Governmental Censorship on Internet: Spanish vs. Catalans Case Study

Prof. Manel Medina – esCERT-inLab-UPC – medina@escert.upc.edu

Biography of the author: Prof. Dr. Manel Medina is a Full Professor and Director of MsC Cybersecurity Management, Blockchain and Cyber-intelligence at the Politecnic University of Catalunya (UPC).

ABSTRACT

This article summarises the actions taken by the Spanish government pretending to censor information published and applications developed by the Catalan government and some independent activists in order to organize an independence referendum. It describes the goals, the technical approaches and some countermeasures, analysing also the level of success achieved. There is also an introduction to the legislation being deployed in the European Union and Spain, that could give support to some kind of Internet censorship and the concerns about the compliance of those regulations with the civil rights of freedom and opinion, that should be guaranteed by governments to citizens. The conclusions suggest some ideas to prevent arbitrary application of censorship practices by national authorities using criteria not widely accepted by the Internet community.

1. INTRODUCTION: GLOBAL SITUATION

Internet governmental censorship is accepted by more than 4/5 of the population, but preserving freedom of expression, which is not always guaranteed. According to the 2018 report from Freedom House, 17 countries have legislation restricting online media in the name of fight against fake news (Shahbaz 2018). This report measures the level of Internet freedom and identifies the evolution of that freedom in that year, categorising the countries according whether that freedom is stable, improves or declines. As we can see, China is in the top of censorship, it was getting worst then and still now, since the recent news show how citizens' behaviour is under control, with the aim of fighting against coronavirus SARS-CoV-2 is being fight there, with impact not only on the behaviour of users in the network, but also in the real life. No too far from Chine we have many Muslim countries, Russia and former Soviet republics, and other Southeast Asia governments mainly, most of them with a declining censorship trend. Internet shutdowns reported to rise from 75 in 2017 to 196 in 2018, some of them affecting only specific services. Here are some recent facts (*The Guardian* 2020):

- Internet was shut down in Kashmir in mid-December 2019, amongst others (e.g. Delhi, Assam, Meghalaya), and it is considered the longest ever imposed in a democracy (Masih, Irfan and Slater 2019), more than 137 days. The shutdown started in August when authorities revoked Kashmir's autonomy and all communications were snapped. Mobile phones voice calls were restored, but

Internet was still blocked 4 months after for more than 7 million people with some collateral damages, like disappearing from WhatsApp after automatic deletion due to 120 days of inactivity. Journalists had just 10 computers to share in a government-run centre. The Kashmir Chamber of Commerce estimates 1,4 billion USD in losses, mostly due to paralysation of online business.

- 20-day shutdown in Democratic Republic of Congo.
- Benin, Togo, Gambia, Sudan, Zimbabwe and Iraq also cut off following some protests, to prevent bidirectional circulation of news.
- China has set up a kind of intranet with its own IP addressing space, requiring most of the citizens and enterprises to do Network Address Translation (NAT) through a big firewall-like gatewaying infrastructure, that filters and scans everything getting in or out of the country. The barrier to block external services is called the Great Cannon, a tool for DDoS attacks. People used VPN to avoid that control and censorship of foreign journal websites, applications like Facebook or Google, etc., until the government banned that kind of tunnelling protocol to undercome the barrier. The excuse is the preservation of national security and stability of the political system and also to redirect their own citizens towards local providers.
- Iran, Russia, and up to 36 countries' representatives have attended trainings in China to learn how to implement their Internet filtering tools and registered exchange points (the gateways used by the internet packets to get in/out of the country).

In addition to those extraordinary cases, there are other more traditional ones (Valdés Cortés 2000):

- Singapore and Myanmar have gatewaying controls in the international internet connections, but maybe not as much over-filtering as China, since they are blocking just some particular platforms.
- Turkey and Spain have reports of people being punished for publishing offensive statements or songs (respectively) on social networks.
- The United Kingdom and Spain have regulations that may require an ISP to facilitate the interception of communications by the police, eventually through the intervention of ISPs themselves if the collaboration is not consider adequate.
- Australia, Chile and the European Union countries are also considering the approval of new regulations for that kind of monitoring and censoring with more limited or similar scope.

