Response of Interisle Consulting Group
to the
UK Department for Science, Innovation and Technology (DSIT)
consultation on
Powers in Relation to UK-Related Domain Name Registries

29 August 2023

Attn: DSIT International Regulation and Trade Team
ukdomainnames.consultation@dcms.gov.uk

Interisle Consulting Group (Interisle) is pleased to submit its input to DSTI on the important matter of Internet domain name abuse and misuse.

Interisle is a leading independent consultancy specializing in Internet and telecommunications networks and their design, use, governance, and growth. We work across government, industry, and the non-profit sector to help address challenges ranging from network and systems architecture to policy and regulatory matters.

Interisle is a major contributor to the Cybercrime Information Center, which works to identify, measure, and expose domain name system (DNS) and Internet addressing systems abuse and the contexts in which it occurs—particularly those in which criminal abuse is highly concentrated. We make our research findings and methodology publicly available and leverage our analysis to assist policymakers, researchers, and industry in evaluating policies and practices that may mitigate (or unintentionally facilitate) cybercrime.

Our global team of partners and associates have decades of experience in Internet technical and policy matters. Among other issues, we have provided subject matter expertise in forums relevant to Internet resources, governance, and cybercrime, including the Internet Engineering Task Force (IETF), Internet Corporation for Assigned Names and Numbers (ICANN), the Commonwealth Cybercrime Committee, and the Council of Europe, among many others.

The Persistent and Prevalent Problem of DNS Abuse

Using data collected at the Cybercrime Information Center, Interisle has been measuring and studying the incidence of cybercrime on the Internet since 2019. Our analyses show that the misuse of DNS resources for criminal acts is persistent and present in nearly all countries. In our August 2023 study, *Phishing Landscape 2023: A Study of the Scope and Distribution of Phishing,* we reported that:

- The number of phishing attacks worldwide *tripled* since May 2020 and continues to trend upward.[1]

- *More than one million unique domain names* were reported for phishing between May 2022 and April 2023 alone, the most we have seen in any period since May 2020.[2]

- *Two-thirds* of domain names reported for phishing were *maliciously registered*, meaning they were *purposely registered* by a criminal with the intent of perpetrating a phishing attack.[3]

[1] *See* *Phishing Landscape 2023: The Study of the Scope and Distribution of Phishing,* p. 5
[2] Ibid. p. 7
[3] Ibid. p. 8

Far from being a hidden problem, stakeholders have known about the scope and scale of domain name misuse for a long time. Yet *cybercriminals can still trivially acquire the Internet and DNS resources they need to conduct their attacks,* which ensnare victims ranging from large corporations and government institutions to small businesses and unwitting pensioners. Interisle believes we must adopt effective mitigation measures to starve cybercriminals of these resources and curb the attacks that harm both national economies[4] and average citizens.

We thank the Department for Science, Innovation & Technology (DSTI) for taking this important matter seriously and undertaking this consultation. We believe governments have an important role to play in combatting DNS misuse, including in the country code top-level domains (ccTLDs) and geographic generic top-level domains (gTLDs) corresponding to their territory or parts thereof.

We further appreciate the active participation of the UK government in private sector and intergovernmental forums discussing Internet resource, governance, and cybercrime issues. The UK has shown itself to be a thoughtful contributor, collaborator, and frequent leader in advancing effective solutions to challenging issues. We believe that the UK has an opportunity to promote strong anti-abuse measures across all UK-related TLDs, reduce victimization of its citizens, institutions, and companies, and demonstrate global leadership in the prevention of cybercrime.

Proactively Combatting Domain Name Misuse and Unfair Use

We note that the current consultation seeks to define categories of domain name "misuse" and "unfair use" and high-level principles for dispute resolution. We provide specific responses below to the consultation's numbered questions. First, we offer here a broader discussion on the *prevention* of DNS misuse for DSTI's consideration as it continues its work in this area.

The most common mitigation frameworks in operation today are reactive: mitigation begins after attacks have already been launched and victims have fallen prey. Historically, private sector actors have been the first responders to cyberattacks. The unabated growth in online crimes involving domain names amply demonstrates that relying primarily on post-hoc remediation fails to reduce victimization. Despite ample evidence that post-hoc remediation is failing, we note that the proposed anti-abuse contract provisions under discussion at ICANN focus on mitigating abuse *after it has already taken place* and formalize practices that many ICANN contracted parties already employ. We are therefore concerned it will have limited meaningful effect.[5] Early detection and pre-emptive actions are urgently needed to complement post-hoc remediation approaches.

Industry research, including our own, shows that cybercriminals often engage in highly identifiable patterns of malicious domain name registration behavior. For example, criminals routinely register names rapidly and in large volumes from a single account (often referred to as "bulk registration"). These names are often suspiciously long, include an excessive number of non-alphabetic characters, include brand names, or have other observably suspicious patterns (*e.g.,* bandao###.com, bd####.com, bdty###.com, ###bdty.com, bdvip###.com.)[6] Domain name registrars and registries are in prime positions to preemptively hold and review such suspiciously composed domain name requests before they are delegated and weaponized for attacks.

