31-Aug-2023

International Regulation and Trade Team
Department for Science, Innovation and Technology
5th Floor
100 Parliament Street
London
SW1A 2BQ

VIA EMAIL: ukdomainnames.consultation@dcms.gov.uk

Consultation reference: Powers in Relation to UK-Related Domain Name Registries: *Proposed requirements for UK-related domain name registries when tackling domain name abuse*.

Dear International Regulation and Trade Team:

The Business Constituency (BC) of the Internet Corporation for Assigned Names and Numbers (ICANN) is the representative body of worldwide business users of the internet. Our constituency represents global businesses ranging from startups in historically economically disadvantaged regions to the Fortune 50. We write in relation to the above-referenced consultation. Thank you for the opportunity to submit comment on this important matter.

The BC, for years, has been concerned about the growing incidences of domain name system (DNS) abuse, and has devoted time and resources both inside and outside the ICANN model to combat this persistent problem. While we have been encouraged by industry's efforts to dissuade such corrosive behavior, such steps do not fully address the misuse and abuse problem that has continued to expand. Accordingly, on behalf of the businesses we represent, we welcome this consultation and encourage your office to continue this important discussion.

BC input context: Our overarching considerations

DNS abuse is a persistent and growing problem
Industry research and documentation have long demonstrated that phishing, malware, infringement, and other forms of abuse and misuse continue to show a disturbing upward trend. For example:

- In its most recent study on phishing trends[1], Interisle Consulting Group found that:
  - *The number of phishing attacks has tripled since May 2020.* Further, phishing attacks during Interisle's annual study period from May 2022 to April 2023 increased 65% over the previous study period (May 2021 to April 2022).
  - *The number of unique domain names reported for phishing continues to increase*. More than one million unique domain names were reported for phishing during the current period, the most observed since Interisle began observations in May 2020.
  - *Two-thirds of domain names reported for phishing across all top-level domains (TLDs) were registered specifically to carry out phishing*. Malicious domain name registrations are the most common way that phishers carry out their attacks. Preventing the registration of these domains, and taking them down quicky, should be a priority for the domain name industry, said Interisle.
- The Cybercrime Information Center published a recent report detailing that the monthly number of phishing attacks reported has more than doubled since 1 May 2020.[2]
- The World Intellectual Property Organization (WIPO) has observed a steady increase year over year in the number of domain names subject to adjudication under the Uniform Domain Name Dispute Resolution

[1] https://interisle.net/PhishingLandscape2023.pdf
[2] https://www.cybercrimeinfocenter.org/phishing-landscape-2022

Policy (UDRP); in 2022 alone, WIPO handled 9,580 disputes, and the 2023 total to date is on pace to exceed the 2022 total.[3]

- The growth of WIPO's caseload is underlined by the latest report by domain name legal expert Doug Isenberg (who reports frequently on UDRP trends). Isenberg writes that "[Indeed,] all of the active UDRP service providers are experiencing bigger caseloads, with increases ranging from about 6 percent (at WIPO) to 330 percent (at the much smaller Canadian International Internet Dispute Resolution Centre) in the number of domain names in reported UDRP decisions this quarter versus the first quarter of the year."[4]

The BC must raise a complicating factor in the ability to address abuse and misuse: this is the lack of ability, via cooperation by registries and registrars, for authorities to act *at scale*. At present, addressing abuse often is done domain name-by-domain name, and not at a higher "party" level – that is, where it is known that one party is employing hundreds of domain names in an abusive campaign. Cooperation by registries and registrars to identify and take action against a single party would help those victimized by abuse to deal with broad swaths of domain names at one time.

As noted in Interisle's recent report, "[p]hishing leverages Internet resources, exploits vulnerable technologies, and takes advantage of policy and legislative regimes that are siloed and often ineffective." The BC agrees with Interisle's observation that "[t]he problem is worsening — domain registrars, domain registries, and web hosting services have not kept pace with preventative measures to reduce the total amount of phishing." As a result, we're encouraged by the direction that the UK is taking with this proposal.