As a general statement, we can say that government censorship is always intended to address hybrid threats, i.e. attacks that have impact on both the Internet and real world. The censorship actions are also applied not only blocking the Internet information flow, but also in some cases this blocking is forced by police agents on the ISP's and other actors' premises.

Moreover, Wikipedia has a couple of interesting summaries of Internet censorship, describing technical approaches (Wikipedia 2020) and the worldwide situation (Wikipedia 2019), summarised in this map.

2. CURRENT REGULATIONS

Currently there are two regulations applying to this case: one from the European Union (EU) to prevent the dissemination of terrorist information, in phase of agreement between the EU Parliament and the European Commission (EC); and another one with a wider scope, already approved by the Spanish Government.

Those regulations are intended to address mainly terrorist and sexual abuse cases. Europol has reported. In the 2019 annual report they issued, they reported that their Internet Referral Unit (IRU) had participated in 222 operations, delivering 339 reference sites with 87,819 pieces of content, which trigged 85,477 decisions of referral, resulting in the removal of 84,85% since mid-2015 (*Europol* 2019).

2.1 European Union Regulation (Draft) Preventing Dissemination of Terrorist Content Online

In September 2018, the European Commission (EC) presented a draft Regulation on preventing the dissemination of terrorist content online (*European Commission* 2018; Robinson 2018; *European Parliament* 2018) It is based on a communication of 2017 giving guidelines and principles on prevention, detection and removal of illegal content online (Cory 2016 and 2018), including child pornography, hatred, violence and terrorist propaganda which was aimed to encourage voluntary application of those guidelines by the relevant actors in Internet and hosting service providers. In the forthcoming recommendation adopted by the EC in March 2018, they included a set of non-binding operational measures to be taken by Host Service Providers (HSP) (defined as "*a provider of information society services consisting in the storage of information provided by and at the request of the content provider and in making the information stored available to third parties*") and member states (MS) to manage that illegal online content. It defines illegal content as "*any information which is not compliant with EU or Member States law*", and this may lead us to the scenario that will be discussed later, where some information may be illegal in one MS and legal in others, due to different regulatory criteria. The recommendation also includes a list of measures aimed at reducing the spread of online terrorist propaganda, notably forbidding its hosting and the obligation to remove it within one hour after having received the requirement by law enforcement authorities and Europol. In order to achieve this very short-term requirement, the HSPs are encouraged to implement some automatic analysis of the content they are hosting in order to detect potentially illegal content. In line with this idea, the Europol's Internet Referral Unit (IRU) has developed tools to actively scan the Internet for terrorist content and refer it to hosting platforms. The EU reports that "*over 50,000 decisions for referrals across over 80 platforms in more than 10 languages have been made since 2015*".

The EC launched one initiative to refine the guidelines to voluntarily restrict the distribution of illegal content on Internet: the cross-sectorial EU Internet Forum, bringing together the Internet industry and governments of member states. Moreover, Europol created the Internet Referral Unit (IRU), the Radicalisation Awareness Network and the European Strategic Communications Network in order to stop the spread of terrorist content online. Some member states have ongoing national legislative initiatives (like Spain being described later) which go a step further, already imposing obligations and stating considerable fines for non-compliant providers

In order to support this draft, the EC launched a survey from April to June 2018, and the results were that:

- ISPs and HSPs (Internet and Hosting service providers) claimed for voluntary recommendations and found themselves ready to collaborate with law enforcement authorities (LEAs);
- Citizens felt safe enough with the current situation on the Internet;
- Civil associations warmed to the need to set up measures to focus censorship practices; and
- Civil rights-protecting organizations were concerned about their preservation, mainly freedom of opinion and ideas;
- Property rights defence organizations strongly supported the enforcement of responsibility of ISP to block the distribution of contents subject to copyright or licensing.