[4] World Economic Forum. "Digital trust: How to unleash the trillion-dollar opportunity for our global economy." August 17,2020. https://www.weforum.org/agenda/2022/08/digital-trust-how-to-unleash-the-trillion-dollar-opportunity-for-our-global-economy/

[5] Interisle believes that the proposed registry and registrar contract modifications being considered at ICANN fall short of an effective DNS abuse mitigation approach. While these issues are outside the scope of DSTI's current consultation, we invite you to read our analysis of the proposed provisions in our *Phishing Landscape 2023* report, starting on p. 40

[6] See *Phishing Landscape 2023: The Study of the Scope and Distribution of Phishing,* p. 11

Criminals often deploy their attacks very quickly after acquiring these domain names, making the implementation of preventative measures particularly important.[7] In our recent phishing study, we reported that 34% of gTLDs domains reported for phishing were used within 48 hours of appearing in the DNS and 46% were used within 14 days. In ccTLDs, 13% of reported phishing domains were used within 48 hours and 20% in 14 days.[8] We argue that adopting measures that deny criminals access to resources used in cybercrimes should be a matter of urgent attention.

Methods and tools for early detection of abusive registrations exist and have already been implemented by some industry players. For example, the .EU registry currently screens registered domains based on lexical features and similarity to known brands.[9] If the string is suspiciously composed, the requested domain name is delayed from delegation by the registry until it can be further investigated. A large registrar, NameCheap, is now limiting the registration of domain names with notable brand names and phrases in them as a way of preventing misuse.[10]

We urge DSTI to include as "adequate mitigation policies and procedures" the adoption of reasonable measures that identify suspicious domain name registration requests and prevent criminals from registering them in the first place. We recommend that mitigation policies and procedures be included in relevant contracts governing registry and registrar operations, obligations, and relationships in a manner that ensures compliance and enforceability.

We also recommend the implementation of "thick" WHOIS records and an obligation to collect complete and accurate domain name registrant data. The EU's Directive on the Security of Network Information Systems (NIS2)[11] includes new requirements for collection and maintenance of accurate and verified registration data by registries and registrars. We urge DSTI to include WHOIS obligations similar to those set forth in NIS2 Article 28 and related recitals. These measures make resource acquisition more complicated for criminals and can expedite misuse and unfair use investigations.

Coordination, cooperation, and consistent action across a range of players will be necessary to create effective change, as cybercriminals also exploit Internet resources beyond second-level domain names to conduct their attacks. We invite DSTI to review the section *Building a Better Future: Policies, Practices, and Legislation* of our recent report[12] for a more in-depth discussion on actions we believe are needed to stem the tide of DNS misuse, as well as the broader abuse of Internet resources used in phishing and other cybercrimes.

<u>Responses to Numbered Consolation Questions:</u>

Interisle is pleased to provide responses to questions 1 to 3 of the consultation, which correspond most closely to our expertise.

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 five types of harmful activities identified under 'Domain Name Misuse' (Malware, Botnets, Pharming, Phishing, and Spam Emails) and the use of domain names registered to promote or display child sexual abuse material should be considered 'prescribed practices.' We do not believe, however, that the current ICANN-defined list and

[7] Ibid. pp. 11 – 12

[8] Ibid. p. 12

[9] L. Desmet, J. Spooren, T. Vissers, P. Janssen and W. Joosen, "Premadoma: An operational solution to prevent malicious domain name registrations in the .eu tld", *Digital Threats: Research and Practice*, vol. 2, no. 1, pp. 1-24, 2021 https://dl.acm.org/doi/10.1145/3419476

[10] See https://www.namecheap.com/legal/domains/registration-agreement/

[11] See https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333

[12] See *Phishing Landscape 2023: The Study of the Scope and Distribution of Phishing*, pp. 40 – 46

definitions are fully comprehensive or congruent with other internationally recognized definitions of some categories of misuse. [13]

The proposed list excludes a variety of harmful and related activities, including a wide variety of scams (such as 419 and advance-fee fraud scams)[14] and ransomware that victimize UK citizens and critical services. Indeed, as ICANN's own Security and Stability Advisory Committee (SSAC) has stated:

> "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."[15]

We urge DSTI to ensure that its list of "prescribed practices" *includes language that is flexible enough to accommodate not-yet-seen types of scams, fraud, and other misuse not individually listed* but as may be identified from time to time.

Regarding the definition of "spam email" specifically, we note that the ICANN-based definition used in the proposal is a new, non-standard, narrow definition of spam not broadly recognized by industry experts. Expert industry advocates, including the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG) and Coalition Against Unsolicited Commercial Email (CAUCE), define spam as "bulk unsolicited email," which is generally illegal to send in most countries.