Definitions of DNS abuse are too restricted

From its consultations within the ICANN community, the BC is very aware that registries and registrars have assigned a definition to the "abuse" term that is extremely restricted: Pharming, malware, phishing, botnets, and spam as a delivery mechanism for the first four. This definition, obviously, excludes multiple types of harm.

Even ICANN's Security and Stability Advisory Committee (SSAC), which advises ICANN's Board of Directors regarding DNS stability matters, says this definition is woefully short:

> "These categories have been adopted within the ICANN realm in specific contracts, but do not represent all forms of DNS abuse that exist, are reported, and are acted upon by service providers. New types of abuse are commonly created, and their frequency waxes and wanes over time. Thus, **no particular list of abuse types will ever be comprehensive**." (Emphasis added)

Further emphasizing this deficit, the BC notes further expert input from researchers Maciej Korczynski, Ivett Paulovics and Andrzej Duda, who in 2022 conducted a European Commission-sponsored study[5] on DNS abuse. The three wrote:

> **Domain Name System (DNS) abuse is any activity that makes use of domain names or the DNS protocol to carry out harmful or illegal activity.** (Emphasis added)

Lack of public access to domain name registration data has halted investigatory capability

Many registries and registrars elected to eliminate publicly available registration data (known as WHOIS data) following the entry into force of the European Union's General Data Protection Regulation (GDPR). Accordingly, investigations of online harms in the UK and elsewhere have been effectively halted entirely.

---

[3] https://www.wipo.int/amc/en/domains/statistics/domains.jsp

[4] https://static1.squarespace.com/static/58febdfcbf629aa913a85974/t/64c260ff752b6d747c8f069c/1690460416144/2023-q2-domain-dispute-digest.pdf

[5] https://op.europa.eu/o/opportal-service/download-handler?identifier=7d16c267-7f1f-11ec-8c40-01aa75ed71a1&format=pdf&language=en&productionSystem=cellar&part=

In their operations, registries and registrars often outright refuse to reveal a domain name registrant's contact information, even in instances when that name has been suspended for abuse. The problem is exacerbated by privacy and proxy services, which further mask a registrant's identity. Even when evidence is supplied documenting abuse, misuse, cybersquatting and other harms, registries and registrars seldom cooperate with requests for disclosure. It is hoped by those concerned with this lack of investigatory capability that WHOIS data can be made available for domain names that are termed "misused" or "abusive" under a reasonably inclusive definition.

There *is* one bright spot: The EU's Directive on the Security of Network Information Systems (NIS2) includes new requirements for collection and maintenance of accurate and verified registration data by registries and registrars; however, the ultimate impact of NIS2 outside the jurisdiction of the EU remains to be seen. Nonetheless, the UK should consider mandating WHOIS obligations similar to those set forth in the Directive's Article 28 and related recitals (for example, mandatory implementation of "thick" WHOIS records, containing complete and accurate registrant data), which would have a substantial impact on the incidences of domain name abuse and misuse.

Domain name registrars also play a key role in combating DNS abuse

This consultation is appropriately oriented toward domain name registries; however, we welcome the inclusion of registrars as subjects for comment. Registrars facilitate registrant domain name registration transactions and thus are the main channel for communication with or enforcement against infringing name holders. Their role is therefore substantial.

Mandates for DNS misuse mitigation should be enshrined in contracts

To ensure that registries and registrars fulfill their public safety responsibilities, the BC recommends updates to the contracts governing their obligations in a matter that guarantees compliance and enforceability. We further recommend that stricter policies be adopted for mitigation of DNS abuse and cybersquatting that "flow" from registries to registrars and are accordingly enforceable by registries.

Our replies to consultation questions (See Consultation)

1. Do you agree we should include all of the types of misuses of domain names set out under the 'Domain Name Misuse' heading, in our 'prescribed practices'? If not, which ones should be omitted and why?

The BC agrees that all forms of misuse (as documented in Sections 3 and 4 of the consultation) are appropriate for inclusion. Further, DNS abuse should be consistent with the principles of cybercrime as outlined in the Budapest Cybercrime Convention, which includes child sexual abuse material (CSAM), infringements on copyrighted and related rights, and abuse defined as "fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person."[6] Having a common criminal policy to serve as a baseline could facilitate multi-jurisdictional mitigation efforts, and it would obviate the need for unproductive discussions over what constitutes DNS abuse.

