DNS Abuse Mitigation

GAC PSWG Speakers:
Gabriel Andrews (US Federal Bureau of Investigation)
Laureen Kapin (US Federal Trade Commission, Co-Chair GAC PSWG)
Chris Lewis-Evans (UK National Crime Agency, Co-Chair GAC PSWG)

GAC Speaker:
Nobuhisa Nishigata (Ministry of Internal affairs and Communications, Japan)

ICANN75

20 September 2022

ICANN | GAC
Governmental Advisory Committee

Agenda

1. **Why DNS Abuse Mitigation is Important to the GAC**
2. **Updates on Community Activities Related to DNS Abuse Mitigation**
   - Contracted Parties DNS Abuse Working group(s)
   - GNSO Small Team on DNS Abuse
   - DNS Abuse Institute
3. **Japan Presentation**
4. **Recent ICANN Compliance Audit of 28 Registries**
5. **Improvement of ICANN Contract Provisions Related to DNS Abuse**
   - ICANN's role
   - Opportunities for improvements
6. **GAC positions to date**

DNS Abuse Mitigation: Importance

Why this is important for the GAC

- **Existing definitions of Abuse of the DNS** include Security Threats such as *Phishing, Malware, Botnets* (GAC Beijing Safeguard Advice) and as "*intentionally deceptive, conniving, or unsolicited activities that actively make use of the DNS and/or the procedures used to register domain names*" (CCT Review definition quoted in the GAC Statement on DNS Abuse, 18 September 2019) **constitute**:
  - **A threat to consumers and Internet users** (individual and commercial) and their trust in the DNS
  - **A threat to the security, stability and resiliency of DNS Infrastructure**

- **The GAC established a Public Safety Working Group** (PSWG) in the ICANN52 Singapore Communiqué (11 February 2015)
  - to focus aspects of ICANN's policies and procedures that implicate the safety of the Public (see ToR)
  - As part of its strategic objectives, as reflected in its Work Plan 2020-2021, the PSWG seeks to: ***Develop capabilities of the ICANN and Law Enforcement communities to prevent and mitigate abuse*** *involving the DNS as a key resource*

- The GAC, the GAC Public Safety Working Group and **many ICANN stakeholder groups prioritize curbing DNS Abuse**, recognizing in particular that **current ICANN contracts do not provide sufficiently clear and enforceable obligations** to mitigate DNS Abuse and need to be improved. This is has been evidenced in:
  - Community discussions
  - Board correspondence (in particular with the Business Constituency in 2020/2019, see 12 Feb. 2020)
  - GAC Inputs in Reviews (CCT, RDS-WHOIS2, SSR2) and in GNSO PDPs (New gTLD Subsequent Procedures)

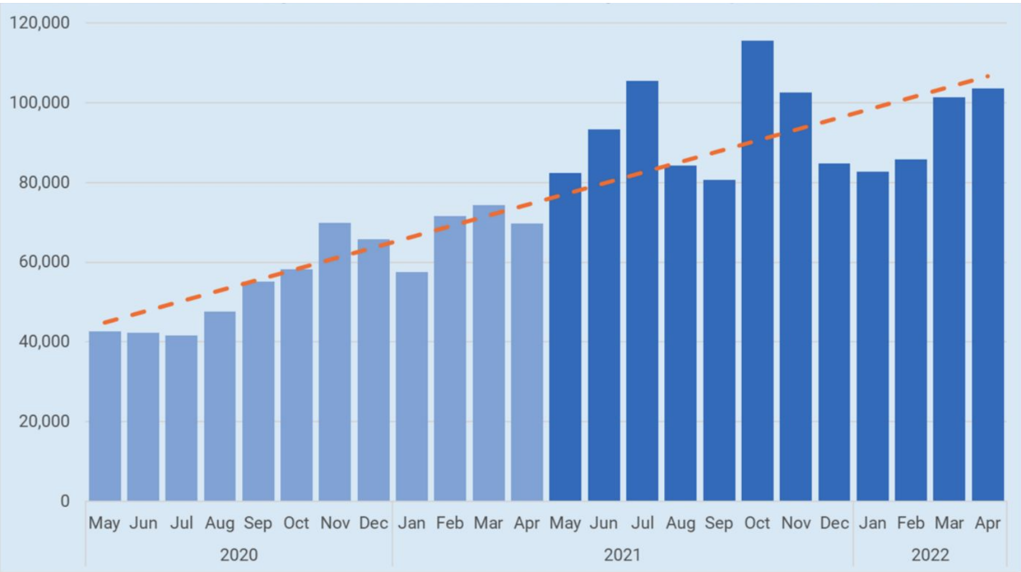
DNS Abuse Mitigation: Importance

Highlights from Interisle Phishing Landscape 2022 Report issued (19 July 2022)

- Interisle defines a Phishing Attack as “*a phishing site that targets a specific brand or entity.*”
    - ○ Web site appears to be run by a trusted entity, such as a bank or a merchant
    - ○ But. . . the web site is a deception, and the site’s content is designed to persuade a victim to provide sensitive information which may then be used for illicit purposes (identity theft; to collect credentials that →compromise/access systems and accounts; etc.)

- Over 1.1 million attacks identified (1-year) a 61% increase year-over-year*
- 854,000 unique phishing domains (1-year) a 72% increase year-over-year*

