Council of European National
Top-Level Domain Registries

Domain name registries and online content

Table of contents

Executive summary 4

Introduction 6

Objective of this paper 6

Outline of this paper 6

The internet, the domain name system and online content 7

The DNS as part of the internet infrastructure 7

The internet and IP infrastructure 7

The domain name system 7

Online content 8

Making content available online 8

Using the DNS as a tool to help to find content 9

Taking action against illegal content on the net 11

What is illegal content? 11

Defined by local legal frameworks 11

Who can judge the legality of content? 11

Where is online content located? 12

Location on the internet 12

Physical location 13

Removing illegal content 13

Contacting the content publisher or the hosting provider 13

Contacting the domain name holder 13

Making finding content more difficult 14

Further steps to take when deleting illegal content is unsuccessful 14

Risk and drawbacks when deleting a domain name at the registry 14

Current ccTLD practices 17

Education and awareness-raising, with special attention for an open dialogue and cooperation with authorities and LEA 17

Community-wide education and awareness-raising 17

Education and close collaboration with authorities and LEAs 18

Registries as providers of authoritative domain name data 20

Sharing registration data with third parties 21

Responding to reports of suspicious content 22

Responding to external reports 22

Detecting illegal activity with additional measures 23

Conclusion 24

Executive summary

CENTR members, who are ccTLD registries, manage internet country code top-level domains (ccTLDs). Their responsibilities range from providing and operating the technical DNS infrastructure for their TLD, organising the domain name registration process to proactively maintaining the registry database, so that domain names can be used to navigate the internet.

Abusive and illegal content decreases trust and confidence in the internet as a platform for innovation, creativity and economic opportunity. ccTLD registries are committed to contributing to a comprehensive and effective approach against illegal online content.

The internet is a global collection of interconnected computer networks that allows communication by using unique numerical IP addresses. The Domain Name System (DNS) functions as a layer on top of the IP infrastructure. Domain names make it easier for humans to navigate the internet. For example, when a user types in a website's domain name, the DNS will tell the user's device what the corresponding IP address is where the content of the website can be found.

To be reachable over the internet, content must be stored on at least one computer or server that is connected to the internet. To effectively remove content from the internet, it has to be deleted from the device where it is hosted, or that device must be disconnected from the internet.

The qualification of content as 'illegal' depends on the local legal framework and may even vary depending on the context. Who has the authority to make this judgement is defined at local level.

Removing illegal content from the internet is the only effective way to avoid content being accessed and consumed. Two parties have direct access to the content or the device that stores the content: the content publisher and the hosting provider. They are the first to be contacted.

Where a domain name is used to facilitate access to content, the domain name holder may be the provider of the content and hosting, or be able to identify the provider. The registry's authoritative database with information on all domain names registered under its TLD can help to identify and contact the domain holder.

When it is not possible to remove illegal content from the internet, which is the only effective solution, one might try to make it more difficult for users to find or access the content. There are different methods of 'blocking' internet content, at different levels and involving different players. However, all have in common that the content remains available and that the action may cause unintended collateral damage. Therefore they should be regarded as an interim measure to be used in the case of an emergency or when everything else has been tried and has failed. Blocking or deleting a domain name is one such measure.

Local legal frameworks define what content is illegal, who has been given the authority to deal with it and what processes are permissible within the rule of law. This may vary from country to country. ccTLD registries have different requirements regarding who can register domain names and what their duties are. The combination of these requirements and the local legal framework influences what policies and initiatives the registry develops to approach the issue of illegal online content.

Typically these policies are rooted in the local community, are compatible with local laws and address local needs, and often have been developed in consultation and cooperation with other local stakeholders. Successful policies and practices for one ccTLD could inspire others. However, due to the local roots and particularities, there is no guarantee that copying the project or policy will lead to the same positive result, or indeed be legal within another ccTLD.

As an approach to illegal content, ccTLD registries, amongst others, focus on:

- Community-wide education and awareness-raising.
- Education and close collaboration with authorities and LEAs.
- The maintenance of the registry database to improve the quality of the registration data. This may have an indirectly positive impact, as it is unlikely that those with bad intentions would register a domain name using correct personal information.
- Establishing procedures to share registration data with third parties within the limits of local privacy regulations.
- Developing processes and procedures to respond to reports of suspicious content. These procedures usually have in common that they are applicable to limited and well-defined cases, and that an external party with expertise in assessing that type of content is involved.

Introduction

CENTR members manage the registry for one or more internet country code top-level domains (ccTLDs). Their responsibilities range from providing and operating the technical DNS infrastructure for their TLD, organising the domain name registration process to proactively maintaining the registry database, so that domain names can be used to navigate on the internet.

CENTR members believe that online trust and safety are essential for the internet to remain a platform for innovation, creativity and economic opportunity. Abusive and illegal content decreases trust and confidence. Registries are committed to contributing with other actors to a comprehensive and effective approach against illegal content on the internet.

Objective of this paper

Joint efforts and successful cooperation require that stakeholders understand and respect each others' function, role and limitations. The objective of this paper is to shed light on the role of a ccTLD registry operator, explain its relation to online content, explore the possibilities and limitations of actions, and set expectations about what a registry can and cannot do when it comes to illegal online content.

Outline of this paper

The first section of the paper provides an insight into how the internet works, where online content is located and how it can be accessed, and explains the facilitating role of the domain name system (DNS).

The second part of the paper looks at the issue of illegal content on the internet and examines how ccTLD registry operators could contribute to actions that lead to the removal of illegal content.

A third section is dedicated to current registry policies and practices. Through its non-exhaustive list of examples, it showcases how different ccTLD registries develop policies and take actions that best serve the needs of their local communities, and contribute as such to the joint battle against illegal online content.

The internet, the domain name system and online content

The DNS as part of the internet infrastructure

The internet and IP infrastructure

The internet is a collection of computer networks that are interconnected and together form a global communication system. The Internet Protocol (IP) is the method or set of rules by which data is sent over the internet from one device to another. To have a successful transfer, it is important that the sender and receiver can be identified and located amongst the millions of computers, smartphones, servers, IoT and other devices that are connected to the internet. Therefore, all connected devices have at least one IP address that uniquely identifies it from all other devices. An IP address can be represented as a numerical label: [1] for example the IP address 2001:db8:85a3::8a2e:370:7334[2] could identify the interface of a server where the content of a website is stored.