We respectfully repeat here, however, the important waring issued by ICANN's SSAC: that no list of types of abuse ever will be considered comprehensive. For example, "abuse" can and should include problems such as domain name compromise, intellectual property (IP) infringement, malicious registrations, and other types of harm. The BC strongly encourages the International Regulation and Trade Team to incorporate latitude into any working definition of abuse to accommodate evolving types of misuse, as advised by SSAC and other industry authorities.

The BC notes that the consultation proposal does not include a definition of "domain name" itself and observes the current proliferation of alternative root domain names, which are subject to *no* oversight by ICANN – or by *any* organization concerned with pragmatic governance and the public interest. As a result, we recommend that the

[6] https://rm.coe.int/1680081561

UK consider adopting an inclusive definition of domain names to ensure that the best practices contemplated herein apply to all types of names.

2. Are the descriptions of the types of domain name misuses set out under the 'Domain Name Misuse' heading fair and appropriate for the purposes of including them in our 'prescribed practices'? If not, please explain why not and propose alternative descriptions.

Yes. However, as noted in reply to Question 1 above, the list should be considered incomplete.

3. Are there any other types of domain name misuse that should be included in the 'prescribed practices'? If so, please describe them and provide reasons as to why you think they should be included.

Yes. Broadly speaking, any type of crime that leverages the DNS should be a candidate for inclusion as types of misuse. And, as stated, no list of types of misuse ever will be comprehensive, given the evolving nature of developing threats. However, the following non-exhaustive list should be considered timely for addition to the relevant list of types of misuse:

Domain name compromise: Wrongfully taking control of a domain name from the rightful name holder, often used for different types of malicious activity (such as phishing, malware distribution, or botnet control). This type of abuse often is enmeshed as a tactic of already articulated varieties of misuse.

IP infringement: The use of the DNS to falsely represent, or attempt to represent, the identity of an established brand, product or service or the operation of a website under a domain name that is dedicated to the sale of counterfeit goods or to copyright piracy. IP infringement through the DNS costs UK businesses millions per year in economic damages. In addition, infringement through the DNS can be a threat vector itself, as misrepresented brands, products and services frequently lure users into becoming victims of multiple types of cybercrime.

Malicious registrations: The intentional registration of domain names to engage in technical and/or content abuse. A domain is generally flagged as malicious if it is reported a very short time after registration, contains a brand name or misleading "string" of characters, or is one of many registered in a batch. Related sometimes (but not limited to) IP infringement, malicious registrations intend to defraud or confuse internet users or otherwise disrupt the flow of information or commerce. This is a critical issue – in its recent study, Interisle "determined that [for the study period] 65% of the domains reported for phishing across all TLDs were registered maliciously by phishers (725,520 of the 1,124,684 domains reported for phishing)."

Domain generation algorithms (DGAs) used for illegal activities: Often used in conjunction with "bulk registration" functions, DGAs dynamically identify a destination domain for command and control traffic rather than relying on a list of static internet protocol addresses or domains. This has the advantage of making it much harder for cybersecurity defenders to block, track, or take over the command and control channel, as there potentially could be thousands of domains that malware can "check" for instructions. While there are legitimate uses of DGAs that should not be prohibited, the proposal should address DGAs used for illegal activities, such as to spread malware or to accelerate phishing attacks.

Sale of Illicit/Counterfeit Pharmaceuticals: This crime often is conducted through domain names used to facilitate the online sale of pharmaceuticals illegally. Counterfeit and/or illegal medications are regularly sold, in contravention of public health concerns, using domain names intentionally registered for such illegal activity.

4. Do you agree with the proposal to include 'cybersquatting' (including 'typosquatting') in the list of unfair uses of domain names in our 'prescribed practices'? If not, why?

Yes. This is a longstanding problem in the DNS.

5. Is the description of 'cybersquatting' fair and appropriate for the purposes of including it in our 'prescribed practices'? If not, please explain why not and propose an alternative description.

Yes. As documented in prescribed practices, cybersquatting is the pre-emptive, bad faith registration of trademarks as domain names by third parties who do not possess rights in such names. Despite the existence of the Uniform Domain Name Dispute Resolution Policy (UDRP), this problem persists within the DNS.

