30 MARCH 2022 • *Brussels, Belgium*

CENTR Comment on the DNS Abuse Study

Summary of CENTR key points

- CENTR members regard keeping abuse low on the internet as an important element to safeguard end-user trust and safety within their zones.
- CENTR members are pleased with the fact that the DNS Abuse Study recognises many good practices in place within European ccTLDs that contribute to low levels of abuse within their managed ccTLDs.
- The DNS abuse definition proposed by the DNS Abuse Study encompasses all common forms of cybercrime, and as a result should also include mitigation and prevention measures addressed at all actors involved in sustaining and using the DNS.
- The recommendations put forward in the DNS Abuse Study do not adequately take into consideration the essentiality of the internet infrastructure, such as the DNS, and the role and responsibilities of different operators active on the internet.
- The data sources used to assess the magnitude of DNS abuse in the DNS Abuse Study cannot be independently verified, and are not optimised for mitigation measures available for domain name registries and registrars.
- The DNS Abuse Study generally disregards the proportionate resolution path targeting the intermediary that is closest to the content, codified in EU legislation, without any clear and abuse-specific justification.
- The DNS Abuse Study disregards the fundamental difference between the governance of ccTLDs and gTLDs and demonstrates incoherent analysis by adopting a “one-size-fits-all” approach with measures targeted at both ccTLDs and gTLDs despite finding that ccTLDs are by far less abused. As a result, any measures targeted solely at ccTLDs will have a limited impact on effectively reducing abuse online.
- The recommendation to adopt harmonised Know-Your-Business-Customer practices across ccTLDs, despite the lack of proof of abuse, is unjustified and disregards the existing data accuracy practices already in place.
- The recommendation for a unified approach to accessing complete registration data across ccTLDs disregards the overarching EU data protection framework, as well as the recommendations put forward by data protection authorities within ICANN community discussions.
- The DNS Abuse Study recommends publishing DNS zone file data without assessing the potential negative consequences that such publication may entail for the security and stability of the DNS, including the confidentiality of customer data.

Introduction

CENTR is the association of European country code top-level domain registries (hereinafter ccTLDs). All EU Member State and EEA country ccTLDs (such as .de, .fr, and .no) are members of CENTR.

CENTR members are at the core of the public internet, safeguarding the stability and security of the internet. The majority of European ccTLDs are non-profit organisations or SMEs, providing an internet infrastructure service in the interest of and in close cooperation with their local internet communities (e.g. registrars, end-users, rightsholders, CSIRTs, law enforcement authorities).

ccTLDs are responsible for operating and maintaining the technical Domain Name System (DNS) infrastructure for their top-level domain. The DNS is a well-established network protocol at the heart of the internet infrastructure – commonly thought of as the "phone book of the internet". It provides a navigation function to map user-friendly domain names to numeric IP addresses, and is equally used by any service running on the internet, either visible to the end-users (e.g. website, email) or entirely behind the scenes (e.g. instant messaging, Voice over IP, and infrastructure management). ccTLDs only hold information enabling users to navigate the internet but do not store, transmit or enhance any third-party content online.[1]

ccTLDs are only one of several internet infrastructure actors that enable users to reach content or send emails. ccTLDs enable domain names to point to an IP address on which these services (e.g. a website or an email server) are hosted. Furthermore, ccTLDs maintain a registration database that contains the names and contact details of domain name holders. Elements of this registration database are publicly accessible via the so-called WHOIS. In addition, ccTLDs, as technical operators of the internet infrastructure, are considered to be 'operators of essential services' under Directive 2016/1148 (NIS Directive) and 'essential entities' under the upcoming revision of the NIS Directive (NIS 2 Directive).

CENTR welcomes the aim pursued by the European Commission to "analyse the scope, impact and magnitude of DNS abuse" with its recently published "Study on Domain Name System (DNS) abuse" (hereinafter the DNS Abuse Study or the Study).

CENTR members regard keeping abuse low on the internet as an important element in safeguarding end-user trust and safety within their zones. CENTR members are pleased with the fact that the Study recognises many good practices in place within European ccTLDs that contribute to low levels of abuse within their managed ccTLDs, in comparison to other actors within the TLD industry. CENTR recognises the challenge in clearly distinguishing DNS abuse from other forms of cybercrime, considering the essentiality of the DNS for the functioning of the internet, as well as the limitations in measuring the magnitude of abuse online.