The domain name system

For humans, reading and remembering numerical IP addresses is difficult. To solve this, the domain name system (DNS) allows for the use of domain names to refer to IP addresses. The DNS functions as a layer on top of the IP infrastructure. When, for example, a user types a domain name in a browser or clicks on a link with a domain name, the device will look up the corresponding IP address in the DNS. When the domain name resolves - 'resolves' means that the DNS returns an IP address - the user's device knows where on the internet the content of a website or the mailbox connected to an email address can be found.

The DNS is characterised by its hierarchical structure, consisting of different top-level domains (TLDs) under a single root. The extension of a domain name, that is the part after the last dot, indicates under which TLD the name is registered (for example .de, .com, .fr). The hierarchical structure is relevant for the functioning of the DNS and the iterative way of looking up domain names.[3]

A domain name registry is responsible for the management of one or more TLDs. All registries need to respect the technical rules and requirements of the DNS, but with regard to policy each TLD remains responsible for setting its own rules. Whilst generic TLDs (gTLDs) have to abide by overall policies and processes developed by the ICANN community, country code TLDs (ccTLDs) set their own policy according to the needs of their local internet communities.

---

1 IPv6 addresses are 128 bits long and portrayed using a hexadecimal string, the older IPv4 version is 32 bits long and is noted in groups of decimal numbers separated by dots.

2 This IP address is for documentation purposes only and is not routed to the public internet (RFC 3849, IPv6 Documentation prefix).

3 For more on the functioning of the DNS: https://www.centr.org/about-the-industry/item/the-dns.html.

Online content

Content has to be created, stored and made available before it can be found on the internet. How this happens is described in this section by identifying the different roles and responsibilities.[4]

Making content available online

Content provider

The content publisher supplies the internet with text, sound, images, videos, animations and other forms of content that are uploaded on a website, published on a blog, made available on social platforms etc. The content publisher can be, but is not necessarily, the original creator of the content.

To be reachable over the internet, content must be stored on at least one computer or server that is connected to the internet. A content publisher can use their own computer or server or, more likely, make use of the services and infrastructure of a hosting provider.

Hosting provider

A hosting provider supplies storage and connectivity, has the technical expertise and, more importantly, the necessary infrastructure, capacity and bandwidth to cope with traffic that could come from anywhere on the internet at any time of the day. Hosting providers provide the platform for content to be hosted but do not decide what is or is not published - their customers (the content publishers) do. With a few exceptions, usually large organisations with their own infrastructure and networks, a content provider will use the services of a hosting provider. Hosting providers have large data centres with servers that contain their clients' content. These servers are connected to the internet and can be identified by their unique IP address. There are different kinds of hosting; the most common are web and email hosting. Social media hosting (e.g. user-generated videos) could be considered a special case in between publishing and hosting.

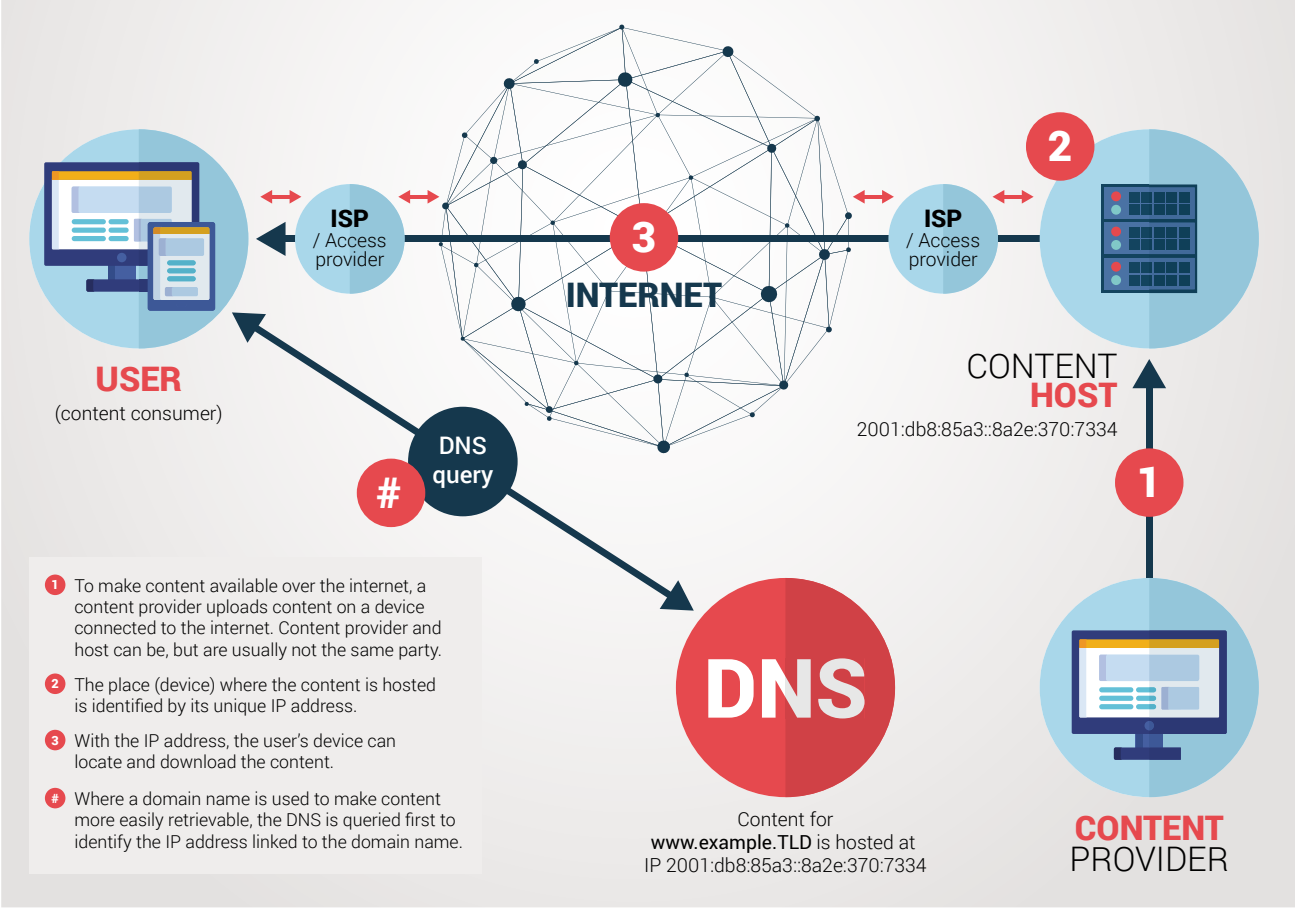
Internet service provider / access provider

The internet Service Provider (ISP) provides internet access. Via the ISP's network and infrastructure its clients can access the internet. The ISP will assign IP addresses to the devices connected to its network, for example the servers of the hosting provider, the modem of the internet user, etc. The ISP is an access provider and so does not store any content, but content travels over its infrastructure.