Cybersquatting also facilitates the problem of *impersonation* – that is, a registrant that intentionally uses a confusingly similar domain name or web presence to impersonate the identity, products or services of another. Internet users believe they are visiting legtimate websites but instead are exposed to counterfeit goods (including harmful counterfeit pharmaceuticals), bogus information, unwanted content, or other problematic outcomes.

6. Are there any other examples of unfair use of domain names that should be included in the 'prescribed practices'? If so, please describe them and provide reasons as to why you think they should be included.

Please see our reply to Question 3 above.

7. What would you consider to be too burdensome in the context of resolving disputes under our prescribed dispute resolution procedure?

The principles outlined in Section 4 of the consultation document appear to be well balanced. We defer further comment until a specific proposed procedure is defined.

8. What does 'expeditiously' mean to you in the context of resolving disputes under our prescribed dispute resolution procedure?

Time is a critical element – if not *the* critical element – during perpetration of online crimes. Attacks on DNS infrastructure, use of names to defraud or confuse, IP infringement, distribution of CSAM and other types of harms all can often be muted if acted upon expeditiously. In most scenarios, however, damages are rapidly incurred while dispute resolution procedures consume valuable time.

The BC counsels that in instances of quickly evolving threats, "expeditiously" should be interpreted to mean "immediate." In no case of harm, however, should a *constructive* response be delayed more than 48 hours. To argue for lengthier response times, frankly, is to enable expansion of cybercrime.

9. What do you consider to be 'low cost' in the context of resolving disputes under our prescribed dispute resolution procedure?

The BC reserves more specific comment on costs until the particulars of the proposed dispute resolution procedure are made available for review. However, we advocate for a procedure that is as cost-effective as possible for all parties involved.

Corollary to this, the BC notes that the prevalence of DNS misuse is so imposing that dispute resolution procedures that cost a complainant significant filing and attorney's fees are not an effective mitigation tactic. We encourage attention to this fact in consideration of potential dispute resolution mechanisms.

In addition, as a cost and time mitigation strategy, we encourage consideration of "trusted notifier" programs. These types of agreements between registries, registrars and expert parties can be highly effective in dealing with cases of DNS abuse or misuse. A trusted notifier is defined by the EU DNS Abuse Study as such:

> *A trusted notifier-system refers according to the European Commission to a mechanism, where a privileged notification channel is provided by an intermediary to specialised entities with specific expertise in identifying illegal content, and dedicated structures for detecting and identifying such content online.*

10. What would you consider a 'fair' and 'equitable' dispute resolution procedure design to be?

The BC believes that a registry or registrar that is highly confident that a crime is under way should take action upon such evidence instead of demanding procedural hurdles.

An effective, cost-conscious and balanced mechanism for dispute resolution should include the following:

- Independence – any dispute procedure should be conducted by an independent, disinterested third party with expertise in domain name- and IP-related issues.
- Accessibility for a complainant –the procedure should be well-outlined and -defined so as to be easily understood and used by those seeking to enlist help to resolve domain name misuse.
- Defined standards – a dispute resolution provider must be as clear as possible with regard to standards that must be met in order to proceed with dispute resolution, so as to avoid unnecessary congestion of any procedure, and to ensure that complaints and replies are correctly focused.
- Due process – any envisioned procedure should safeguard fairness to both sides of a complaint by ensuring due process is followed.
- Appeal mechanism – a sound procedure will include a path to appeal a decision that the complainant or respondent considers to be in error.
- Consolidation of disputes – as a means for managing costs and ensuring efficiency, the dispute resolution procedure should allow for disputes involving multiple domain names registered to the same party to be consolidated into one action.

11. Do you have any further comments on best practice or about the overall design of our dispute resolution procedure?

Yes. With regard to cybersquatting, administrative proceedings such as dispute resolution mechanisms do not serve effectively as a deterrent to infringing behavior, as the only availably remedy to the (financially) damaged party is transfer of or suspension of the domain name(s). We encourage consideration of a design for the award of damages – one similar to the Anti-Cybersquatting Consumer Protection Act in the United States, which allows statutory damages that are a deterrent to misuse.