<u>Depicted:</u> Monthly number of Phishing attacks reported



Source: Phishing Landscape 2022, Interisle Consulting Group

**May 2020 to Apr. 2021 period vs. May 2021 to Apr. 2022 period*

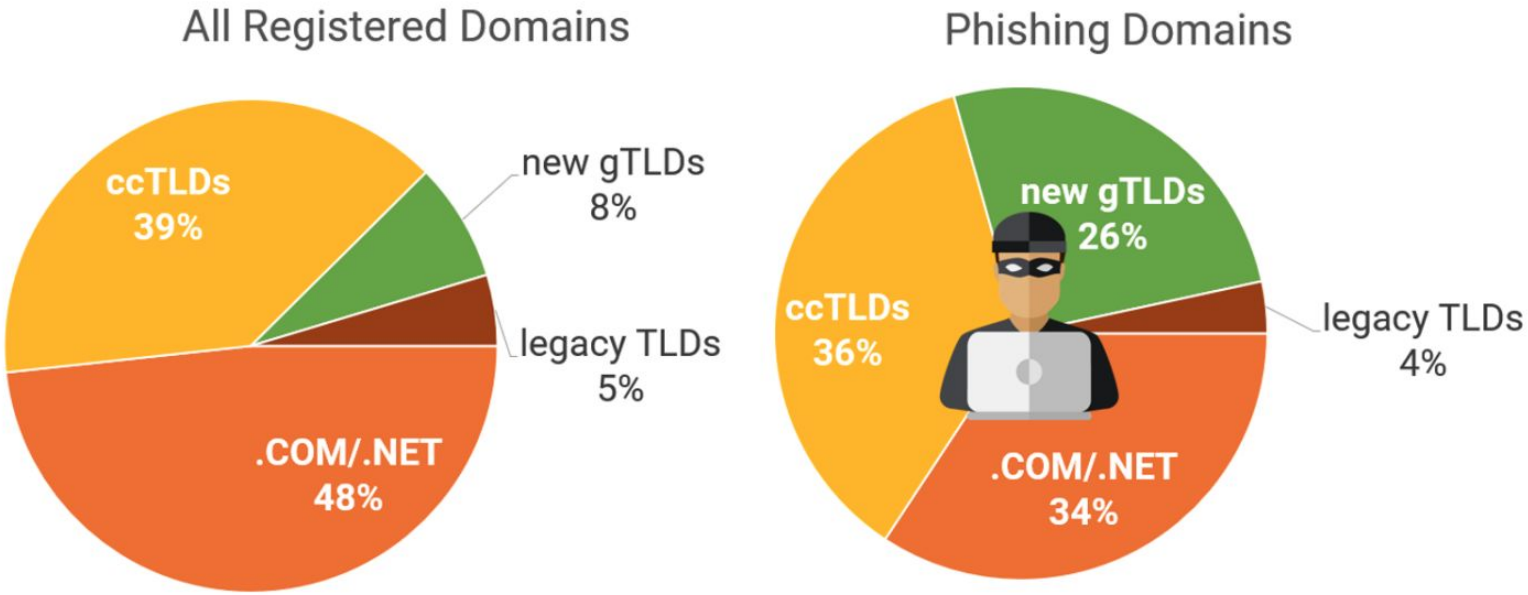
DNS Abuse Mitigation: Importance

Highlights from Interisle Phishing Landscape 2022 Report issued (continued)

Phishing remains a significant threat to millions of Internet users

- 69% of Phishing Domains observed were **maliciously registered**

- Domains registered in New gTLDs continue to be used disproportionately for phishing



Source: Phishing Landscape 2022, Interisle Consulting Group

DNS Abuse Mitigation: Importance

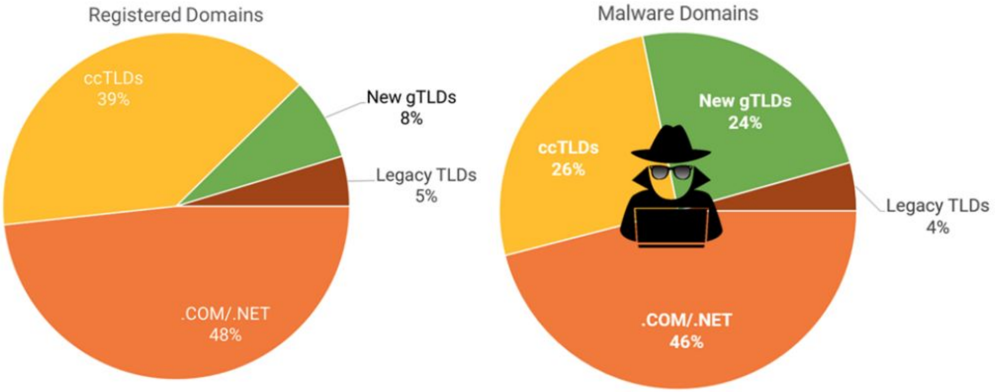
Highlights from Interisle Malware Landscape 2022 Report (June 2022)

- **Malicious code** that **can infect and compromise any device** connected to a network, including computers, smartphones, “smart home” devices, and industrial control systems

Malware reports growing

299k reports in April 2021
800k reports in March 2022

- Some types of malware create **networks of compromised machines (“botnets”)** that can be used to:
  - perpetrate **spam or phishing** campaigns,
  - or to disrupt services or merchant activities through **denial-of-service attacks**.
- Criminals use a wide variety of endpoint malware that serve different purposes:
  - **information stealing malware** (banking trojans for identity theft or fraud)
  - **backdoor trojans** (for remote control execution or administration)
  - **“Ransomware”** (particularly vicious form of malware used for digital extortion).



Source: Malware Landscape 2022, Interisle Consulting Group

Community Activities on DNS Abuse Mitigation

Contracted Parties (ICANN75 Outreach on DNS Abuse)

- A **Discussion Paper on Malicious vs. Compromised Domains** is expected from Contracted Parties before the end of the year.

- Registries are working on **voluntary sharing of statistics** relating to "evidenced and escalated" instances of DNS Abuse, as part of their obligation to monitor Security Threats (RA Specification 11 3b)

  > *Registry Operator will periodically conduct a technical analysis to assess whether domains in the TLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets. Registry Operator will maintain statistical reports on the number of security threats identified and the actions taken as a result of the periodic security checks. [...]*

- The Registrar Stakeholder Group developed acidtool.com (Abuse Contact IDentifier) to provide contact information of relevant parties to whom to direct **DNS Abuse reports**, including: hosting and email service providers, registrar and registrant.

- During ICANN74 the DNS Abuse Institute presented to the GAC netbeacon.org,
  a free centralized reporting tool (for phishing, malware, botnets and spam) which standardizes and enriches reports and distributes them automatically to registrars (currently only for gTLDs).

- The DNS Abuse Institute shared its first monthly report on **DNS Abuse trends**, measuring phishing and malware, including levels of mitigation, time to mitigation, and distribution between compromised and malicious domains.

Community Activities on DNS Abuse Mitigation

GNSO Small Team on DNS Abuse

- Formed in January 2022, tasked to "*consider what policy efforts, if any, the GNSO Council should consider undertaking*" including "*to better understand what tackling DNS Abuse means [...] and what constitute DNS abuse being addressed*"

- The GAC provided a response (4 April 2022) to this team's **outreach to the Community**. Other community responses were received from the ALAC, the SSAC, the BC, RySG and DNS Abuse Institute.