There are other players that ensure the transportation and exchange of data between networks, like Internet Exchange Points (IXPs) and operators of (short or long distance) carrier networks, or Content Delivery Networks (CDN)[5] that host copies of their clients' content on servers at different geographic locations to optimise the experience for the end user (for example Cloudflare). Their relation to content is not discussed further here.

4 Actors can combine one or more roles described in this section, for example an ISP can also provide hosting services.

5 https://en.wikipedia.org/wiki/Content_delivery_network



Using the DNS as a tool to help to find content

The Domain Name System (DNS) provides a function that helps "navigate" the internet, it allows for the retrieval of the IP address linked to a domain name. Therefore, some compare the DNS with a telephone book or a property or company register.[6]

Domain name holder / registrant

A content publisher may register a domain name to make it easier for internet users to retrieve the content they have made available online. The domain name functions as a label on top of the IP address, is easier to memorise than the numerical IP address and can contain useful information, such as a company name in an email address, or a reference to the content in a website's domain name.

The domain name holder is not necessarily the (or the only) provider of the content published under the domain name. For example large university websites, blog sites, or social network websites allow others to publish content on a site identified by a single domain name.

A domain name holder or registrant holds the right to use a specific domain name. To obtain this right, a person or an entity registers the name with the TLD registry, directly or via a registrar. The domain holder is responsible for how the name is used.

6 https://en.wikipedia.org/wiki/Domain_Name_System

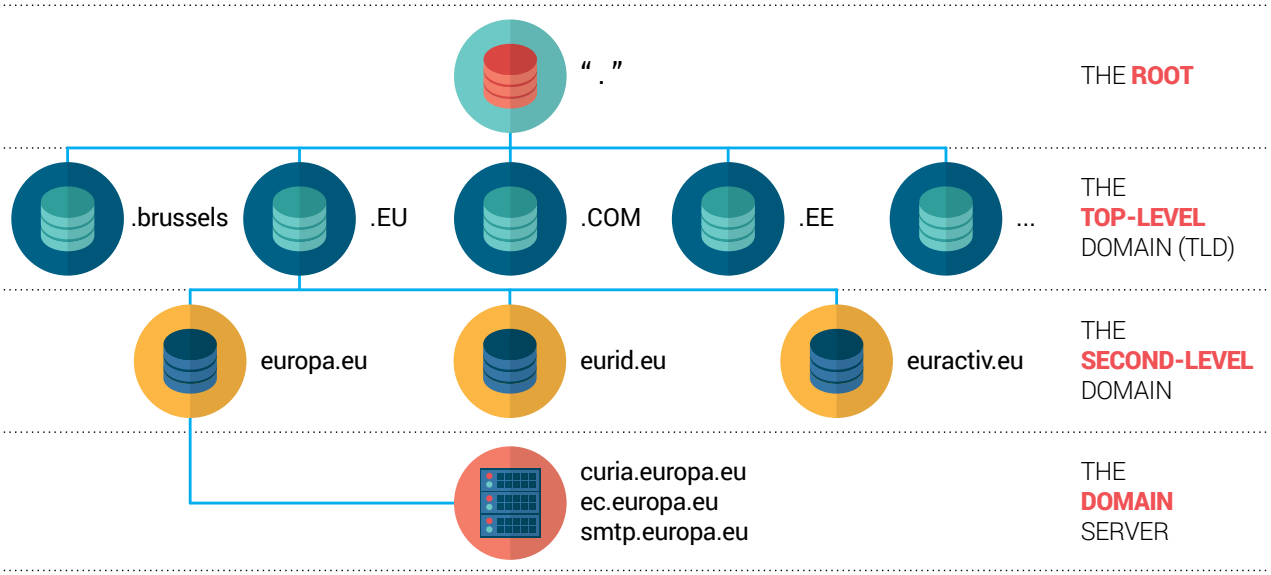
Domain name registrar

A registrar is a company that provides domain registration services to companies and individuals, directly or via a network of resellers. The registrar is accredited by one or more registries to offer domain names under their TLD. The registrar will check the availability of the domain name and handle the registration process, whilst the registry manages the TLD of the requested name. As part of the registration process, the registrar will submit the domain holder's contact information and the technical information related to the domain name (for example, what name servers contain the DNS records that will tell web browsers and email clients where to find the webserver with the site's content or the mail server handling email). A registrar does not host content, and no content passes through its infrastructure. In practice however, many registrars will also provide hosting and other services for their clients.

TLD Registry Operator

The registry manages the one and only authoritative database of registered domain names under its TLD and publishes this information in the DNS. The servers of a domain registry contain information on the domain holder, the domain registration (for example, the date of expiry), the IP addresses linked to the domain name, and other technical details. A registry will publish an updated zone file several times per day, which is a text file that contains mappings between the domain name and the domain name's own nameservers for each registered name, as well as other resources. This file contains the information on how to locate IP addresses and other information needed to navigate on the internet. Registries do not store or enhance content.

> Note: Most ISPs cache DNS information on recently queried domain names from different TLDs in so-called non-authoritative name servers to speed up the surfing experience for their clients. It is only when a recent answer is not available on the ISP's server that the DNS will be queried. As a consequence, changes made to the DNS (such as the removal of a domain name from the DNS by the registry) may take some time before they become effective everywhere on the internet.



Taking action against illegal content on the net

What is illegal content?