Having taken part in the stakeholder interviews that served as the basis for the DNS Abuse Study, CENTR would like to also respond to several assumptions and inconsistencies present in the documents published as part of the DNS Abuse Study.

As the DNS Abuse Study provides several recommendations targeted at CENTR members, with the aim to guide possible future policy development in the field, CENTR would like to point out that the existing good practices

[1] For more information on the role of domain name registries, see CENTR, "Domain name registries and online content". Available here: https://centr.org/policy/policy-documents/download/10204/5751/41.html

that are continuously being improved and developed by European ccTLDs have contributed to the overall safety and security online, and continue to be considered as "best practices" within the global domain name industry.

In this regard, CENTR would like to submit the following comment as part of its response to the DNS Abuse Study that is considered to provide evidentiary basis for future policy discussions.

DNS abuse definition and magnitude

Inconsistency in definition and recommended mitigation measures

The DNS Abuse Study provides an extensive definition of DNS abuse, while acknowledging that "consensus on a global and comprehensive DNS abuse definition is still missing".[2] According to the definition adopted by the authors of the Study, DNS abuse "is any activity that makes use of domain names or the DNS protocol to carry out harmful or illegal activity".[3] The definition provided by the Study is therefore broad and seems to encompass all current forms of cybercrime.[4]

In addition to the suggested definition of the DNS abuse, the authors of the Study provide a slightly more nuanced definition in the explanatory statement following their aforementioned suggestion: "DNS abuse exploits the domain name registration process, the domain name resolution process, or other services associated with the domain name (e.g., shared web hosting service)"[5], taking a slightly narrower approach in defining the issue.

The explanation of the broad definition does not take into account the role of different DNS service providers, internet service providers, online platform operators and other categories of stakeholders that are part of the "complex ecosystem", apart from the service providers mostly involved in offering a domain name registration process. Furthermore, the different scenarios of mitigation measures available depending on the type of abuse that only concern the use of domain names or their registration process solely concern the following types of service providers: TLD registries, registrars/resellers, hosting service providers, as well as a largely generalised group of "DNS service providers" that may or may not include TLD registries and registrars in its scope. The Study seems to have interchangeably used DNS service providers, TLD registries and registrars when discussing abuse mitigating measures, without clearly referencing which actors are included under "DNS service providers", when not explicitly referencing TLD registries/registrars. The Study gives limited attention to actions addressing abuse at hosting level on the other hand, only doing so in relation to juxtaposing it with actions possible for "DNS service providers".

While the DNS abuse definition clearly encompasses all illegal activity that takes place online, irrespective of whether it includes content (e.g. hosting) or infrastructure (e.g. DNS) abuse, the authors of the Study have

[2] DNS Abuse Study, p. 50.

[3] DNS Abuse Study, p. 10.

[4] As acknowledged in the Study, at least on the ICANN community level there seems to be a broader consensus on the purely technical-related aspects, while the content-related ones are under continuous debate. Meanwhile, other fora like Internet & Jurisdiction and the DNS Abuse Framework have adopted DNS abuse definitions that distinguish between technical security threats and abuse related to illegal content.

[5] DNS Abuse Study, p. 10.

largely disregarded the differences in legal frameworks governing different operators. Most notably for the hosting level, the current EU legal framework is very different from the current legislation and soft law governing action at DNS level. As a result, the conclusions on the general practices of "DNS service providers" and hosting service providers when addressing abuse do not reflect the full picture, nor the full list of regulatory realities different operators are subject to.

For example, the Study largely disregards the current EU intermediary liability framework concerning the provision of internet access, caching and hosting level, when discussing abuse mitigation, while in principle these actors also rely on the DNS in order to provide their services to the public. The existing rich body of law concerning the intermediary liability framework in the EU, reiterated in the Digital Services Act proposal that maintains the key principles of limited liability, includes a clear prohibition of imposing a general monitoring obligation for illegal activity taking place in connection to the services offered by intermediaries, as well as a notice and action procedure relevant for hosting service providers.

The conclusion of the DNS Abuse Study on **the definition of DNS abuse** that in principle includes all illegal activity on the internet (e.g. cybercrime, hacking, malicious conduct, (cyber)security threats, illegal and fraudulent activity) **is inconsistent with its accompanying explanation, together with the described abuse mitigation measures** that only target a limited number of technical intermediaries, without adequately considering the legal frameworks and the existence of voluntary measures governing each actor.