- **Expected preliminary recommendations** for the GNSO Council (shortly) to:
  - Consider requesting a Preliminary Issue Report towards initiating a tightly focused PDP on the topic of **malicious registrations** used for the distribution of malware, phishing or the operation of Botnet command and control systems
  - Encourage Contracted Parties to promote/improve tools to simplify **reporting of DNS Abuse**
  - Recommend Contracted Parties to consider **addressing lack of clarity and diverging interpretation with ICANN Compliance of certain DNS Abuse mitigation obligations** (including steps registrars are to take in response to abuse reports, and inclusions of DNS Abuse provision in Registry/Registars Agreement) and possibly set a baseline of behavior/practices that most Contracted Parties already follow.

Community Activities on DNS Abuse Mitigation

Security and Stability Advisory Committee (SSAC)

- Role of SSAC:
  - focuses on matters relating to the security and integrity of the Internet’s naming and address allocation systems
  - engages in ongoing threat assessment and risk analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie, and advises the ICANN community accordingly

- Two recent inputs relate to DNS Abuse:
  - SAC 114 - SSAC Comments on the GNSO New gTLD Subsequent Procedures (“next round”) Draft Final Report (Feb. 2021)
  - SAC115 - SSAC Report on an Interoperable Approach to addressing Abuse Handling in the DNS (March 2021)

Community Activities on DNS Abuse Mitigation

Security and Stability Advisory Committee (SSAC)

- SAC 114 - SSAC Comments on the GNSO New gTLD Subsequent Procedures (“next round”) Draft Final Report
    - while SSAC agrees that a **holistic approach to DNS abuse issues has merit**
    - security threats and attendant **abuse of the DNS remain a constant and rapidly evolving challenge**, and that ICANN recognizes “Domain name abuse continues to grow” as a Strategic Risk 4 to the achievement of its Strategic Objectives
    - **waiting** until efforts to mitigate DNS abuse can be equally applied to all existing and new gTLDs **effectively cedes the ground to malicious actors** who can depend upon a long policy development process to hinder meaningful anti-abuse measures
    - **recommends** that the ICANN Board, prior to launching the next round of new gTLDs, commission **a study of the causes of, responses to, and best practices for the mitigation of the domain name abuse** that proliferates **in the new gTLDs** from the 2012 round
    - **best practices should be incorporated into** enforced requirements, as appropriate, for at least **all future rounds**

Community Activities on DNS Abuse Mitigation

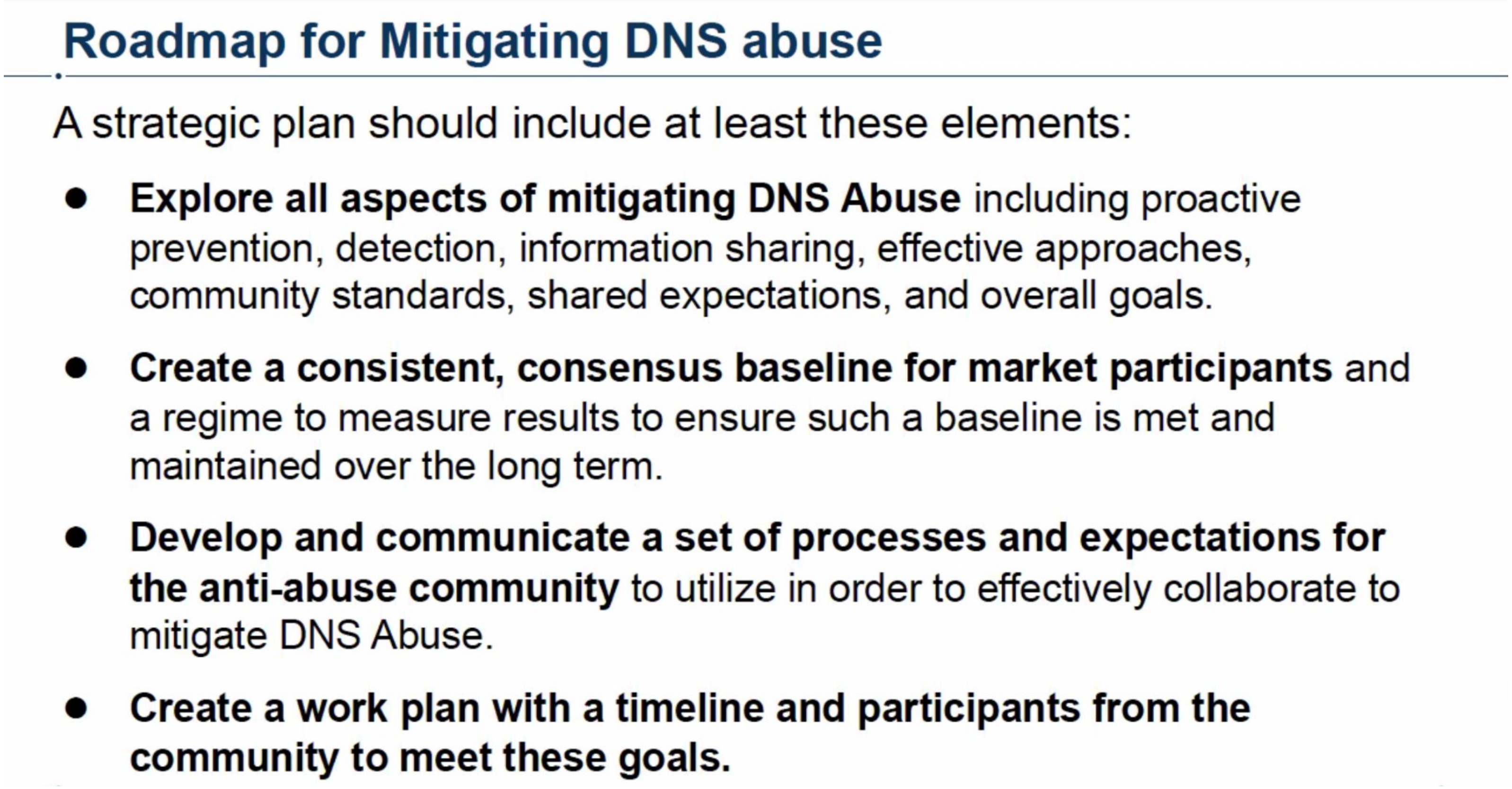
Security and Stability Advisory Committee (SSAC)