Defined by local legal frameworks

The term "illegal" is used to describe content that is prohibited in a national context, no matter what the reason. The European Commission for example defines illegal content as "any information which is not compliant with Union law or the law of a Member State concerned".[7] Apart from issues relating to child sexual abuse, there is little international consensus on what constitutes appropriate content from a public policy perspective. What is allowed in one jurisdiction may be prohibited in another. The permissibility of content can also be context-related: content that is judged illegal in one context (such as indecent comedy viewed by children) may be acceptable in another (such as when viewed by adults) even within the same jurisdiction.[8]

Some countries have established a targeted legal framework on online content, while in other jurisdictions online content issues are addressed based on existing general frameworks that are not specific to the internet. A comparative study in 47 CoE Member States found four broad categories of legal grounds to judge the legality of online content:

- the protection of health and morals (including child sexual abuse material or illegal gambling);
- the protection of national security, territorial integrity or public safety (including counter-terrorism);
- the protection of intellectual property rights; and
- the protection from defamation and unlawful treatment of personal data.[9]

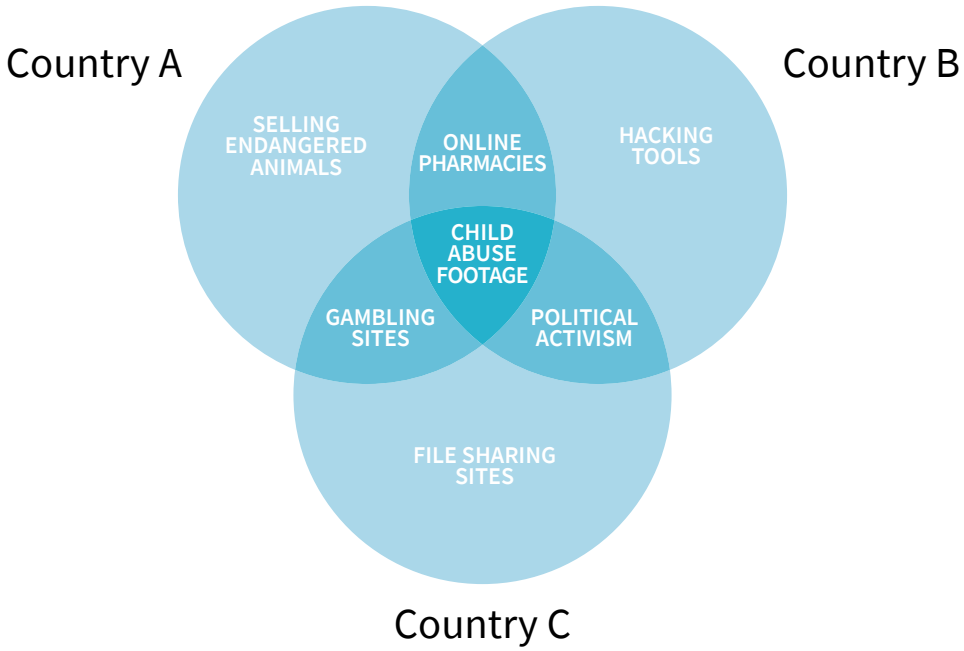
Who can judge the legality of content?

The qualification of content as 'illegal' depends on the local legal framework and may even vary depending on the context. Whether content is illegal or not is a decision for local courts or competent authorities. Furthermore, the process followed may vary even within the same jurisdiction. Some authorities may have the power to judge the legality of content and act directly from that judgement, while other authorities must seek a court decision in order to be empowered to act on the content.

7 Commission Recommendation of 1.3.2018 on measures to effectively tackle illegal content online, C(2018)1177, European Commission, March 2018, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32018H0334

8 Internet Society Perspectives on Internet Content Blocking: An Overview, Internet Society, March 2017, https://www.internetsociety.org/wp-content/uploads/2017/03/ContentBlockingOverview.pdf

9 Comparative study on blocking, filtering and take-down of illegal internet content, CEO, December 2015, https://edoc.coe.int/en/internet/7289-pdf-comparative-study-on-blocking-filtering-and-take-down-of-illegal-internet-content-.html (accessed on 7 June 2018).



Venn diagram showing that what is legal in some countries is not in others

The content publisher is responsible for the content that is made accessible to other internet users. It is the domain holder's responsibility that his or her domain name is not used to facilitate finding illegal content on the internet. To add another layer of complexity, the provider and the user consuming the content might not be in the same jurisdiction. Moreover, the content itself might be hosted in yet another geographical region with its own laws, morals and definitions of what is legal and not.

A ccTLD registry is in the same position as any organisation or even individual with regard to online content. A registry can make an assessment and form an opinion of what it thinks is within and outside the borders of the law. It does not have a special authority to effectively judge the legality of content that is put online. When a registry accesses online content, it does this in the same way that any person would surf over the internet to a website and load the content on its computer. There is no shortcut where a registry can gain insight into what content is published by the domain holders. ccTLD registries do not host any content and no content passes through their infrastructure.

Some registries foresee the possibility to take action in obvious cases of illegal content where there is not much doubt and the liability risks are minimal in their terms and conditions. In general, registries are not equipped, staffed or well placed to proactively scroll the internet for illegal content.

Where is online content located?

Location on the internet

To be reachable over the internet, content must be stored on at least one computer or server that is connected to the internet. The location of the content is specified by the unique IP address(es) of the device(s)[10] on which it is stored.

10 Technically speaking the IP address identifies the interface across which the device exchanges information, not the device itself.

Physical location

Geographically, the device(s) that contain(s) the content can be placed anywhere in the world where there is power and a connection to the internet. Other than that, there are no strict rules or requirements for where content should be hosted technically, even though the physical location can have an influence on the speed and quality of the connection.

Content can be stored on just one server, or placed on different servers (for example, cloud hosting, clustered hosting). Content can be on one or more servers in the same country as the content provider and the user of the content. These servers can also be anywhere in the world and fall under the rules of different jurisdictions.

Removing illegal content

Removing illegal content from the internet is the only effective solution that avoids content being accessed and consumed. It can be achieved by either deleting the content from the device on which it is stored or by disconnecting that device from the internet.[11]

Contacting the content publisher or the hosting provider

Two parties have direct access to the content or the device that stores the content: the content publisher and the hosting provider. The content publisher has the tools and access codes to change or remove the content he or she has put on a website, made available on a social media platform, or elsewhere. The hosting provider can remove the content from its servers or effectively prevent the content from being accessed on its infrastructure.