The ICANN-based formulation narrows the definition of spam to a subset of activities: only "when spam serves as a delivery mechanism for the other forms of DNS Abuse" — i.e., phishing, malware, etc.[16] The formulation is flawed because the domain names used to perpetrate harmful activity are *often not used to send the email*. Commonly, the domain name that is harmful is one that is advertised or contained in the body of the email as the location to which the victims are enticed to go. ICANN's formulation may excuse DNS registries and registrars from responding to most spam reports, which is especially problematic since many spam messages advertise products and scams of other types.

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.

As noted in our response above, we do not believe that the current list of "prescribed practices" and definitions are fully comprehensive or congruent with other internationally recognized definitions of some categories of misuse.

[13] For descriptions that are more in line with conventional definitions, see the Security Skeptic article *Lending Clarity to Security Risk Definitions - for ICANN Community and Beyond* which can be found at https://www.securityskeptic.com/2016/02/lending-clarity-to-security-risk-definitions-for-icann-community-and-beyond.html

[14] For a definition of these scams see https://en.wikipedia.org/wiki/Advance-fee_scam

[15] See SAC115 *SSAC Report on an Interoperable Approach to Addressing Abuse Handling in the DNS* p.13 https://www.icann.org/en/system/files/files/sac-115-en.pdf

[16] We recommend that DSTI consider Council of Europe's Convention on Cybercrime, Guidance Note #8 for its definition of spam, which we believe to be a more accurate and comprehensive definition, as we further discuss in our response to consultation question 2

We encourage DSTI to base the list and definitions of "prescribed practices" on threats and harmful activities that are considered cybercrimes in the Council of Europe's Convention on Cybercrime (the Convention).[17] The Convention is an international treaty for crimes that are committed via the Internet and other computer or device networks.[18] Its Articles and Guidelines include definitions of fraud, network security, and copyright infringement address phishing, malware, botnets, and spam, as well child sexual abuse material (CSAM) and infringements on copyright and related rights. It also includes a broad description of abuse defined as "fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person," that could provide flexibility to include other misuses that may emerge but are not specifically listed. The Convention enjoys broad global adoption through ratifications and accessions.[19] As the UK is already a party to the Convention, incorporating its descriptions as a baseline could help facilitate multi-jurisdictional mitigation and enforcement efforts.

For reference, we provide below a mapping of common domain name misuses to the relevant sections of the Convention. Again, we further recommend that any list of "prescribed practices" outlined by DSTI includes additional language that is flexible enough to *accommodate not-yet-seen* types of scams, fraud, and other misuse not individually called out.

Domain Name Misuse	**Relevant Article (Guideline) from the Council of Europe's Convention on Cybercrime**
Malware	Malware falls within Articles 2 and 6 - Illegal Access and misuse of device/software
Phishing (e.g., business email compromise)	This form of phishing falls within Articles 3 and 21 address - Illegal interception, interception of content data
Ransomware (an extortive form of malware)	Ransomware falls within Articles 4 and 5 - Data interference, System interference
Phishing, Scam, Fake/Counterfeit Sites	These cybercrimes fall within Article 8 - Computer related fraud
Child pornography, Child Abuse	Article 9, CSAM
Cybersquatting, Typosquatting	Article 10, Copyrights infringement
Spam, Botnets	Guidance Note #8 describes the circumstances where spam content, the act of sending spam, and the mechanisms for delivering spam (delivery infrastructures such as botnets) should be treated as cybercrimes

[17] The Council of Europe's Convention on Cybercrime is also known as "the Budapest Convention"

[18] The Council of Europe's Convention on Cybercrime can be found at https://rm.coe.int/1680081561

[19] A list of signatories and ratifications can be found at https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185

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.

Broadly speaking, any type of fraud or crime that uses DNS resources in the perpetration of the harmful activity should be a candidate as a "prescribed practice" misuse. As indicated, no list will ever be comprehensive, given the evolving nature of threats.

As noted above, we believe DSTI should use the Council of Europe's Convention on Cybercrime descriptions and definitions as the basis for its list of "prescribed practices," as well as its broad description of abuse to cover similar types of scams, fraud, and other misuse not individually listed but as may be identified from time to time.

We believe the Convention's descriptions and definitions provide a more comprehensive foundation for creating such a list. Furthermore, we believe that the widespread and consistent adoption of the Convention and/or its principles will help facilitate multi-jurisdictional abuse mitigation and enforcement efforts. We believe doing so for the UK will not only more effectively reduce victimization of UK citizens, institutions, and companies but also demonstrate global leadership in the prevention of cybercrime.

We would be pleased to further share our experience and expertise and discuss our research and recommendations in greater depth at your request. We look forward to contributing to future consultations and the successful implementation of the related provisions of the Digital Economy Act 2010.

For further information contact:

Dave Piscitello
Partner, Interisle Consulting Group
dave@interisle.net
+1 843-295-9329