- SAC115 - SSAC Report on an Interoperable Approach to Addressing Abuse Handling in the DNS
  - **Proposed Framework:**
    - Primary Point of Responsibility for Abuse Resolution
    - Escalation Paths
    - Evidentiary Terminology and Standards
    - Reasonable Time Frames for Action
    - Availability and Quality of Contact Information
  - **The SSAC recommends** that the ICANN community continue to work together with the extended DNS infrastructure community in an effort to:
    1. **examine and refine the proposal for a Common Abuse Response Facilitator** to be created to streamline abuse reporting and minimize abuse victimization
    2. **define the role and scope of work for the Common Abuse Response Facilitator**, using SAC115 as an input.

Community Activities on DNS Abuse Mitigation

Security and Stability Advisory Committee (SSAC)

- SSAC presentation during the GNSO Council Working Session (18 Sep.): Proposal to create a **cross-community Roadmap for mitigating DNS** Abuse, bridging ICANN's Strategic Objectives and ongoing community activities (to be discussed between SSAC and ICANN Board in KL)



Roadmap for Mitigating DNS abuse

A strategic plan should include at least these elements:

- **Explore all aspects of mitigating DNS Abuse** including proactive prevention, detection, information sharing, effective approaches, community standards, shared expectations, and overall goals.
- **Create a consistent, consensus baseline for market participants** and a regime to measure results to ensure such a baseline is met and maintained over the long term.
- **Develop and communicate a set of processes and expectations for the anti-abuse community** to utilize in order to effectively collaborate to mitigate DNS Abuse.
- **Create a work plan with a timeline and participants from the community to meet these goals.**

Japan Presentation

Overview

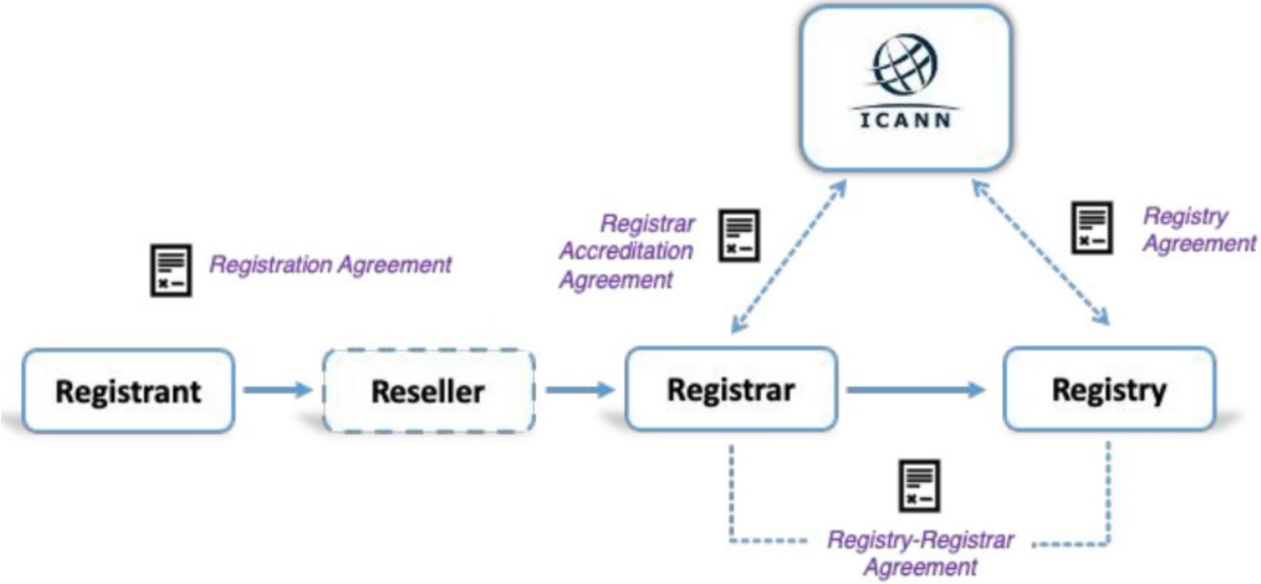
Japan has been engaged in the DNS Abuse discussion since ICANN70.

➢ Responding to the whole-of-government action plan against Manga piracy platforms

During the sessions, Japan…

✓ Identified strategies of malicious registrants to avoid detection (e.g. domain hopping)

