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

Comments of the Messaging Malware Mobile Anti-Abuse Working Group (M^{3}AAWG) on Powers in Relation to UK-Related Domain Name Registries

Introduction and Context

The Messaging Malware Mobile Anti-Abuse Working Group (M^{3}AAWG) appreciates the opportunity to submit comments in response to the above-referenced consultation. M^{3}AAWG is a technology-neutral global industry association. As a working body, we focus on operational issues of internet abuse including technology, industry collaboration, and public policy. With more than 200 institutional members worldwide, we bring together stakeholders in the online community in a confidential yet open forum, developing best practices and cooperative approaches for fighting online abuse.

Executive Summary

We applaud the UK government's interest in tackling online abuse and cybercrime.

We recognize that the scope of the powers described in the proposals is limited to situations where there has been a serious relevant failure in relation to an internet domain registry or any of its registrars in scope country code top-level domains (*.uk*) and generic top level domains (gTLDs) (*.scot* / *.wales* / *.cymru* / *.london*) that are targeting the UK. We generally support the powers in order to protect the public from harm in these limited circumstances.

As DNS abuse directly correlates with cybercrime, DNS abuse definitions should be consistent with the internationally recognized Convention on Cybercrime, which enumerates explicit definitions and categories of cybercrime. Moreover, the UK signed the Convention on Cybercrime's "Second Additional Protocol"[1] facilitating cooperation for domain name registrations.

Indeed, M[3]AAWG recommends that the UK consider preparing a model policy for the *.uk* and related registries that could also be voluntarily adopted by other registries, be they based in the Crown Dependencies or beyond.

Our comments below seek to enhance the effectiveness of the proposals to tackle the growing problem and scale of online abuse and cybersquatting. In summary, our comments address several topics:

DNS abuse is a significant and growing problem that calls for effective solutions.
Ample research exists demonstrating that phishing, malware, and other forms of abuse continue to show a disturbing upward trend. A study conducted by Interisle Consulting group found that "The use of domain names in malware URLs grew sharply. Interisle found a 121% increase in the use of domain names in 4Q 2022."[2] The Cybercrime Information Center also published a recent report detailing that the monthly number of phishing attacks reported has more than doubled since 1 May 2020.[3]

Interisle's Phishing Landscape 2023 Report[4] states that the number of phishing attacks has tripled since May 2020, and has increased 65% over the previous yearly study period. It also found that the number of unique domain names reported for phishing continues to increase. Interisle also noted that malicious domain names are the most common way that phishers carry out their attacks. Preventing the registration of these domains and taking them down quickly should be a priority for the domain name industry.[5]

The 2022 EU DNS Abuse Study commissioned by the European Commission similarly found that "malicious activities on the DNS have been a frequent and serious issue for years, affecting online

[1] https://www.coe.int/en/web/cybercrime/second-additional-protocol
[2] https://interisle.net/MalwareLandscape2023.pdf
[3] https://www.cybercrimeinfocenter.org/phishing-landscape-2022
[4] https://interisle.net/PhishingLandscape2023.html
[5] https://interisle.net/PhishingLandscape2023.html

security, causing harm to users and third parties, and thus undermining their trust in the Internet."[6] The study concluded:

> To date, the response to DNS abuse in terms of preventive and reactive measures includes a broad set of voluntary and prescriptive instruments ranging from technical measures and contractual clauses, to cooperation between DNS operators and competent authorities, and to regulatory actions. However, past initiatives are fragmented and, as data shows, have not yet resulted in a significant reduction of DNS abuse.

The definitions of DNS abuse should be expanded.
We support a broader definition of DNS abuse, especially in light of the changing nature of cybercrime and the speed by which criminals change tactics. Discussions and disagreements about definitions have hampered and delayed various attempts to tackle DNS abuse. As a result, we encourage the adoption of a flexible definition that focuses on risk, threats, and harms rather than just set categories, in order to protect the UK public from the growing emergence of new threats. Indeed, the UK should look to the scope of the Budapest Convention[7] to ensure that the types of cybercrimes it enumerates are included in the definition of DNS abuse.

The UK should address the lack of availability of WHOIS data by tracking NIS2 requirements.
M[3]AAWG members have identified the lack of WHOIS data as an impediment to the investigation, mitigation, and prevention of cybercrime, as is reflected in the findings of the M[3]AAWG study "ICANN, GDPR, and the WHOIS: A Users Survey – Three Years Later."[8] While steps have been taken in Europe to rectify this problem through the adoption and transposition of the revised EU Directive on Security of Network and Information Systems (referred to as NIS2),[9] this development may not fully address the topic of WHOIS access and availability outside of the EU. As a result, a UK-specific solution is called for.