It should be noted that hosting providers usually store content from different clients on the same physical machine, therefore disconnecting or seizing a server may affect different content providers and make legitimate content inaccessible. Social network and blog site operators may have the possibility to remove objectionable posts or illegal content that is posted on their platforms.

Contacting the domain name holder

The domain holder is the first party to contact if a domain name is used to facilitate access to illegal content. It could be that the domain holder is the same person or in close contact with the content publisher. The domain holder may not be the source of the illegal content or may not be aware that their domain name is being used to facilitate access to illegal content.[12] However, in most of those cases the domain name holder should be able to help identify the source of the illegal content and take action to remove it.

The registry maintains the authoritative database with information on all domain names registered under its TLD and can help to identify and contact the registrant. The registry's database contains amongst other information on the domain holder, the domain registration (e.g. date of expiry) and the nameserver addresses related to the domain name.

---

11 CENTR video on ccTLDs and online content explained: https://www.youtube.com/watch?v=kVwKDq-qUwY

12 For example in the case of large university networks or social media platforms, where many users publish content etc., or when a server is compromised and used by criminals to host content.

ccTLD registries put a lot of effort into the maintenance of their database and accept legitimate requests for information. Contacting the registry for information on the domain holder can be a first step in the process of effectively removing illegal content from the internet. There is more about this in section III on current registry practices.

Note: for law enforcement and authorities in particular, it might be worth contacting registrars, as they may be able to provide additional useful information such as billing or credit card details and information on what other domains are registered by the same client, etc.

Making finding content more difficult

Further steps to take when deleting illegal content is unsuccessful

When it is not possible to track down or get in contact with the content publisher or hosting provider to remove the illegal content from the internet, which is the only effective solution, one might try to make it more difficult for users to find or access the content. There are different methods of blocking internet content, at different levels and involving different players. A 2017 report by the Internet Society[13] describes the most current methods and assesses how well they work. The paper looks at IP and protocol-based blocking, deep packet inspection-based blocking, URL-based blocking, platform-based blocking and DNS-based blocking at network or ISP level. The report concludes that, regardless of the level and method, "the use of internet blocking to address illegal content is generally inefficient, often ineffective and prone to cause unintended collateral damages to internet users". Blocking content does not solve the problem: the content remains available and therefore blocking should be regarded at as an interim measure in the case of an emergency or when everything else has been tried and has failed.

This paper focuses on actions taken at the domain registry, such as when a registry prevents a domain name from resolving to a valid IP address by temporarily blocking the domain name or deleting it from the zone.

Risk and drawbacks when deleting a domain name at the registry

Blocking or deleting a domain name and as such removing it from the DNS means that a user will no longer get a valid IP address when looking up the domain name. The user will receive an error message informing them that the domain name does not exist instead of loading the expected website.[14]

Deleting or blocking a domain name is a fairly simple technical operation but a drastic intervention in the DNS, with the effect that the domain name can no longer be used to

13 Internet Society Perspectives on Internet Content Blocking: An Overview, Internet Society, March 2017, https://www.internetsociety.org/wp-content/uploads/2017/03/ContentBlockingOverview.pdf

14 Domain Conflicts in the Legal System, Norid, September 2017, https://www.norid.no/en/om-domenenavn/veiledere/domenekonflikter-i-rettssystemet/

navigate to content (illegal as well as legal) that is published under the domain name and its different subdomains, and that all services linked to the domain name, such as email, stop working. This usually happens within hours, but can also take some days because of caching. Any decision to delete or block should take into consideration all the consequences and balance prudence with proportionality. The EU Regulation on Consumer Protection Cooperation (effective January 2020) for example clearly states that ordering registries to delete domain names should only be considered "where no other effective means are available to bring about the cessation or the prohibition of the infringement covered by this Regulation and in order to avoid the risk of serious harm to the collective interests of consumers."[15]

Some ccTLDs, based on their local law and jurisdiction, have established relationships with their domestic law enforcement agencies (LEAs) and/or reputable security companies or national CERTs to improve trust and security in their ccTLD by expeditiously deleting or deactivating domain names which are used for criminal purposes. Such relationships are generally characterised by a mutual understanding of processing and controls to ensure that decisions are fair and accountable. What actions can be taken depends on a ccTLD's national policy framework and the legal and accountability issues around notifications by third parties.

The next paragraphs address some of the risks and issues linked to blocking or deleting domain names.

Blocking or deleting a domain name may make it more difficult to find illegal content on the internet but does not solve the issue or the crime, as the content remains available for those who want to find it. On top of this, there are a number of risks and drawbacks. These are discussed below.

Doubtable efficacy and false feeling of security, as the content remains available.

Blocking or deleting a domain name does not remove illegal content from the internet. The content remains available and can be directly accessed by using the IP address instead of the domain name. How this is done is not rocket science, and a simple web search returns ample explanations and videos explaining how to access a site by its IP address. Deleting the domain name will reduce the chance that users are accidentally confronted with illegal content, but will not stop those actively looking for that type of content. "Due to the internet's architecture, blocking by domain name can be easily bypassed by end users and is thus likely to be largely ineffective in the long term and fraught with unanticipated consequences in the near term".[16]

Moreover, providers of illegal content can anticipate blocking and can take precautionary measures to further reduce the effect of the measure. A content provider, for example, might register multiple domain names under the same TLD or under different TLDs in different jurisdictions and let them all resolve to the same IP address, and thus the same content. Hyperlinks used in emails or placed on platforms or websites might directly link to the IP address, without using the DNS.

---

15 Regulation (EU) 2017/2394 of 12 December 2017, entering into force 17 Jan 2020. Art.9, 4, (g), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R2394&from=EN

16 'SAC 056 - SSAC Advisory on Impacts of Content Blocking via the Domain Name System', SSAC, 9 October 2012.