Consequently, **any mitigation and prevention measures addressed within the Study should also encompass all actors involved in sustaining and using the DNS,** per the broad definition adopted by the authors.

Limited research on the magnitude of DNS abuse

The estimation of the magnitude of DNS abuse across different TLD zones was essentially based on 16 blacklists provided by 6 blacklist providers, according to the Study. It is worth noting that data provided solely by blacklist feed providers is primarily optimised for blocking (by inter alia internet service providers), rather than for the suspension of domain names by registries and registrars. CENTR acknowledges the limitations of these feeds, as also rightfully stressed by the authors of the Study. However, it is worth pointing out that any research based on the blacklists provided by these commercial actors is not available for independent verification. Furthermore, these lists may include URLs randomly queried by Domain Generation Algorithms (DGAs) and other botnets that include domain names that may not even be registered by specific TLDs to be mitigated by the measures targeting domain registration processes.

It would have been helpful for the Study, when acknowledging the limitations of its own research, to identify the shortcomings of these data sources and provide valuable input either directly to the blacklist providers or independent cybersecurity researchers on how to measure abuse more accurately.

Overlooking the essentiality of the DNS for the provision of services

ccTLDs, as technical operators of the internet infrastructure, are considered to be 'operators of essential services' under the NIS Directive and consequently also 'essential entities' under the upcoming NIS 2 Directive.

Each ccTLD maintains the authoritative name servers for the specific top-level domain(s) managed by that ccTLD. Every authoritative name server managed by a ccTLD provides information about all the delegations and complete DNS information of registered domain names.

A domain name and its management are distinct from, and cannot be equated with the content of any services related to the domain name, that are provided by other intermediaries (such as web hosting companies, mail service providers etc).

The essentiality of the DNS, and specifically of TLD operators is recognised in the EU.[6] ccTLDs do not have the technical capacity to directly target unlawful content online. They can only suspend the underlying technical infrastructure, i.e. the domain name that will disrupt the functioning of all associated services (such as website or email hosting). However, this drastic measure does not remove illegal content from the internet: the unlawful content remains reachable through other means (e.g. directly typing the IP address in the browser). The existing EU legal framework in the area of consumer protection clearly establishes a certain proportionality standard when action at ccTLD level can be mandated. In addition, any action at ccTLD level can only be mandated "when appropriate" and when contacting other intermediaries closer to the content have not brought about any results.[7]

The DNS Abuse Study makes an assumption that goes against this established proportionality principle that has been codified in EU legislation. According to the authors of the DNS Abuse Study, "to effectively address abuse cases, requiring the abuse reporters the[*sic*] exhaust a rigid linear referral path (website operator - registrant - hosting provider - reseller, if any - registrar - registry operator) is not appropriate"[8].

The authors of the Study solely base their findings on one generalised example when dismissing the proportionate resolution path first targeting the intermediary that is closest to the content. The DNS Abuse Study has therefore **not provided any clear justification, nor abuse-specific explanation on why a proportionate resolution path targeting the intermediary that is closest to the content first is not appropriate**, beyond a simplistic statement that this is generally not effective.

In some specific and clearly-defined cases, action at DNS level might indeed be appropriate without the need to exhaust the linear referral path. However, it is worth pointing out that any action at DNS level, considering the essentiality of the DNS infrastructure to the functioning of any connected services, must be based on a clear legal basis (e.g. obligation under local legislation, contractual or local policy requirement, a court order, referral from the competent public authority, including law enforcement etc).

Furthermore, with a suggested definition of DNS abuse ranging from malware distribution to intellectual property rights infringements to the availability of child sexual abuse material, the legal basis for action at DNS level can be different, together with the legal framework governing the needed intervention. Each case depends

[6] Regulation (EU) 2019/881 ('EU Cybersecurity Act'), Recital 22: "The public core of the open internet, namely its main protocols and infrastructure, which are a global public good, provides the essential functionality of the internet as a whole and underpins its normal operation.[...]public core of the open internet and the stability of its functioning, including, but not limited to, key protocols (in particular DNS[...], the operation of the domain name system (such as the operation of all top-level domains)[...]".