In the area of best practices, more can be done. Country code top-level domains (ccTLDs) in Europe (including those administered by Nominet) employ useful best practices; results of those practices are reflected in relatively lower abuse and misuse statistics. The BC endorses examination and consideration of best practice recommendations as put forward by research and industry authorities.

In the above-referenced DNS Abuse Study by the European Commission, author Korczynski made best practice recommendations that could readily be adopted by UK registries and registrars. Specifically, these include:

- Verification[7] of the accuracy of domain registration (WHOIS) data, among others through harmonised Know Your Business Customer (KYBC) procedures and eID authentication;
- Encouragement to develop and offer similarity search tools or surveillance services to enable third parties to identify domain names that potentially infringe their rights;
- Services allowing intellectual property rights (IPR) holders to preventively block infringing domain name registrations;
- Encouraging the use of predictive algorithms or other methods to prevent abusive registrations;
- Monitoring of abuse rates on an ongoing basis by independent researchers in cooperation with institutions and regulatory bodies;

[7] See report from ENISA, the European Union's agency for cybersecurity, regarding the positive impact on abuse and misuse incidences resulting from registrant verification procedures: https://www.enisa.europa.eu/publications/dns-identity

- Revocation of a registry's or registrar's accreditation if abuse rates still exceed predetermined thresholds within a given time period; and
- Financial rewards for lower abuse rates through a reduction in domain registration fees.

As noted above in our comment regarding the need to act against abuse and misuse at scale, we reiterate that it is critical to enable the capability to mitigate harms against known bad actors more efficiently, use available technology and tools to prevent abuse from occurring in the first place, and to significantly reduce existing timelines for *constructive* responses from registries and registrars to pleas for assistance in abuse scenarios.

12. To what extent do you agree or disagree with our assessment under the 'Summary of Business Impact' section? Please provide details for your answer.

The estimated cost appears to be bearable. The BC reserves final input until additional details are known.

13. Are there potential positive impacts (including costs or financial implications) that the proposals outlined in this consultation may have on businesses, consumers or the public sector? Please provide any evidence or comments on what you think these positive impacts would be.

Cost-effective and efficient means for combating DNS harms and for resolving disputes, the BC is confident, will have a positive impact on UK businesses and consumers. The reduction of confusion, removal of active harms, safeguarding the public's interest in a well-functioning DNS, and other benefits will accrue to the benefit of all parties experiencing the difficulties of domain name misuse.

It is imperative that these proposals serve the public safety objective of reducing harm to UK consumers – thoughtful and assertive measures will result in less economic damage, fewer threats to public health, and more stability and security for the DNS.

14. Are there potential negative impacts (including costs or financial implications) that the proposals outlined in this consultation may have on businesses, consumers or the public sector? Please provide any evidence or comments on what you think these negative impacts would be.

Based on its experience in DNS governance, the BC would anticipate few, if any, negative outcomes to proceeding with these proposals. Our input is that it is important to include UK-based registrars (as well as registries) in the combating of DNS-related harms.

There however may be *de minimis* impacts on the consumer experience. For example, registrars and registries in theory could raise consumer domain name costs to compensate for the resources necessary to increase attention on DNS-related harms. However, given the relatively low cost of domain names in general, this would not be anticipated to be a significant burden to internet users. In addition, it would further benefit the trustworthiness of .UK and other UK-based top-level domains.

15. Please provide any other comments or evidence that relates to or is about the analysis under the 'Summary of Business Impact' section.

N/A

16. Do you have any comments about the potential positive and/or negative impacts that the options on the broad purposes of the commencement of the DEA 2010 powers outlined in this consultation may have on individuals with a protected characteristic under the Equality Act 2010? If so, please explain what you think these impacts (both positive and/or negative) would be.

No.

17. If you believe there may be negative impacts, what do you think could be done to mitigate them?

N/A

On behalf of the businesses we represent, we welcome this consultation and encourage your office to continue this important discussion.

Thank you for the opportunity to submit comment on the draft proposal.

Sincerely,

Steve DelBianco
Vice Chair for Policy Coordination
ICANN Business Constituency
1-703-615-6206