Risk of massive overblocking and collateral damage

When a domain name is deleted or blocked this affects all the content that is reachable under the domain name and subdomains, including the envisaged illegal content but also all other content. Deleting the domain name of a social network or blog site where individual users can post their own content or create their personal blog will impact all users; not only those who posted illegal content but also all those who posted their family pictures, expressed a political opinion, businesses that use the site for promotion and e-commerce, etc. When blocking a domain name, all services linked to the domain name, for example email, immediately stop working.

In a fictive case study in 'Domain Conflicts in the Legal System', the Norwegian registry describes the impact and consequences of the blocking of the University of Oslo's domain name, after a student posted illegal content on a webpage under the university's domain.[17]

Risk of over-enforcement and easy to make mistakes

The technical ease with which domain names can be blocked raises the risk of over enforcement.[18] Error costs are low on the side of the enforcer, but by contrast might have a dramatic impact on the side of the domain holder who sees his domain erroneously blocked,[19] for example a business which has its e-commerce site blocked or an institution that can no longer be reached via email.

> Note: there are other forms of blocking or intervening in the DNS, for example at ISP or registrar level. Most of them come with similar caveats and can be circumvented. No blocking measure is a comprehensive solution as none of them removes the content.

17 See 'Domain Conflicts in the Legal System', Norid, September 2017, https://www.norid.no/en/om-domenenavn/veiledere/domenekonflikter-i-rettssystemet/

18 'Notice and Takedown in the Domain Name System: ICANN's Ambivalent Drift into Online Content Regulation: (pp. 1379 - 1383)

19 An example is described in the following blog post: "Main French Internet Provider Orange blocks traffic to Google', Alix Guillard, 27.10.2016, https://en.blog.nic.cz/2016/10/27/french-orange-blocks-traffic-to-google/

Current ccTLD practices

As mentioned earlier, local legal frameworks define what content is illegal, who has been given the authority to deal with it and what processes are permissible within the rule of law. This may vary from country to country. Furthermore, ccTLD registries have different requirements regarding who can register domain names and what their duties are. The combination of these requirements and the local legal framework influences what policies and initiatives the registry develops to approach the issue of illegal online content.

Typically these policies are rooted in the local community, are compatible with local laws and address local needs, and often have been developed in consultation and cooperation with other local stakeholders. Successful policies and practices for one ccTLD could inspire others. However, due to the local roots and particularities, there is no guarantee that copying a project or policy will lead to the same positive result, or indeed be legal within another ccTLD.

Education and awareness-raising, with special attention for an open dialogue and cooperation with authorities and LEA

There are different kinds of risks and dangers that users face when going online (technical, privacy, etc.), and recognising and dealing with illegal content is one of them. Several ccTLD registries see it as their duty to warn their community about the dangers of the internet. They educate and provide guidance on how users can better protect themselves, how to mitigate risks or to resolve issues.

Community-wide education and awareness-raising

ccTLD registries are engaged in awareness-raising towards and education of their local internet communities to make the internet a safer place. Registries take initiatives to warn and educate domain holders and the wider local community of users about unwanted content, and to provide guidance on how to react. There are a variety of ways in which registries inform their communities, for example by organising meetings or participating in workshops, giving presentations, discussing illegal content in their publications, etc.

Many registry websites contain a page or section on illegal content. It describes potential issues and dangers, explains the registry policy, clarifies the role of the registry and what it (technically) can and cannot do in case of illegal content.

The registry will guide any user who wants to complain about potentially illegal online content towards organisations and government agencies that are specialised in assessing and dealing with specific types of online content (for example illegal gambling, child sexual abuse material, counterfeit goods, etc.).

Examples

Nic.at (.at): the Austrian registry website provides advice for internet users on how to deal with illegal activities on the internet as well as links to Stopline, the national reporting office against child sexual abuse material and national socialism on the internet. See here and here.

Nominet (.uk): the British registry has published a policy paper on criminal practices to explain how the registry tackles criminal activity and which provides links to a number of UK-based authorities that may be able to help. Instead of removing domain names from the zone file, Nominet redirects internet users to an educational landing page. See here.

Afnic (.fr): The French registry provides a link to the dedicated reporting platform of the Ministry of Internal Affairs where "website content, or conduct that illicit or contrary public law and order" can be reported. Afnic's website also contains a form that users can fill in to notify the registry of unlawful domain names.

Norid (.no): the Norwegian registry website provides a link to the police website with tips on how to inform the police of illegal activity online, as well as to the slettmeg.no service, which gives advice on how to remove information from the internet.

DNS.PT (.pt): the Portuguese registry, in cooperation with other organisations dealing with the unauthorised dissemination of copyright-protected content, has developed and hosts a portal website that provides fast and easy access to websites that offer digital content which respects the intellectual property rights of authors and creators. DNS.PT also publishes a quarterly magazine dedicated exclusively to cybersecurity in order to raise awareness on online threats.

SWITCH (.ch): the Swiss registry supports the internet community through security awareness platforms and offering services to educate and train users' security skills. See here.

Registries will sometimes use their communication channels to warn against criminals using fake websites, for example to obtain a user's credentials for banking or e-commerce, and demonstrate how users can verify the legitimacy of a website. Usually the fake website will be registered under a more exotic TLD of a foreign country, and the registry itself has no access or influence on the domain name used.

SIDN's (.nl) tips to recognise fake webshops.

Norid's (.no) advice to identify email scams.

TRAFICOM's (.fi) website entitled "scammers disciplined - project", which proposes packages to identify and recognise digital scams.

Education and close collaboration with authorities and LEAs

Many registries put a special focus on raising awareness and establishing good relations with law enforcement and other authorities (such as consumer protection agencies or gaming commissions). It is important that these agencies and authorities, who in many cases have the

authority to assess the legality of the content, understand what a registry does, what it can do to help them in cases of illegal content, and to establish good communication channels. This will avoid important time from being wasted when they ask the registry to take actions that are not within the registry's capability, or do not address their requests to the person or service that can adequately react. Law enforcement plays an important role in the fight against illegal online content and should, in most cases, be considered as a first contact point for complaints.

It is important that the people working in LEAs and relevant authorities have a good understanding of how the internet and the DNS works, including of the role of the registry and the possibilities and limitations of action at registry level. Some registries also develop guidelines or procedures for smooth and quick communication between specified agencies or authorities and the registry.

