interoperability in cyberspace. Its stakeholders work together to preserve the cross-border nature of the internet, protect human rights, fight abuses, and enable the global digital economy. Since 2012, the Internet & Jurisdiction Policy Network has engaged more than 400 key entities from six stakeholder groups around the world including: governments, the world's largest internet companies, the technical community, civil society groups, leading universities and international organizations.

The regular Global Conferences of the Internet & Jurisdiction Policy Network are institutionally supported by six international organizations: Council of Europe, European Commission, ICANN, OECD, United Nations ECLAC, and UNESCO. Host partner countries include France (2016), Canada (2018) and Germany (2019).

The Community

6
STAKEHOLDER GROUPS

70+
COUNTRIES

400+
ENTITIES

STATES

INTERNET COMPANIES

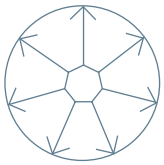
TECHNICAL OPERATORS

CIVIL SOCIETY

INTERNATIONAL ORGANIZATIONS

ACADEMIA

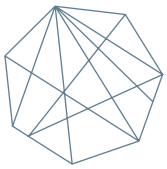
Mission



INFORM

The debates to enable evidence-based policy innovation

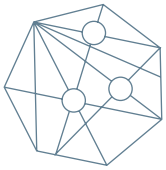
Informational asymmetry and mistrust between actors often result in uncoordinated policy action.
The I&JPN facilitates **pragmatic** and well-informed policy-making by framing issues and taking into account the **diversity of perspectives** while documenting tensions and efforts to address problems.



CONNECT

Stakeholders to build trust and coordination

Cooperation is important in a digital environment that is increasingly polarized, and where actors function in policy silos, with insufficient factual information.
The I&JPN serves as the **connective tissue** between stakeholder groups, regions, and policy sectors, as well as by **bridging gaps** within governments or organizations.



ADVANCE

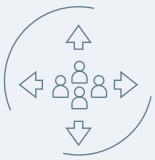
Solutions to move towards legal interoperability

The Policy Network strives to develop shared **cooperation frameworks** and **policy standards** that are as transnational as the internet itself.
The Network promotes a **balanced and scalable approach** to policymaking, aiming for legal interoperability, taking inspiration from the fundamental principle that enabled the success of the internet and the World Wide Web.

Core activities

POLICY PROGRAMS

EVENTS



KNOWLEDGE MUTUALIZATION

5. ACKNOWLEDGEMENTS

This Toolkit is based on the work of the Members of the Domains & Jurisdiction Program Contact Group of the Internet & Jurisdiction Policy Network 2017-2020, and its Outcome Documents, as well as the Roadmaps that resulted from the Global Conferences of the Internet & Jurisdiction Policy Network in 2016 (France), 2018 (Canada) and 2019 (Germany).

The Secretariat is grateful for the hundreds of hours of intense work of the Members of the Domains & Jurisdiction Contact Groups, and their alternates, composed of senior-level representatives from governments, internet companies, technical operators, civil society, leading universities, and international organizations from around the world since 2017.[1] The Secretariat also expresses thanks to the two Contact Group Coordinators between 2017-2020: Maarten Botterman, Director, GNKS Consult and Board Director, ICANN (2017-2019) and Brian Cimbolic, Vice President and General Counsel of Public Interest Registry (2019 - Present).

The following list of Members and their appointed alternates indicates the affiliation of stakeholders at the time they served in the Contact Group. Members served in their personal capacity.

Benedict Addis, Chair, Registrar of Last Resort (RoLR) • **Fiona Alexander**, Distinguished Policy Strategist in Residence, American University • **Gabriel Andrews**, Supervisory Special Agent, Cyber Division - Cyber Initiative & Resource Fusion Unit, Federal Bureau of Investigation • **Mohit Batra**, Technology Analyst, National Internet Exchange of India (NIXI) • **Tijani Ben Jemaa**, Executive Director, Mediterranean Federation of Internet Associations (MFIA) • **James Bladel**, Vice President of Policy, GoDaddy • **Pierre Bonis**, CEO, AFNIC • **Graeme Bunton**, Manager, Analytics and Insights Manager, Public Policy, Tucows • **Brent Carey**, Domain Name Commissioner, .NZ Domain Name Commission • **Jordan Carter**, Chief Executive, InternetNZ • **Mark Carvell**, Head of International Online Policy, United Kingdom - Department for Culture Media and Sport • **Lucien Castex**, Representative for Public Affairs and Partnership Development, AFNIC • **Susan Chalmers**, Internet Policy Specialist, United States - Department of Commerce • **Mishi Choudhary**, Legal Director, Software Freedom Law Centre • **Edmon Chung**, CEO, DotAsia Organisation • **Mason Cole**, Vice President, Communications and Industry Relations, Donuts • **Rocio De La Fuente**, Policy Officer, LACTLD • **Heath Dixon**, Senior Corporate Counsel - Registry, Registrar, and Domains Legal, Amazon Web Services • **Kristine Dorrain**, Senior Corporate Counsel, Amazon Web Services • **Keith Drazek**, Vice President, Public Policy and Government Relations, VeriSign • **Heather Dryden**, Senior Advisor, Canada - Department of Innovation, Science and Economic Development • **Stephanie Duchesneau**, Program Manager, Google • **Miguel Ignacio Estrada**, General Manager, LACTLD • **Rita Forsi**, Director General, Superior Institute for Communications and Information Technology, Italy - Ministry of Economic Development • **Jothan Frakes**, Executive Director, Domain Name Association (DNA) • **Grace Githaiga**, Associate, Kenya ICT Action Network (KICTANet) • **Hartmut Glaser**, Executive Secretary, Brazilian Internet Steering Committee (CGI.br) • **Rahul Gosain**, Director, IRSME, India - Ministry of Electronics and Information Technology • **Rudolf Gridl**, Head of Division, Internet Governance, Germany - Federal Ministry for Economic Affairs and Energy • **Rob Hall**, CEO, Momentous • **Statton Hammock**, Vice President of Global Policy and Industry Development, MarkMonitor • **Jamie Hedlund**, Vice President, Contractual Compliance and Consumer Safeguards, ICANN • **Ashley Heineman**, Director Global Policy, GoDaddy • **Byron Holland**, President and CEO, Canadian Internet Registry Authority (CIRA) • **Will Hudson**, Senior Advisor for International Policy, Google • **Manal Ismail**, Executive Director, International Technical Coordination, Egypt - National Telecommunications Regulatory Authority • **Peter Koch**, Senior Policy Advisor, DENIC • **Konstantinos Komaitis**, Director, Policy Development, Internet Society (ISOC) • **Allan MacGillivray**, Senior Policy Advisor to the President, Canadian Internet Registration Authority (CIRA) • **Marilia Maciel**, Digital Policy Senior Researcher, Diplo Foundation • **Polina Malaja**, Policy Advisor, Council of European National Top-Level Domain Registries (CENTR) • **Fulvia Menin**, Policy