✓ Proposed the discussion, particularly on the improvement of contract terms



Japan Presentation

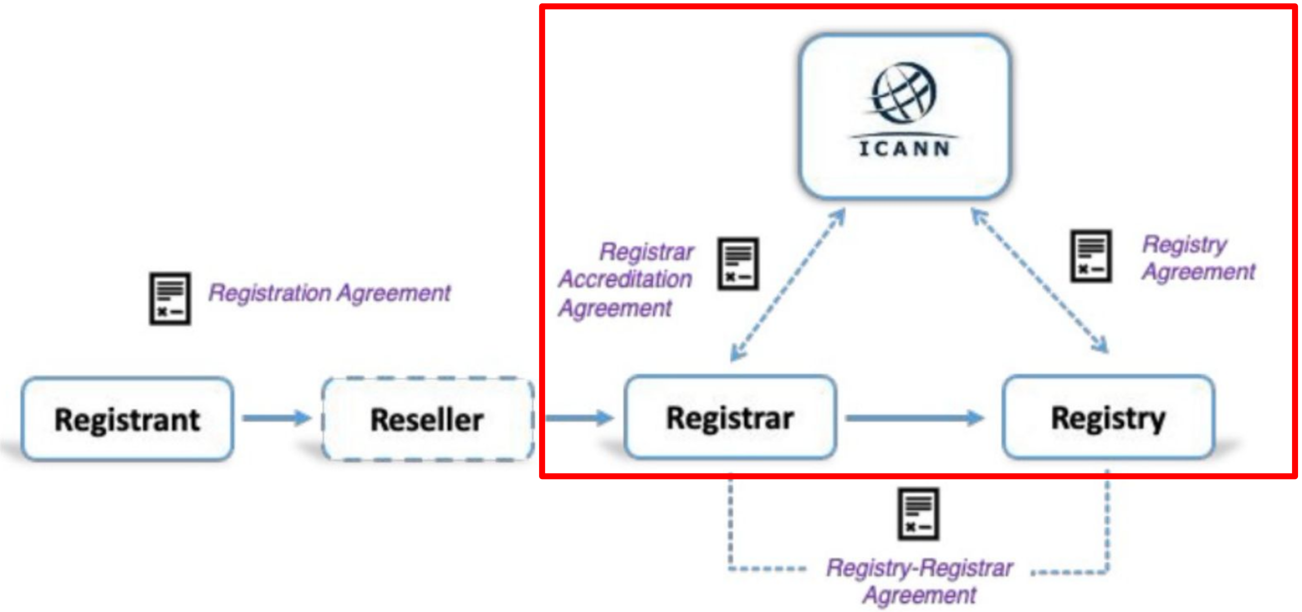
Overview

Japan has been engaged in the DNS Abuse discussion since ICANN70.

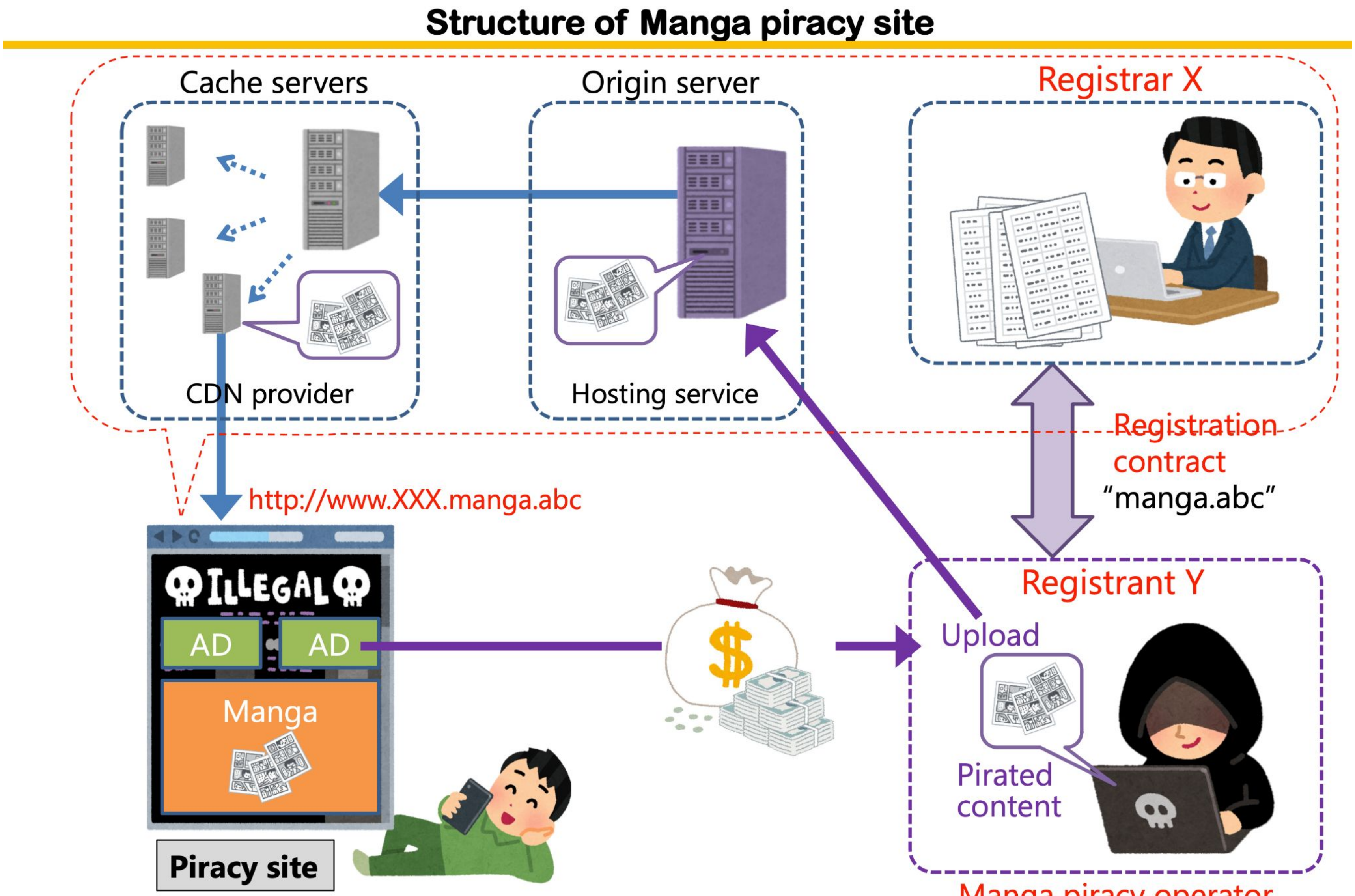
- ➢ Responding to the whole-of-government action plan against Manga piracy platforms

During the sessions, Japan…

- ✓ Identified strategies of malicious registrants to avoid detection (e.g. domain hopping)
- ✓ Proposed the discussion, particularly on the improvement of contract terms