Examples

Norid (.no) is the author of an informative guide for law enforcement, police and people working in the judicial system - 'Domain conflicts in the legal system'. The registry has also, in collaboration with the prosecuting authority, developed specific guidelines for how law enforcement should proceed when seizing a domain name registration. See here and here.

CZ.NIC (.cz) has signed a Memorandum of Cooperation with the Czech Department of Special Activities of the Criminal Police and Investigation Service. The Memorandum aims to increase collaboration between CZ.NIC and law enforcement authorities regarding the prevention and tracing of criminal activities and the prosecution of crimes whilst reducing administrative burdens. CZ.NIC also made a Joint Declaration with the National Headquarters for Combating Organised Crime's Police and Investigation Service to better tackle online child sexual abuse material, and recently signed a Memorandum of Cooperation with the Czech Trade Inspection Authority to facilitate the detection of risky e-shops.

SWITCH (.ch): In cases of criminal or administrative proceedings, authorities may approach the registry with requests to revoke or block domain names. In collaboration with the regulator, the registry has developed guidelines for how an authority should proceed in such cases and what scope for action is available to SWITCH when responding to instructions from authorities.

Nominet (.uk), in consultation with its local internet community, has evolved a process of collaboration with UK law enforcement agencies. Under this process, UK LEAs can present Nominet with formal certificates of criminal use or content in relation to .uk domains which will lead to their suspension within 48 hours following notice to the domain registrant and registrar. A criminality report is published annually.

The Irish registry (.ie) is working on the implementation of a cooperative arrangement with the local police authority.

DK Hostmaster's (.dk) policy enables the registry to release data about registrants to a range of authorities, which include police and prosecuting authorities, the Ministry of Culture, the Complaints Board for Domain Names, tax authorities and the data inspectorate. See here.

Registries as providers of authoritative domain name data

As mentioned before, the only effective solution to illegal content is to remove the content from the internet. If a user or organisation discovers illegal content on a website, one of the first actions is to contact the domain holder who can remove or adapt the content.

A registry collects data because it needs to be able to identify who the domain holder (their customer) is, and to be able to contact the holder in case of a dispute, technical problems, changes to the Terms and Conditions, missing payments, etc. A registry's Terms and Conditions usually explicitly require the domain holder to provide correct data and contact details upon registration and keep this information up-to-date. Providing false or incorrect data is a violation of the Terms and Conditions and can lead to the deletion of a domain name.

Registries put a lot of time and effort into the maintenance of the database. This not only improves the quality of the registration WHOIS data, but also may have an indirectly positive impact, as it is unlikely that those with bad intentions would register a domain name using their correct personal information. The actions and practices to maintain a high-quality database depend on factors specific to the registry, such as local legislation, size of the registry, the amount of registrations processed, etc., and could consist of:[20]

- High level screening of the data provided upon registration, to filter out obviously-false entries (for example, registrants called 'Mickey Mouse);
- Automated format checks of provided data (for example, email address, phone number);
- Check of legal documentation provided by the registrant, in countries where such a legal documentation requirement exists;
- Random verification of registration data of already-registered domain names (for example, the registry randomly selects and verifies a number of domains per day, month or year);
- Verification of the data in case of a complaint;
- Cross-checks of provided data with official databases (for example, valid postal code, existing phone number, company/organisation number or national identification number if such information is required upon registration).

It is important to note that many ccTLD registries have no direct contact with the registrant of a domain name. Where this is the case, all contact, including providing and updating the registration data, goes via the registrar.

Examples of registry efforts to obtain and maintain correct registration data:

Norid (.no) requires all domain holders to be either registered in the Norwegian Central Coordinating Register for Legal Entities or in the National Population Register for individuals. The .no registry operator regularly checks that the legal entities that holds domain names still exist, according to the Central Coordinating Register for Legal Entities. Domains held by legal entities that have been disbanded are automatically slated for removal.

20 These examples are based on a 2017 CENTR members' survey.

DK Hostmaster (.dk) requires Danish domain registrants to identify themselves using MitID, a login-solution used by Danish banks, government websites and other private companies. Foreign registrants are subject to a risk assessment, which will determine whether they receive a request to provide proof of identity before registration - high risk - or within 30 days after registration - low risk- (no risk customers are not requested to provide proof). If the domain holder cannot or does not provide proof of its identity, the domain name is suspended. DK Hostmaster has also introduced a contact form enabling users to report incorrect registrant data, following which the registry is under a legal obligation to further examine the case in order to ensure accurate data. See here and here.

SIDN (.nl) considers fake webshops to be harmful to .nl's reputation as a strong and secure top-level domain. It has deployed an early detection system of domains used for fake webshops and looks into reports from victims of scams and information received from the National internet Fraud Report Desk. If the registration data of the domain names involved is fake, the registry is able to deactivate them.

SWITCH (.ch): The registration of a .ch domain name does not require verification of the identity of the registrant. However, if there is reason to believe that the registrant (a) is providing false identification data or is unlawfully using the identity of a third party and (b) will use the requested domain name for an unlawful purpose or in an unlawful manner, the .ch registry may not activate a domain name until the verification of the registrant's identity. This new instrument is provided for in the Ordinance on Internet Domains and is based on the obligation of domain name registrants to identify themselves correctly. If a registrant fails to identify themself correctly within a 30-day period, the domain name is revoked. See here.

Some registries have special procedures in place to report or complain about false registration data.

Nominet (.uk): complaints about incorrect WHOIS data.

Afnic (.fr): verification request registrant information, which leads to the blocking of domain names within 7 days.

DNSBelgium (.be): Revoke/Revoke+

Sharing registration data with third parties

Registries have to respect local privacy regulations when sharing information about domain holders with third parties. The policy and procedure for obtaining contact information can be found on the registry website. There are different practices, some registries request the information manually via an online form, other registries provide a (limited after the GDPR) access to the registration database (via the WHOIS protocol), and yet other registries have built a tool that allows to send a message directly to the registrant.

Examples

Afnic (.fr) has a form to request the disclosure of the personal data of a private individual who has a domain name and provides an interface which allows the third party to send a message to the registrant without knowing their email address.

DomReg (.lt) provides a form which enables users to contact domain name registrants.