[7] Regulation (EU) 2017/2394 ('Consumer Protection Cooperation Regulation'), Article 9(4)(g).

[8] DNS Abuse Study, p. 38.

on the gravity of the specific infringement, its persistence and widespread reach, together with several means available for authorities and abuse reporters to pursue the mitigation (including the difference between the intermediary that is considered to be the closest to the source of the problem).

Any generalised statements without providing a clear analysis on the existing practices of DNS service providers, TLD registries and registrars in the context of specific abuses cannot be considered as factual and evidence-based research.

The Study's recommendations to address DNS abuse

A "one-size-fits-all" approach

According to the Study, EU ccTLDs are "by far the least abused in absolute terms and relative to their overall market share",[9] with only 0.8% of all abused domains registered under EU ccTLDs, in comparison to other actors active on the domain name market (such as generic TLDs or gTLDs). Yet, the DNS Abuse Study adopts a "one size fits all approach", as the proposed recommendations target either both ccTLDs and gTLDs, or solely ccTLDs, despite the fact that the level of abuse has been shown to be the lowest amongst European ccTLDs. Most notably, the DNS Abuse Study recommends further harmonisation of ccTLD practices, or calls on ccTLDs to adopt the practices of gTLDs.

Requiring ccTLDs to unify their policies and practices with gTLDs despite the differences regarding the level of abuse between both actors is incoherent with the Study's own conclusions. Most importantly, it creates a risk of imposing a disproportionate burden on ccTLDs, who seem to have demonstrated the efficiency of their current practices in limiting DNS abuse according to the findings of the Study.

Secondly, the **recommendations requiring ccTLDs to put in place similar measures to gTLDs also disregard the fundamental difference between the governance of gTLDs and ccTLDs.** While technically a ccTLD and a gTLD perform similar functions in the DNS, their widely different policy arrangements are openly recognised by all stakeholders in the internet ecosystem. ccTLDs are governed by national and international law, while gTLDs also need to comply with ICANN policies. The specific rules and policies that govern ccTLDs depend on their country of establishment.

The one-size-fits-all approach recommended by the DNS Abuse Study disregards the well-established principle recognised in global Internet Governance that allows discrepancies between the policy arrangements of ccTLDs and gTLDs, but also amongst ccTLDs. While it is beneficial to share experiences across the industry, including by ccTLDs that already share their experiences amongst peers in different fora, including ICANN, it is unclear why ccTLDs should strive for a greater harmonisation of their operations, while the conclusions of the DNS Abuse Study show no evidence of wide-spread abuse across European ccTLDs.

In the absence of compelling evidence of a widespread problem with DNS abuse at EU ccTLD level, it may be assumed that the existing good practices and voluntary measures taken by ccTLDs to limit abuse are sufficient to keep abuse out of their zones.

[9] DNS Abuse Study, p. 53.

Registration data accuracy obligations

The Study recommends that TLD registries "verify the accuracy of the domain registration (WHOIS) data", among others, through harmonised Know Your Business Customer (KYBC) procedures and eID authentication.

First of all, this recommendation disregards the fact that harmonised data verification and KYBC obligations through eID authentication are not feasible due to the absence of functioning eID schemes across all EU Member States: out of 27 EU Member States only 16 currently have an eID scheme in place. As a result, ccTLDs would be required to collect and store additional personal information in order to fulfil KYBC obligations, in conflict with many existing efforts to comply with the EU data protection framework.

Furthermore, registration policies across ccTLDs are deeply rooted in the national legal frameworks of the Member States. European ccTLDs have established various ways and methods to keep registration data accurate. Some ccTLDs make use of national eID schemes in the domain name registration process,[10] others perform additional registration data checks post-registration based on the internal tools available for screening new registrations.[11]

In the absence of proof regarding significant abuse across EU ccTLDs, it is unclear why the Study recommends further harmonisation of KYBC practices through eID authentication. **ccTLDs should be able to continue carrying out their existing data accuracy practices, in line with the basic data protection principles** (such as purpose limitation and data minimisation) and in accordance with locally available tools. It is important to keep this in mind in light of the ongoing negotiations on the data accuracy obligation within the NIS 2 Directive that will strive for a minimum harmonisation of all TLDs active within the EU market (not only targeting EU ccTLDs).