20. An overview of the Members of the Domains & Jurisdiction Program Group by year can be found here.

Officer, European Commission, DG CONNECT • **Julie Michel**, Legal Counsel, EURid • **Desiree Miloshevic**, Senior Advisor of International Affairs and Public Policy, Afilias • **Paul Mitchell**, Senior Director, Technology Policy, Microsoft • **Cristina Monti**, Head of Sector, Internet Governance and Stakeholders' Engagement, European Commission, DG CONNECT • **Alice Munyua**, Founder, Kenya ICT Action Network (KICTANet) • **Michele Neylon**, CEO, Blacknight Internet Solutions • **Seun Ojedeji**, Chief Network Engineer, Federal University of Oye-Ekiti • Crystal Ondo, Policy & Compliance Manager, Google • **David Payne**, Vice President and Deputy General Counsel, Afilias • **Richard Plater**, Policy Executive, Nominet • **Mathieu Potter**, Policy Analyst, Canada - Department of Innovation, Science and Economic Development • **Suzanne Radell**, Senior Policy Advisor, National Telecommunications and Information Administration (NTIA) • **Rod Rasmussen**, Principal, R2 Cyber • **Vinicius Santos**, Expert Advisor, Brazilian Network Information Center (NIC.br) • **Bryan Schilling**, Consumer Safeguards Director, ICANN • **Thomas Schneider**, Head of International Affairs, Switzerland - Federal Office of Communications • **Rowena Schoo**, Policy and Government Relations Manager, Nominet • **Jorg Schweiger**, CEO, DENIC • **Tim Smith**, Executive Director/General Manager, Canadian International Pharmacy Association • **Melina Stroungi**, Policy Officer, European Commission, DG CONNECT • **Hilde Thunem**, CEO, Norid • **Geo Van Langenhove**, Legal Manager & Data Protection Officer, European Registry of Internet Domain Names (EURid) • **Peter Van Roste**, General Manager, Council of European National Top-Level Domain Registries (CENTR) • **Chris Wilson**, Senior Manager, Public Policy, Amazon Web Services • **Alan Woods**, Senior Compliance and Policy Manager, Donuts

I&JPN SECRETARIAT

LEAD DOMAINS & JURISDICTION PROGRAM:

Bertrand de la Chapelle, Executive Director
Elizabeth Behsudi, Director, Domains & Jurisdiction Program
Ajith Francis, Policy Programs Manager
Sophie Tomlinson, Communications and Outreach Manager
Juri Wiedemann, Young Professional

Paul Fehlinger, Deputy Executive Director
Martin Hullin, Director of Operations and Knowledge Partnerships
Hedvig Nahon, Events and Office Manager

FINANCIAL AND INSTITUTIONAL SUPPORTERS

This Toolkit would not exist without the support of the unique coalition of leading states, international organizations, businesses, technical operators and foundations, which enable the work of the Internet & Jurisdiction Policy Network.

Please consult the overview of these key actors and their logos at
https://www.internetjurisdiction.net/about/funding

The Internet & Jurisdiction Policy Network is the multistakeholder organization fostering legal interoperability in cyberspace. Its stakeholders work together to preserve the cross-border nature of the internet, protect human rights, fight abuses, and enable the global digital economy. Since 2012, the Internet & Jurisdiction Policy Network has engaged more than 400 key entities from six stakeholder groups around the world including: governments, the world's largest internet companies, the technical community, civil society groups, leading universities and international organizations.

www.internetjurisdiction.net