Nominet UK: response to CMA consultation: cmareview@homeoffice.gov.uk

Thank you for the opportunity to respond to the open consultation on the introduction of new powers to suspend and seize domain names and IP addresses via a review of the Computer Misuse Act 1990.

As the public benefit company running the .UK, .cymru and .wales Top Level Domains, it is within Nominet's remit to raise standards and work to ensure that UK citizens and businesses are protected from avoidable criminality on the internet. We therefore welcome the discussion of any proposals which promote this objective. We also believe that in addition to improvements in the legislative framework, better education and understanding for both internet users and law enforcement are important factors to take into consideration. This should also be a part of any overall strategy to reduce criminal behaviour on the internet.

Preliminary comment: intervention at the DNS/ domain name level may be appropriate in certain circumstances, but it is useful to remember that it is a blunt instrument which leads to the complete shut down of a domain and associated services (e.g. email). A registry does not control or host websites of its domain registrants, and so we are unable to modify any content, merely to disable the domain name entirely. This may be disproportionate in effect, for example where there are multiple users of a domain or platform. In any event, it should be noted that the illegal content may still be accessible even after registry action, and that for removal from the internet to be completely effective it is much better to do this at source by working with the hosting provider or domain registrant directly.

As a general principle we agree that UK law enforcement agencies should have access to a Court supervised suspension process, with a clear basis in law. As regards any voluntary arrangements currently undertaken by us, we note that these are expected to continue as the primary means of taking down domains, given that they provide a fast and effective response and are unchallenged in the vast majority of cases. Nominet has voluntarily supported UK law enforcement for many years now in disrupting criminality on the internet and publishes an annual transparency report.

Having considered the issues, we are happy to confirm that we would look to continue with our current voluntary arrangements, but that we would use the introduction of any statutory power as effectively an appeal mechanism where a domain registrant disagrees with the suspension of their domain.

However, on the question of blocking of domain names which are predicted will be used for criminal purposes we have considerable reservations. There are well-known problems with this idea which would be extremely difficult to legislate for. There are also the speech and human rights considerations, and strong legitimate use cases (for example security training companies frequently register what on the face of it could be malicious domains, but use them for the laudable objective of raising awareness of phishing and other fraudulent attacks).

We look forward to discussing both of these aspects further in due course.

Answers to the specific questions follow below.

Q1. What should be the threshold for the use of this power, what tests would an application have to meet and what safeguards should apply to it?

A1. This power should only apply where it is very clear that criminality has occurred via a domain name, and that suspension is the appropriate remedy because there are no freedom of expression considerations or collateral damage caused to other internet users due to the imprecise nature of intervention at the DNS level. Domain name suspension should therefore be considered as a remedy of last resort and unless there is an exceptional need for urgent action we would expect any authority to evidence that they have first approached the domain registrant or hosting provider, particularly where it may only be one small part of a website which falls over the line into criminality. In order that a domain registrant can make representations we consider that where possible both the registrant and their registrar should be given notice of the application and given a reasonable period of time in which to raise a defence/ objection. Any application should be well-evidenced in terms of screenshots and/or other evidence of the alleged offence, and details of the specific criminal law breached.

Q2. Which organisations should have access to the power?

A2. Nominet's Criminal Practices Policy sets out the UK LEAs who currently carry out domain suspensions on a voluntary basis and this would be a good place to start. https://nominet.uk/wp-content/uploads/2021/02/Criminal-Practices-Policy-26-11-2021.pdf

Q3. What will a statutory power enabling the seizure of domain name and IP addresses allow that voluntary arrangements do not currently allow?

A3. Probably nothing as far as Nominet is concerned although we are considering whether the court process proposed could be used effectively as an independent appeal route where a registrant objects to a voluntary suspension. We do however appreciate that in order for reciprocal cooperation to work in other jurisdictions via MLAT, a domestic legal basis is required to be in place.

Q4. What activity would we ask the recipients of an order to undertake that they do not undertake under voluntary arrangements?