Disproportionate verification obligations will hamper access to basic infrastructure by businesses and customers who wish to establish their online presence within the European domain space. This would cause a competitive disadvantage to the EU ccTLD industry, as end-users would rather opt for a more convenient option than a European domain name. Other options (such as a social media page) will allow the user to establish an online presence much faster and at much less cost.

Finally, the Technical Report accompanying the Study acknowledges the uncertainty of attributing low abuse levels solely to verification checks, as there seems to be only "anecdotal evidence indicating that cybercriminals choose to[...] avoid TLDs that strictly verify the registrant identity". The Technical Report concludes that "there is a need for a very comprehensive statistical analysis of factors driving DNS abuse."[12]

While making recommendations in the executive part of the Study, the authors of the DNS Abuse Study should have made these limitations more evident, as otherwise their conclusions can be considered construed.

---

[10] E.g. The use of NemID for verifying identities of individuals and businesses based in Denmark by DK Hostmaster (.dk); the Estonian Internet Foundation requires verification of .ee registrants with the use of Estonian eID solutions and also accepts the use of ID cards from Belgium, Latvia, Lithuania, Finland.

[11] E.g. the APEWS tool developed by EURid to screen for potentially abusive registrations; screening system developed by DNS Belgium to scan new registrations for incorrect registration data; machine learning tool used by SIDN (.nl) to identify potentially fake webshops.

[12] Technical Report - Appendix 1, p. 35.

Access to complete WHOIS data

The Study recommends that "ccTLDs should, in the same manner as gTLDs, provide a scalable and unified way of accessing complete registration (WHOIS) information using the Registration Data Access Protocol (RDAP)".

First of all it is worth mentioning that RDAP is not an industry-wide recognised standard across TLDs. While RDAP has been developed to address some of the shortcomings of its predecessor - the WHOIS protocol - neither the Study nor the accompanying Technical Report provide any reasoning as to *why* RDAP should be the preferred standard for providing access to registration data, beyond the statements of its alleged benefits for third party access.

In this regard, it should be recalled that WHOIS (and RDAP) records contain the personal data of domain holders, such as their name and contact details alongside other information, e.g. the registration and expiration date of the domain. Personal information, such as names and contact details of domain name holders, fall under the scope of the EU General Data Protection Regulation (GDPR). Under the GDPR, any processing of personal data, including its consultation, use, and disclosure by transmission[13] can only be considered lawful under certain conditions, e.g. when the data subject has given their express consent to the processing of their personal data, when it is necessary to comply with legal obligations, or for the purpose of legitimate interests.[14]

Furthermore, the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) have confirmed that entities providing domain name services, including ccTLDs, can only grant access to registration data if there is a clear legal basis for such action provided by law,[15] whilst the Court of Justice of the European Union (CJEU) has clarified that such a legal basis must define the scope of limitation of the exercise of the rights concerned.[16]

The recommendation put forward by the Study to "provide a scalable and unified way of accessing complete registration (WHOIS) information" therefore **disregards the current data protection framework in the EU and the requirement to balance the interest of third parties and data subjects on a case-by-case basis.**

Furthermore, it is worth recalling an earlier analysis issued by WP29 (the predecessor of the EDPB) in the context of ICANN's response to GDPR compliance in 2018 that found that any unspecified requirement to provide "legitimate access" to "uniform registration data" does not amount to a specified purpose within the meaning of Article 5(1)(b) of the GDPR. Furthermore, **the interests of third parties in the processing of and access to personal information should not determine the purposes pursued by TLD operators in collecting and providing access to personal information.**

---

[13] Regulation (EU) 2016/679 ('General Data Protection Regulation'), Art 4(2).

[14] Ibid, Art 6(1).

[15] The European Data Protection Board's Statement in 02/2021 on new draft provisions of the second additional protocol to the Council of Europe Convention on Cybercrime (Budapest Convention), adopted on 2 February 2021. Available here: https://rm.coe.int/edpbstatement022021onbudapestconventionnewprovisions/1680a1617f; European Data Protection Supervisor, Opinion 5/2021on the Cybersecurity Strategy and the NIS 2.0 Directive, 11 March 2021. Available here: https://edps.europa.eu/system/files/2021-03/21-03-11_edps_nis2-opinion_en.pdf

[16] See for example CJEU, C-419/14, paragraph 81.