Norid (.no) offers a limited domain lookup where the public can find the email address of a registrant and can find additional information about who the registrant is, if it is a legal person. See here.

DENIC (.de) supports both a general request and an abuse contact per domain for email contact to either the registrant or the responsible registrar without a need to share the registrant's data. In addition, DENIC offers various forms for law enforcement agencies and bearers of legitimate interest to guide efficient submission of supporting documents for data disclosure in full compliance with the GDPR.

Responding to reports of suspicious content

Responding to external reports

Some registries have established procedures to respond to reports of suspicious content by blocking or suspending a domain name in specific cases. These procedures usually have in common that they are applicable to limited and well-defined cases, and that an external party with expertise in assessing that type of content is involved.

Such a procedure can be useful where a court decision to revoke a domain name takes a considerable amount of time. One of the dangers is that complainants do not realise the limited impact of the measure taken by the registry and no longer pursue action to remove the content from the internet.

Examples

SIDN (.nl) established a voluntary Notice-and-Take-Down procedure based upon the Dutch national code of conduct. The Notice-and-Take-Down-procedure can only be invoked if the complainant can prove that sufficient steps were taken to approach the content provider, the website manager, the registrant and registrar of the domain name, for the obvious reason that it is within the reach of those parties to effectively solve the problem and remove the content. Only in unmistakable illegal cases SIDN may decide to (temporarily) remove the nameservers for a domain.

SWITCH (.ch): The Ordinance on Internet Domains (OID) provides for the blocking of a domain name if there is reason to believe that the domain name in question is being used to (a) access critical data by illegal methods (b) distribute or use malicious software; or (c) support one of the aforementioned acts. If the criteria of the OID are met, bodies recognised by the Federal Office of Communication (OFCOM) may request the suspension of the domain name for a limited period of 30 days. If no further measures are taken after 30 days, the suspension must be lifted. See here.

DNS Belgium (.be) has put in place a Notice and Action procedure in collaboration with the FPS Economy. This entails that following reports of serious infringements from the FPS Economy, DNS Belgium makes the relevant .be domains inaccessible by overriding nameservers and redirecting users to a warning page. If the domain name holders cannot prove that they are bona fide, the domain names are removed. See here and here.

EURid (.eu, .ею, .ευ) collaborates with various organisations and institutions which aim to fight against cybercrime (product counterfeiting, piracy, phishing, etc.). These collaborations help clear EURid's registration database from fraudulent domain names and to establish a more secure domain space for internet users.

TRAFICOM (.fi): article 172 of the Act on Electronic Communication Services provides TRAFICOM with the right to undertake the necessary measures in order to detect, prevent, investigate and commit to pre-trial investigations of any significant information security violations aimed at public communications networks or services using .fi code domain names or their holders. The necessary measures may be actions targeted at .fi root name server data and may include the following: 1) prevent and restrict traffic to the domain name; 2) reroute traffic to the domain name to another domain name address; and 3) any other comparable technical measures in the meaning of subsections 1–2. The registry can remove a domain if the domain name holder's information is not correct, up-to-date and identifying, and the domain name holder has not, regardless of a request, corrected or complemented the data, a court of law has prohibited the use of domain or if the Finnish Competition and Consumer Authority or Market Surveillance Authorities have taken a decision to remove the domain.

Detecting illegal activity with additional measures

To support increased consumer protection and safety online, some regsitries have developed tools and/or automated processes to help identify illegal activity or abuse online. These practices range from regular scans of domain names to identify fraud, to technical algorithms aimed at detecting phishing attempts.

Examples

SIDN Labs (.nl) has developed DMAP, a crawler which scans all .nl domains, amongst others, for characteristics associated with fraud each month in order to identify illegal activity (e.g. fake webshops). See here and here.

EURid (.eu, .ею, .ευ) has developed an abuse prevention mechanism called APEWS which predicts malicious registrations, i.e. whether a domain name could potentially be used for abusive purposes. If APEWS finds that a registered domain name could be related to abuse, it will delay its delegation to the .eu zone file. EURid will then review these domain names and potentially ask the holders to confirm their registration data before deciding whether the domain name should be delegated to the .eu zone file or suspended. See here.

Nominet (.uk) has developed an anti-phishing systems entitled Domain Watch that identifies and suspends domains which make phishing attempts through technical algorithms and manual intervention. If a domain is suspended, registrars and registrants are informed via email. The domain is then unsuspended if the registrant is able to confirm the legitimate use of the domain name.

Conclusion

Abusive and illegal content decreases trust and confidence in the internet. Local legal frameworks define what content is illegal, and who has the authority to deal with it within the rule of law. This may vary from country to country.

Removing illegal content from the internet is the only effective solution that avoids it being accessed and consumed. The content publisher and the hosting provider have direct access to the content or the device that stores the content. ccTLD registries have no access to content and neither do they host or transfer content through their infrastructure.

ccTLD registries are committed to contributing to a comprehensive and effective approach against illegal online content, and will develop policies and initiatives, for example:

- to raise awareness and educate their communities on the dangers of the internet;
- facilitate cooperation with LEAs and authorities;
- provide registration data on suspicious domain names;
- respond to reports of domain names used to facilitate access to suspicious content, within the framework of their local jurisdiction;
- or help detect illegal activity with additional measures.

The successful policies and practices showcased in the paper could inspire other ccTLDs. However, due to the local roots and particularities, there is no guarantee that copying a project or policy will lead to the same positive result, or indeed be legal within another ccTLD.

Council of European National
Top-Level Domain Registries

About CENTR

CENTR is the association of European country code top-level domain (ccTLD) registries, such as .de for Germany or .si for Slovenia. CENTR currently counts 52 full and 9 associate members – together, they are responsible for over 80% of all registered domain names worldwide.

The objectives of CENTR are to promote and participate in the development of high standards and best practices among ccTLD registries.

Full membership is open to organisations, corporate bodies or individuals that operate a country code top level domain registry.

CONTACT

CENTR VZW/ASBL
Belliardstraat 20
1040 Brussels, Belgium
0885.419.166 | RPR Brussels

+32 2 627 5550

secretariat@centr.org

www.centr.org

FOLLOW US

To keep up-to-date with CENTR activities and reports, follow us on Twitter, Facebook or LinkedIn

Publication date: 13 May 2022