DNS misuse mitigation requirements should be included in contracts.
At a minimum, the UK should adopt best practices with regard to DNS abuse (as described in greater detail below) to be included in the contracts with registrars and registries to ensure swift mitigation of DNS abuse.

Transparency increases confidence in DNS abuse mitigation measures.
As DNS abuse mitigations evolve, it will become increasingly important to consider transparency so that good actors can maintain confidence in the deployed DNS abuse mitigations. For example, open reporting of actions taken and details of mitigation techniques can avoid perceptions of bias on the part of law enforcement, regulators, registries, and registrars. We encourage the UK authorities to consider how best to ensure transparency for DNS abuse mitigation measures and to periodically re-evaluate this position as techniques and deployments evolve.

[6] https://op.europa.eu/en/publication-detail/-/publication/7d16c267-7f1f-11ec-8c40-01aa75ed71a1/language-en/
[7] https://rm.coe.int/1680081561
[8] https://www.m3aawg.org/sites/default/files/m3aawg_apwg_whois_user_survey_report_2021.pdf.
[9] https://eur-lex.europa.eu/eli/dir/2022/2555/oj

Responses to Specific Consultation Questions

For reference: text of proposal
Domain Name Misuse

Below are our initial proposals of the types of misuse of domains in scope for which the registries should have in place adequate policies and procedures to mitigate against.

1. Registries should have in place adequate policies and procedures to mitigate against domain names being registered, and deal with instances when they have been notified that domain names are being used, with the purpose of carrying out the below misuses. We deem misuses to include these five broad categories of harmful activity as identified by ICANN.3

- ***Malware****: installing malicious software 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.*

- ***Botnets****: collections of Internet-connected computers that have been infected with malware and commanded to perform activities under the control of a remote administrator.*

- ***Pharming****: redirection of unknowing users to fraudulent sites or services, typically through the Domain Name System (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.*

- ***Phishing****: 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. Phishing differs from pharming in that the latter involves modifying DNS entries, while the former tricks users into entering personal information.*

- ***Spam emails****: when used as a vehicle for at least one of the preceding 'misuses'.*

2. Registries should also have in place adequate policies and procedures to combat the use of domain names administered by those registries which are registered to promote or display ***Child Sexual Abuse Material****. This refers to any representation by whatever means of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child primarily for sexual purposes, as outlined in the Optional Protocol to the Convention on the Rights of the Child on the sale of Children, Child Prostitution and Child Pornography.*

Questions on the list of misuse of domain names:

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?

All types of misuses identified in the consultation should be included. M[3]AAWG notes that the definition should look to the Budapest Cybercrime Convention to be consistent with mitigation strategies in multiple jurisdictions and to expand the list of items covered by the definition. This would include 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."[10]

We note that ICANN's categorization is insufficient and must be expanded to an actual definition focused on risks, threats, and harms. For example, spam *per se* should be an abuse category of its own, rather than viewed solely as a tool used for malware, botnets, pharming, and phishing.

We recognize that no list of abuse types will ever be considered comprehensive. The UK should expect to adjust the definition to new and evolving types of threats and to include language that speaks to the nature of misuse and harm rather than providing simple categories of illicit behavior.

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.

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. We encourage the UK to examine the findings of the EU's DNS Abuse Study, which contains a series of recommendations for best practices, and types of abuse to be addressed.[11]

Compromised Domain Names
From the EU DNS Abuse Study: "domain names registered by bona fide third-party for legitimate purpose, compromised by malicious actors in order to carry out harmful and illegal activity." Here, we note that legitimate registrants should be supported in recovering access to their legitimately held names if possible. We caution, however, that the UK proposal should be carefully drafted to avoid collateral damage such as affecting domain names with legitimate uses and purposes.

Maliciously registered domain names
From the EU DNS Abuse Study: "domain names registered with the malicious intent to carry out harmful or illegal activity."

Malicious domain generation algorithms (DGAs)
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 could potentially be thousands of domains that malware can check for instructions. Where DGAs are used to carry

[10] https://rm.coe.int/1680081561
[11] https://op.europa.eu/en/publication-detail/-/publication/7d16c267-7f1f-11ec-8c40-01aa75ed71a1/language-en/

out harmful or illegal activity, registries and registrars should follow best practices to mitigate these domain names registered in bulk.

DNS as a potential DDoS attack weapon
DNS is increasingly weaponized for distributed denial of service attacks. This is a major emerging theme for the cyber underground. Cloudflare notes in their *DDoS Threat Report for 2023 Q2*,[12] "Over the past quarter, the most common attack vector was DNS-based DDoS attacks — 32% of all DDoS attacks were over the DNS protocol."

Sale of Illicit/Counterfeit Drugs
This activity often is conducted through domain names used to facilitate the online sale of drugs illegally, which can raise serious public health concerns.