Furthermore, WP29 has stressed that in the context of access to WHOIS, there is a need to implement appropriate technical and organisational security measures that result in the appropriate identification, authentication and authorisation of the entities which are allowed to access non-publicly available WHOIS information.[17]

Unfortunately, the overarching EU data protection framework has received minimum recognition within the DNS Abuse Study, evident from one limitation in parentheses and a mere footnote within the recommendations[18], while the confidentiality of data is considered to be one of the cornerstones of information security.[19]

Consequently, calling for "a scalable and unified way of accessing complete registration (WHOIS) information" disregards the overarching EU data protection framework, as well as the recommendations put forward by WP29 in the context of ICANN's response to GDPR compliance.

Finally, the Study makes several assumptions and cites difficulties in accessing non-public WHOIS records based solely on experiences within gTLDs and other contracted parties with ICANN. The DNS Abuse Study, in this regard, completely disregards European ccTLD experiences who were largely complying with their national data protection frameworks per the previous EU Data Protection Directive, long before the EU GDPR entered into force. By the time the EU GDPR entered into force, the majority of EU ccTLDs were already redacting publicly available registration data. The majority of ccTLDs provide some form of access to non-public registration data containing personal information, primarily for law enforcement purposes, to the parties identified in a court order and all other parties who can demonstrate their legitimate interest in obtaining access to non-public registration data.

Publication of zone file

The Study recommends that ccTLDs consider "publishing DNS zone file data through DNS zone transfer of a system similar to the Centralized Zone Data Service (CZDS) maintained by ICANN". The Technical Report accompanying the Study concludes that the majority of ccTLDs do not make their zone files available to third parties, putting forward only one possible reason behind it which is a risk of "unforeseen negative consequences" for the security and stability of ccTLDs. The Technical Report does not provide any further reasoning or analysis as to what these potential negative consequences for security and stability might be, nor any further detail about ccTLDs' reasoning for not making their zone files publicly available. At the same time, the Technical Report concludes that zone file publication was introduced by ICANN in the interest of mitigating abusive and criminal activity, and therefore that ccTLDs should consider following a similar recommendation.

First of all, as the aim of the Study is to provide analysis on the scope and reasons why certain types of abuse are recurring, it is unacceptable to support recommendations that are based on simple statements without an

[17] ARTICLE 29 Data Protection Working Party correspondence with ICANN, April 2018. Available here: https://edpb.europa.eu/news/news/2018/european-data-protection-board-endorsed-statement-wp29-icannwhois_en

[18] Footnote 21 on p. 15 of the DNS Abuse Study: "This recommendation is without prejudice to current legislation on data protection (GDPR)[...]".

[19] See for example the definition of 'security of network and information systems' as enshrined in Article 4(2) of the NIS Directive.

attempt to understand the reasoning of the "operators of essential service" in the EU (such as ccTLDs) and why ensuring a stable, secure and resilient service is important for such operators.

Second, the differences in approaching the publication of zone files from a ccTLD perspective have also been recognised by the ICANN community, citing risks of abuse of data, data harvesting, distribution of spam and online scams as some of the potential cybersecurity risks expressed by the ccTLD community.[20] Subsequent research on the topic of abuse and cybercrime in new gTLDs has also concluded that "making the zone files of new gTLDs open to security research ***may indirectly contribute*** to improving the security of the new gTLD domain space. It does not, however, prevent miscreants from registering domains for malicious purposes" [emphasis added].[21]

Considering the purpose of the Study is to encompass any illegal or harmful activity involving the DNS, irrespective of whether it concerns purely technical threats or the availability of illegal content, it is not entirely clear why the authors of the Study avoided looking into the risks of further distribution of online scams and spam as a result of publicly available zone files, and failed to consider these as potential DNS abuse issues.

Furthermore, by including a recommendation where the net positive effect on cybersecurity depends strongly on local context, without considering the potential negative effects on the stability and resilience of an essential service and on the confidentiality of customer data, the Study comes across as biased and non-fact based research.

[20] ICANN Zone File Access Advisory Group, Concept Paper gTLD zone file access in the presence of large numbers of TLDs, 18 February 2010.

[21] Maciej Korczyński, Maarten Wullink, Samaneh Tajalizadehkhoob, Giovane C. M. Moura Arman Noroozian, Drew Bagley, and Cristian Hesselman, "Cybercrime After the Sunrise: A Statistical Analysis of DNS Abuse in New gTLDs", 2018.