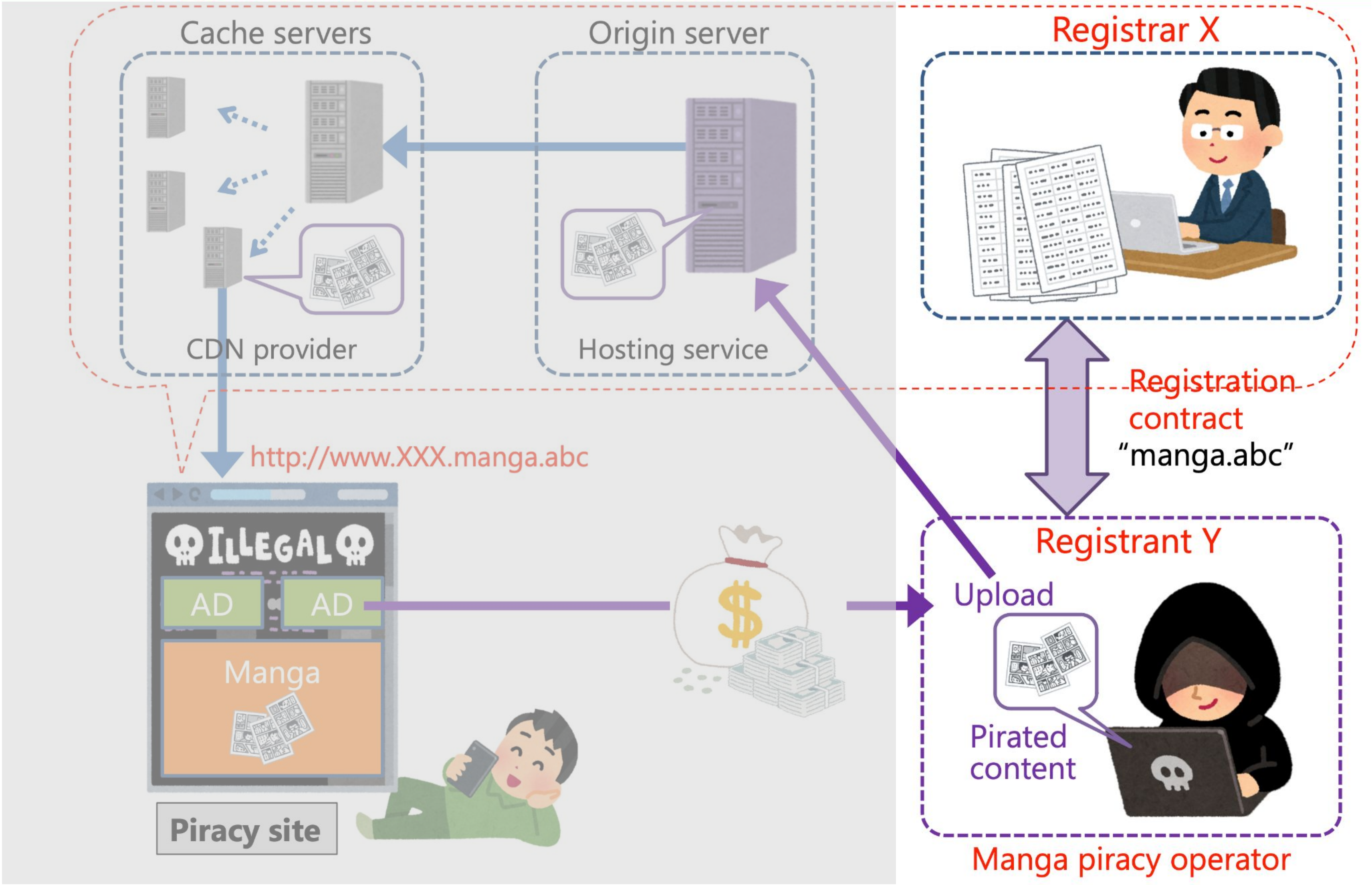


Japan Presentation



Japan Presentation

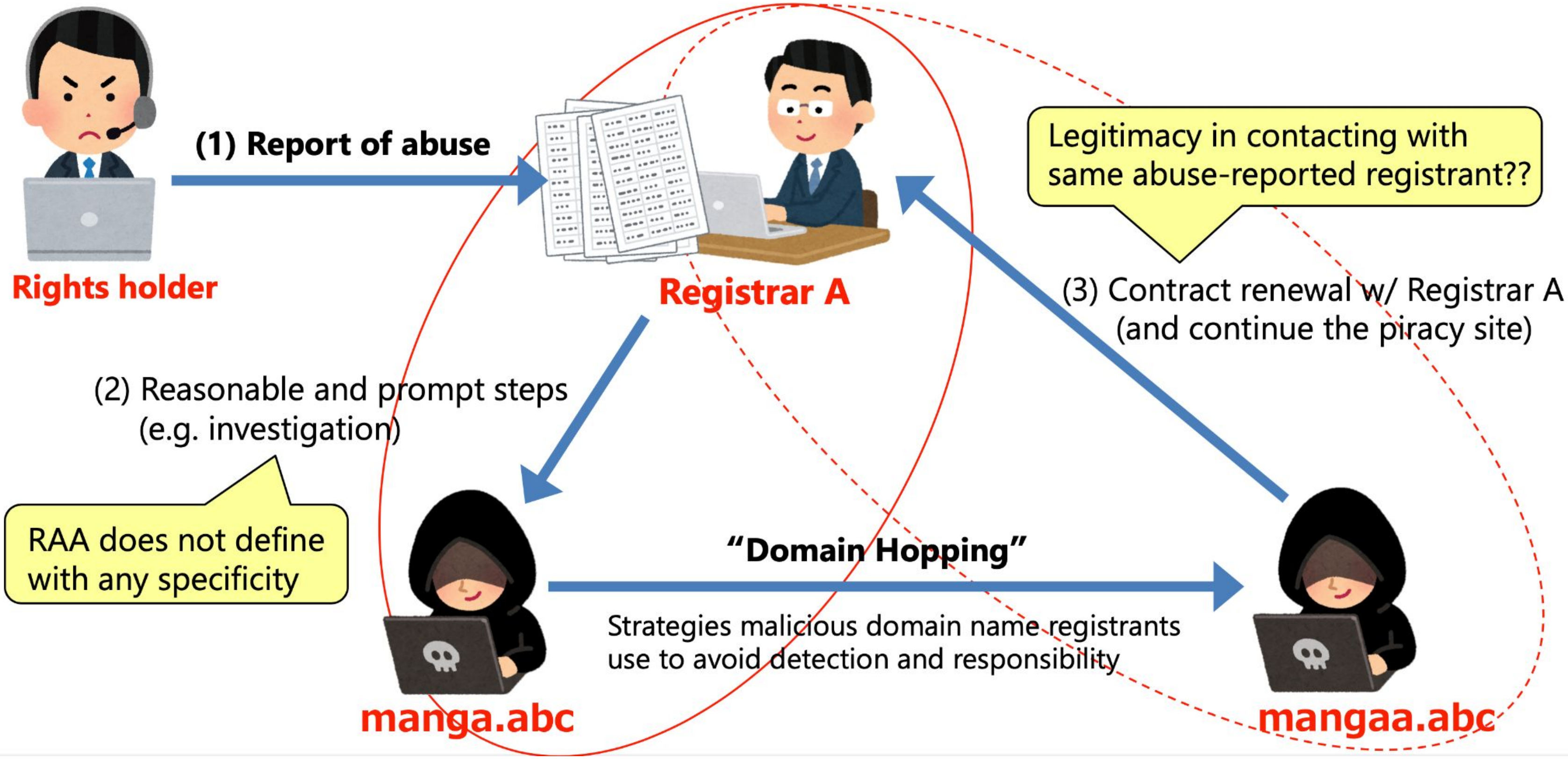
Structure of Manga piracy site



Japan Presentation

Possible improvement in RAA contract terms

3.18 Registrar's Abuse Contact and Duty to Investigate Reports of Abuse.
3.18.1 Registrar shall maintain an abuse contact to receive reports of abuse involving Registered Names sponsored by Registrar, including reports of Illegal Activity. Registrar shall publish an email address to receive such reports on the home page of Registrar's website (or in another standardized place that may be designated by ICANN from time to time). Registrar shall **take reasonable and prompt steps** to investigate and respond appropriately to any reports of abuse.



Rights holder

(1) Report of abuse

Registrar A

Legitimacy in contacting with same abuse-reported registrant??

(3) Contract renewal w/ Registrar A (and continue the piracy site)

(2) Reasonable and prompt steps (e.g. investigation)

RAA does not define with any specificity

"Domain Hopping"

Strategies malicious domain name registrants use to avoid detection and responsibility

manga.abc

mangaa.abc

Results of Compliance Audit of 28 Registries

- **Latest Audit** by ICANN Compliance announced on 13 April 2022
  - Audit of 28 gTLDs registries not previously subject to a full-scope audit, found to have the highest abuse score as reported by publicly available Reputation Blocklists (excluding Spam)

    .africa .app .art .bar .best .blog .buzz .cat .cloud .club .com .coop .gift
    .icu .ink .istanbul .moe .one .ooo .org .ren .ryukyu .tel .tirol
    .xin 我爱你 (Xn--6qq986b3xl) .닷컴 (Xn--mk1bu44c) .Pyc (Xn--p1acf)
  - Audit Report published on 16 September 2022

- **Summary of results**
  - 3 registries (11%) received an audit report with no initial findings.
  - 10 registries (36%) whose reports had initial findings, were able to fully resolve them
  - 15 registries (54%) were unable to fully resolve their initial findings prior to the completion of the audit.

- **Some good behavior too:** actions taken in addressing abusive domain reports include:
  - contacting the sponsoring registrar to investigate the reported domain and
  - suspending the domain name in case of an abuse validation.

Results of Compliance Audit of 28 Registries

- **Audit Issues** (selected) and ***Potential Impact Analysis*** *by ICANN Compliance*
  - **WHOIS educational materials not found on registry webpage**: **11 Registries (39%)**
    Public and potential customers might be unaware of the use and importance of accurate WHOIS information
  - **Abuse contact email is not responsive** to ICANN's testing: **8 Registries (29%)**
    May result in Internet users' inability to contact the gTLD registry with abuse comments or complaints.
  - **Insufficient technical analysis of Security Threats**: **3 Registries (11%)**
    A number of security threats sources remain unidentified and not acted upon.
  - **Registry/Registrar Agreement missing Required DNS Abuse Clause** **2 Registries (7%)**
    Removes the contractual basis for terminating a domain name registration, which is operating in an abusive manner.

Note: *All registries provided ICANN with a specific remediation plan, which includes the estimated time for completion; in the process of implementing necessary changes to prevent the instances of non-compliance from recurring in the future. ICANN will confirm that remediation plans have been implemented.*