A4. It is not clear whether the recipient of an order refers to the domain name registrant (who has registered and uses the domain), or the registry (which in the example of Nominet is the central organisation which administers the register of domain names and ensures their technical functionality), or the domain registrar (who is accredited by the registry and has technical access to the registry database to create and administer domain names on behalf of their customers). In any event, we would expect all relevant parties to be given notice of the application for an order, and a reasonable opportunity in which to make representations. Any order made should be clear and unambiguous as to the action required – whether to suspend a domain name, or to redirect it – and importantly the time frame that the suspension

or redirection should last for. An order should never effectively be for an indeterminate period of time or perpetual duration.

Q5. How can voluntary agreements, which are the preferred route for take downs, be protected?

A5. As the consultation document notes, the current voluntary arrangements provide a fast and effective remedy for criminal use of domains and remain the preferred route in terms of speed and cost, but also flexibility. Registries (such as Nominet) are generally private sector organisations, and part of the current difficulties with voluntary arrangements is that we are occasionally put in the position of having to decide on a technical and complex area of the criminal law (where for example there is a dispute between a law enforcement agency and a domain registrant). Ultimately having a clear process to bring a suspension order before the Court to decide whether suspension or seizure is lawful against clear criteria would be a positive move in our opinion, and could actually help to protect the current voluntary arrangements.

Q6. Should seizure mean the legal control and ownership (at least of the lease period) of domain names and IP addresses, or more temporary action such as sinkholing, pass to the law enforcement agency responsible for the order? Would law enforcement agencies pay for the lease?

A6. We would recommend leaving the registration in the name of the registrant during any period of suspension or seizure as this is administratively simplest both for registries and registrars. A change of registrant opens up questions as to who pays for (and benefits from) the registration, which has the potential to introduce unnecessary complexity. It is important that registrars are supported and encouraged to prevent/ report/ mitigate any criminality, and therefore not penalised with domain name registration and renewal charges. Where relatively modest numbers of domains need to be pre-emptively registered and sink holed (e.g. because they have been identified as potentially abusive as a future DGA) then we think it is reasonable for their registration to be provided as a blocking registration by the registry free of charge in the public interest.

Q7. If action is taken by law enforcement, should that be done for both the domain name and the IP address, and are there different recipients for orders for these?

A7. The domain registry only administers the domain name and so any order relating to an IP address would need to be referred either to the ISP / local internet registry or the relevant regional IP address registry (ie RIPE NCC for the EU region). We would urge caution when ‘seizing’ IP addresses however; as above for domain names this is a blunt instrument and can have a disproportionate impact, and this is especially the case for IP addresses where it is rare for a site to have its own IP address and the risk of unintended collateral damage could be significant.

Q8. Should multiple domains / IP addresses feature on one application or will separate applications be required?

A8. This will depend on the circumstances. Where there are multiple domains to be seized as part of DGA mitigation, it should be possible to make a single application for all the domains. Similarly where a single registrant has multiple domains, these should be covered in one application. However it becomes administratively and evidentially complex very quickly for multiple registrants accused of a range of different criminal behaviours to be included in the same application and it would probably be best for these to be separate applications.

Q9. Should there be scope for an emergency interim order to be made in advance of a hearing for a full order?

A9. Speed is certainly of the essence in some cases (e.g. advance fee ticket scams) and where it can be demonstrated that serious consumer harm is being caused there should be scope for an ex parte interim order to be made (in the same manner as an Anton Piller or Mareva injunction). However in any event the process should still allow for registrants to be able to challenge the suspension and have it quickly reversed (if applicable).

Q10. Should there be an opportunity for extensions to the order?

A10. In our experience, the utility of a domain for criminal purposes tails off relatively quickly, within a matter of weeks. Prudentially it could be the case that suspension for up to a year could be justifiable. For sinkholing DGA domains there could be a basis for longer periods of seizure. We think that all seizures should be time limited, with the domain/ IP address being seized being cancelled/ reallocated at the end of the order period. However there should be the option for an LEA to apply for an extension for a longer period of time where there is tangible evidence that this would more effectively mitigate the criminality.