> **For reference: text of proposal**
> *Domain Name Unfair Use*
>
> *Below are our initial proposals of types of unfair uses of domains in scope for which the registries should have in place an adequate dispute resolution procedure to deal with. This dispute resolution procedure should follow the principles outlined in the 'prescribed requirements' (see Section Four) in order to address these types of domain name abuse when they occur.*
>
> *Registries should have in place an adequate dispute resolution procedure to deal with instances when they have been notified that domain names have been registered with the purpose of carrying out unfair practices which constitute 'cybersquatting'.*
>
> *Cybersquatting refers to the pre-emptive, bad faith registration of trade marks as domain names by third parties who do not possess rights in such names. This includes 'typosquatting', when an end user takes advantage of common misspellings made by Internet users who are looking for a particular site or a particular provider of goods or services, in order to obtain some benefit.*

Questions on the list of unfair uses of domain names:

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.

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.

Cybersquatting enables the impersonation of governments and businesses through the registration of domain names that contain the actual spellings or misspellings of trademarks that trick consumers into believing that they are interacting with a legitimate site. Often, registries and registrars do not

[12] https://blog.cloudflare.com/ddos-threat-report-2023-q2/

take down domain names that cybersquat even when it is clear that the domain name will in all likelihood be used for fraud. For example, domain names that include in the domain string a famous name plus a word that is highly suggestive of fraud (such as "login," "password," "security center," "verification," or "help") should be taken down at the request of the brand holder, if not suspended by the registrar pending investigation. Resolution through a domain resolution procedure that is costly and takes months to conclude should be the last resort. During that time, millions of UK citizens, as well as non-citizens worldwide, are at risk of falling prey to scams. However, the rule should be narrowly construed to address cybersquatting involving DNS abuse in order to avoid takedowns of domain names that may have fair-use or free speech implications (such as a domain string with brand + sucks).

WIPO has reported rising numbers of Uniform Domain-Name Dispute Resolution Policy proceedings (UDRPs) since 2018, when registrant WHOIS data became largely unavailable.[13] While the UDRP and Nominet procedures are generally available to address cybersquatting, it is clear that criminal actors are not deterred by losing these proceedings (such as the UDRP), since the only penalty is to transfer the domain name. Yet brand holders are compelled to spend thousands of dollars to hire an attorney to draft the transfer and to cover the filing fees.

While the UK's trademark law has been applied to infringing domain names,[14] M^{3}AAWG observes that the UK has not adopted a cybersquatting statute similar to the Anti-Cybersquatting Consumer Protection Act in the US, where statutory damages are available ranging from US$1,000 – $100,000 per infringing domain name. The UK should consider similar remedies for cybersquatting to deter bad actors from engaging in this activity.

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.

> **For reference: text of proposal**
> *4. Design of the Dispute Resolution Procedure*
>
> *This part of the Regulations is in relation to the arrangements made by the registry for dealing with complaints in connection to internet domain names. Unlike the lists of misuses and unfair uses, this part of the Regulations is still at early stages of development and we are seeking your views on the overall principles which we want our dispute resolution procedure to follow.*
> *We propose that the below principles, which draw upon text from binding domain name dispute provisions found in multilateral free trade agreements, underpin our prescribed dispute resolution procedure:*
>
> - *Ensuring flexibility so that the rules established in existing relevant registries' dispute resolution procedures can be met.*
> - *Ensuring that it is not overly burdensome for the domains in scope of the powers to meet.*
> - *Ensuring it is fair and equitable in its design.*
> - *Ensuring that it does not preclude resort to judicial proceedings.*

[13] See https://atlasvpn.com/blog/cybersquatting-cases-reach-record-highs-in-2022
[14] See, for example, 1998 judgment in British Telecommunications Plc v One in A Million Ltd.

- *Ensuring that disputes are resolved expeditiously and at low cost.*
- *Ensuring that the procedure is clearly set out in an open and transparent way.*

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 fair and balanced.

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

For a procedure to be effective, it must allow for the immediate suspension of content that is harming the public, even if the procedure is still underway. This means that it should build in a temporary takedown or suspension mechanism depending on the type of harm to the public.

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

M[3]AAWG favors procedures that are as cost effective as possible for all parties involved, recognizing that since the volume of abuse is so high, the resolution procedures under consideration may not actually be used to address expeditiously the types of abuse that the UK seeks to eliminate.

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

Dispute resolution is important, as false positives are always possible. As in any such case, all relevant parties should be able to present evidence and have their arguments heard. The procedure should be managed independently by actors without financial or other interests. Both parties should be able to request that managers should be replaced if there is a conflict of interest.

However, we also note that in true "false positive" cases, an expedited, simple process should be achievable and appropriately supported.

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

We have four further comments.