Contracts and Improvements

What is ICANN’s role ?

- Defined in Articles of Incorporation, Bylaws and Contracts with Registries and Registrars
  - Not-for-profit public benefit corporation, promoting the global public interest in the operational stability of the Internet
  - Mission: ensure the stable and secure operation of the Internet's unique identifier systems
  - May negotiate, enter into and enforce agreements, including public interest commitments, with any party in service of its Mission
  - Commits to duly taking into account the public policy advice of governments and other public authorities

Contracts and Improvements

Current ICANN Contracts

- ICANN's standard Registry Agreement (Spec 11.3.a) required new gTLD registry operators to include provisions in their Registry-Registrar Agreements (RRA) that prohibited registrants from:
  - distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law
    - but what happens when the registrant breaks this agreement with the registrar?

- Registry Operators must "periodically conduct a technical analysis to assess whether domains in the TLD are being used to perpetrate security threats, **such as** pharming, phishing, malware, and botnets."
  - but what needs to happen next?

- ICANN's standard contract for Registrars requires registrars to promptly "investigate and respond appropriately to any reports of abuse" (RAA 3.18.1)
  - Board 2/20 letter: "The RAA does not define, with any specificity, what "reasonable and prompt steps to investigate and respond appropriately" means.

Cross-community discussions on reporting, handling, and enforcement of contract terms for DNS Abuse could help to address this lack of "specificity."

Contracts and Improvements

Potential topics for discussion with Community Groups

1. **Incentives**
   - ○ Financial:
     - – contracted parties with portfolios with less than a specific percentage of abusive domain names could receive a **fee reduction** on chargeable transactions up to an appropriate threshold
     - – additional financial incentives to contracted parties without any abusive domain names
   - ○ Reputational:
     - – ICANN could consider collating and **publishing reports of the actions that Registries and Registrars have taken**, both voluntary and in response to legal obligations, to respond to complaints of illegal and/or malicious conduct

Reference:
SSR2 Review Team Final Report (21 January 2021) - Recommendation 12.4; 14.2 and 14.5
GAC Comments on the SSR2 Final Report (8 April 2021)

Contracts and Improvements

Potential topics for discussion with Community Groups

2. **Thresholds of Abuse and Compliance Triggers**
   - Include provisions aimed at **preventing systemic use** of specific registrars or registries **for DNS Abuse.**
   - **establish thresholds of abuse** at which compliance inquiries are automatically triggered, with a higher threshold at which registrars and registries are presumed to be in default of their agreements.
   - **set specific deadlines** for contracted parties to reduce the fraction of abusive domains below the threshold or to demonstrate that ICANN's conclusions or data are flawed.
     - if a contracted party fails to rectify within a determined period, ICANN Contractual Compliance could consider sanctions (i.e. move to the de-accreditation process).

Reference:
CCT Review Team Final Report (8 September 2018) - Recommendation 15
SSR2 Review Team Final Report (21 January 2021) - Recommendation 9.2 and 14.4
GAC Comments on the SSR2 Final Report (8 April 2021)

GAC Positions

GAC ICANN69 Communiqué (23 October 2020)

- The GAC took "*note of the GNSO Subsequent Procedures PDP Working Group determination that* ***DNS Abuse issues should be addressed in a holistic manner****,* ***such that any proposed approach/methodolog****y for addressing DNS abuse* ***would be applicable to both existing and new gTLDs***"
- The GAC noted that is belief that "*[b]eginning with the recommendations from the CCT-RT and the SSR2 RT and continuing through several cross-community sessions and more recent work on a DNS Abuse Framework",* "***there is now a solid expression of broad support for concrete steps to be taken*** *to address the core components of effective DNS abuse mitigation".*
- The GAC indicated that it "*stands* ***ready to work with the ICANN Board and the Community*** *to advance this shared goal, including* ***through proposals to improve policies and/or improve contract provisions and enforcement****, in relation to curbing DNS Abuse."*

GAC ICANN70 Communiqué (25 March 2021)

- The GAC stated that "***DNS Abuse should be addressed in collaboration with the ICANN community and ICANN org prior to the launch of a second round of New gTLDs****. The GAC supports the development of proposed contract provisions applicable to all gTLDs to improve responses to DNS Abuse."*
- The GAC emphasized "*the i****mportance of taking measures to ensure that Registries, Registrars and Privacy/Proxy Services providers comply with the provisions in the contracts*** *with ICANN, including audits."*
- The GAC welcomed "*the recently-launched* ***DNS Abuse Institute*** *and encouraged community efforts to* ***cooperatively tackle DNS Abuse in a holistic manner***"

GAC Positions

GAC ICANN71 Communiqué (21 June 2021)

- The GAC recognized "*the **collaborative efforts taking place within the ICANN community to develop voluntary mechanisms to address DNS Abuse**, such as the Framework on Domain Generating Algorithms Associated with Malware and Botnets, and appreciates the **efforts from all parties within the multistakeholder community to identify opportunities for advancement on the topic** of DNS Abuse when and where possible*".
- The GAC acknowledged "*the **importance of ensuring that registries and registrars comply with ICANN contractual obligations***" noting that *"At the same time, **the GAC continues to emphasize the need to develop and implement improved contract provisions**, with clear and enforceable obligations, to better address DNS Abuse before further expanding the root through any subsequent application round for new gTLDs.*"
- The GAC indicated "*it will continue to closely follow developments within the community*" related to "***Improvements to the measurement, attribution, and reporting of abuse***" which it stressed were "*much needed*"

GAC ICANN72 Communiqué (1 November 2021)

- The GAC highlighted "***the need for improved contract requirements to address the issue of DNS Abuse more effectively**. In this regard, ICANN's role under the Bylaws includes duly taking into account the public policy concerns of governments and public authorities and acting for the benefit of the public.*"
- The GAC noted that *"The Bylaws also authorize ICANN to negotiate agreements, including Public Interest Commitments, in service of its Mission. Hence, **ICANN is particularly well placed to negotiate improvements to existing contracts to more effectively curb DNS Abuse, as informed by the GAC and other stakeholders** advocating in the public interest."*
- The GAC emphasized *"the **importance the GAC places in the work of ICANN compliance** not least in ensuring registrars and registries comply with the undertaking they give when registering a name."*

GAC Positions

GAC ICANN73 Communiqué (14 March 2022)

- The GAC reported its discussion of "*a **recent study on DNS abuse** provided by the European Commission*" which "*provides **recommendations on how the different actors** (e.g., registries, registrars, resellers, hosting providers, registrants, etc.) **can respond to DNS abuse** that takes place within the different layers of the DNS system*"
- The GAC noted that "*While not all harmful or illegal activities covered by the study fall into ICANN's remit, **the GAC is an important venue for governments to discuss DNS abuse and work toward solutions** that can be accomplished **both within and outside ICANN.***"
- The GAC expressed "*appreciation for the DNS Security Facilitation Initiative Technical Study Group's Final Report [...] which addressed real-world security incidents targeting DNS infrastructure and recommended actions for ICANN org [...]*"
- The GAC noted "*the news pertaining to the **forthcoming launch of a Centralized Abuse Reporting Tool** (CART), as developed by the DNS Abuse Institute, and expressed interest in receiving more detailed information*"
- The GAC also noted "*it was **universally agreed** [during a plenary session] that the **distinction [between malicious and compromised domains] is important**, and the GAC supports the community exploring the **opportunities highlighted [...] for further work to disrupt DNS Abuse***".

GAC Positions

GAC The Hague Communiqué (20 June 2022)

- The GAC reiterated “***the importance of building on the community’s work on DNS Abuse***” and highlighted “*the **continued importance of effectively responding to DNS Abuse**”* and shared its appreciation for *“the continued work by ICANN org and the ICANN community on these issues”*
- The GAC noted that “***Enhanced Abuse Reporting would*** *enable more focused dialogue within the ICANN community and **provide the basis for targeted contractual improvements**”*
- The GAC welcomed *“the **launch of a free, centralized abuse reporting tool by the community** in response to recommendations made in both SAC115 and the SSR2 Review Final Report.”*
- The GAC stated that “***Improved contract provisions could focus*** *on the reporting and handling of DNS Abuse and enforcement of related contract requirements*” and that “*In its role as a public benefit corporation tasked with ensuring the stability and security of the Internet’s unique identifier systems, **ICANN org is particularly well placed to receive public policy input from the ICANN community and negotiate updates to the standard Registry and Registrar Agreements**. This would help ensure that these contracts promote the public interest by including clear and enforceable obligations to detect and respond to DNS Abuse.*
- The GAC also stated that “***Targeted Policy Development Processes (PDPs) could also yield contract improvements***. *Any PDP on DNS Abuse should be narrowly tailored to produce a timely and workable outcome.”*