1. The UK should consider adopting the best practices as identified in the EU DNS Abuse Study. Specifically, this study recommends:

   "TLD registries, registrars, or resellers, depending on their role, should:
   - verify the accuracy of the domain registration (WHOIS) data, among others through harmonized Know Your Business Customer (KYBC) procedures and eID authentication;
   - be encouraged to develop and offer similarity search tools or surveillance services to enable third-parties to identify domain names that potentially infringe their rights;

- offer services allowing intellectual property rights (IPR) holders to preventively block infringing domain name registrations;
- be encouraged to use predictive algorithms or other methods to prevent abusive registrations;[15]
- be identified with respect to the concentration and rates of DNS abuse in their ecosystems;
- have abuse rates being monitored on an ongoing basis by independent researchers in cooperation with institutions and regulatory bodies;
- have their accreditation revoked if their abuse rates still exceed predetermined thresholds within a given time period;
- be financially rewarded for lower abuse rates through a reduction in domain registration fees."

2. The UK should recognize the importance of access to WHOIS to address DNS abuse. Since WHOIS access is so integral to the ability to detect, investigate, and proactively mitigate domain name abuse at scale, the UK should consider adopting similar WHOIS requirements for registries and registrars to collect, maintain, and ensure the accuracy of WHOIS data as specified in Article 28 and its corresponding recitals in the recently adopted EU Directive on Security of Network and Information Systems (NIS2).

Cybercriminals rely on domains to launch coordinated and automated attacks on a global scale and to perpetrate a plethora of consumer fraud and scams. Accessing WHOIS data – the authoritative record of domain ownership – is the only viable means to obtain the information necessary to identify criminal actors, prevent harms, and protect the public from online harms.

For more information on the effect of WHOIS on anti-abuse mitigation efforts, please refer to the study completed by the Messaging Malware Mobile Anti-Abuse Working Group: "ICANN, GDPR, and the WHOIS: A Users Survey – Three Years Later."[16]

Key findings include the following:

- Since 2018, cyber-investigators have been significantly impaired in their ability to investigate relationships between malicious domains and actors.
- Response times are significantly longer, causing harm.
- Requests to access non-public WHOIS by legitimate investigators for legitimate purposes remain ineffective.
- WHOIS has become an unreliable and less meaningful source of threat intelligence.

Thus, dealing with malicious domains – and in consequence, addressing crime and abuse – has become considerably harder and more time intensive. The lack of access to accurate WHOIS records inhibits the work undertaken by law enforcement, cybersecurity professionals, and others. This has an effect on security on the internet as a whole.

[15] If adopted, predictive algorithms used for DNS abuse mitigation should be coupled with complete transparency of their use.

[16] https://www.m3aawg.org/sites/default/files/m3aawg_apwg_whois_user_survey_report_2021.pdf

3. The proposal does not address systemic abuse, such as when thousands of similar domain names are registered by the same party for use in a malware attack. The proposal appears to address abusive domains only on an individual basis. There is no obligation to take proactive steps that will prevent having multiple domain names linked to the same abusive party. M[3]AAWG recommends that the UK call for registries and registrars mitigate proactively when it is shown that the registrant has registered malicious domains in the past, and that the account has other domain names that follow the same abusive patterns and are thus likely to harm the public in the same ways.

4. M[3]AAWG acknowledges that the UK is a signatory to the Second Additional Protocol to the Budapest Convention, which, in the context of WHOIS, will mean that, once the appropriate legislation is enacted, domain name registrars and registries should have the obligation of sharing non-public WHOIS data with law enforcement requestors from other signatory countries.

> **For reference: text of proposal**
> *Summary of Business Impact*
>
> *The cost of the proposed approach to commencing the DEA 2010's provisions relating to internet registries and domain names is expected to be minimal. The introduction of these powers is to ensure that the UK continues to meet international best practice on the governance of country top-level domains (ccTLDs).*
>
> *Therefore, the approach focuses on continuing existing practices and is unlikely to result in material changes to the actions/steps businesses currently take.*
>
> *Based on a proportionate assessment of the proposals at the consultation stage, impacts are expected to fall well below the de minimis threshold of +- £5 million per year and therefore, a full impact assessment has not been prepared to support the consultation. The department will keep this under review as the policy develops or if further evidence becomes available in preparation for the final stage.*

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.

Agree.

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, we are 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.

We anticipate few, if any, negative outcomes to proceeding with these proposals. Our only input in this regard is that it is important to consider inclusion of 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. This, however, would have the added benefit of further safety in the DNS itself.

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

We appreciate the opportunity to submit these comments, and we welcome the opportunity to engage as needed to answer any questions during this process. Please address any inquiries to M^{3}AAWG Executive Director Amy Cadagin at comments@m3aawg.org.

Sincerely,
Amy Cadagin, Executive Director
Messaging Malware Mobile Anti-Abuse Working Group
comments@m3aawg.org
P.O. Box 9125
Brea, CA 92822