In this scenario, EC decided to go ahead with the regulation, with the following provisions:

- 1 hour rule: Content appointed as illegal by a national competent authority must be removed from public access within 1 hour after the reception of the removal order. The fulfilment of this rule will require the service providers to set up a 24/7 contact point.
- A definition of terrorist content as anyone that "*incites or solicits the commission or contribution to the commission of terrorist offences, provides instructions for the commission of such offences or solicits the participation in activities of a terrorist group and guides on how to produce and use explosives, firearms and other weapons for terrorist purposes*";
- The commitment of all platforms to ensure they are not misused for the dissemination of terrorist content. Service providers might be required to take proactive measures to better protect their platforms against illegal use from third parties (black hat hackers, i.e. not their customers) for terrorist abuse and set up mechanisms to actively scan the content on their servers for early detection and warning about potentially terrorist or abusive content. Those actions should be *"appropriate, reasonable and proportionate*". HSPs following "*a systematic failure to comply with removal orders*", thus breaching the obligations stated in the draft regulation, risk incurring penalties, with a financial value of up to 4% of the HSP's latest yearly global turnover.
- A framework for strengthened cooperation between HSPs, member states and Europol must be created, given the difficulty to define the correct filtering of terrorist or abusive information that will be both compliant with the Europol requirements and the civil rights of the citizens and civil organizations in general. This includes the programming and configuration of automated (Artificial Intelligence) tools and the corresponding benchmarks for testing and validation mechanisms to guarantee its transparency, safeguards for civil rights and prevention of the existence of bias on those automatic search and decision algorithms and tools. They consider the possibility of creating a "hash database" of malicious content to ease the detection of replication or further uploads of

censored materials. Failure of the expected performance could lead also to sanctions to the HSP.

Where content has been removed unjustifiably, the service provider will be required to reinstate it as soon as possible. Effective judicial remedies will also be provided by national authorities and platforms and content providers will have the right to challenge a removal order. For platforms making use of automated detection tools, human oversight and verification should be in place to prevent erroneous removals based on detailed assessment of relevant context factors that may have impact on the consideration of terrorist content. Transparency and accountability will be guaranteed by annual transparency reports.

Removal orders sent to HSPs shall contain inter alia, a statement of reasons explaining why the content is considered terrorist content with reference to the definitions used in the draft regulation, information enabling the identification of the content referred (typically a URL), and information about redress available to both the HSP and to the content provider. Thus, the provider can only decide whether to remove the relevant content or to block access thereto.

A number of organisations have complained about this draft regulation, and here are some of them:

- On 7 December 2018, three independent experts of the United Nations Human Rights Council expressed concerns about the proposal.
- On February 2019 the EU Fundamental Rights Agency (FRA) stated the key fundamental rights implications of the proposal.
    - FRA considers that the definition of terrorist content has to be modified as it broadens the terms of the directive on combating terrorism (2017/541). The definition of the content is considered too wide by FRA and would interfere with freedom of expression and information.
    - According to FRA, the proposal does not guarantee any type of involvement by the judiciary.
    - Online providers have to receive sufficient information.
    - FRA considers that the member states' obligation to protect fundamental rights online has to be strengthened, as well as due diligence.
- The EU Parliament itself has launched the question about the compliance of the proposal with the existing legislation on electronic commerce and on audiovisual media services.
- It is worth noting the concerns voiced by David Kaye, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, a few weeks before publication of the draft regulation. In his report (UN General Assembly 2018), Kaye makes specific reference to the application of artificial intelligence (AI) tools to online content and states:

> *"Even when algorithmic content moderation is complemented by human review – an arrangement that large social media platforms argue is increasingly infeasible on the scale at which they operate – a tendency to defer to machine-made decisions (...) impedes interrogation of content moderation outcomes, especially when the system's technical design occludes that kind of transparency.*"

2.2 Spanish regulation to stop ISP, Telecom Operators and Social Networks

In order to support the censorship actions described later, the Spanish Parliament, approved the regulation Real Decreto-ley 14/2019 (Oct. 3st), stating the following aim "*adopting urgent measures following public safety reasons in digital administration, procurement in the public sector and telecommunications*". This regulation allows the government to take *exceptional and transitory* agreements to assign direct management and shut down of telecommunication services and networks in some exceptional assumptions that may affect public order, public safety and national security. It will be possible to apply those censorship actions in the whole or part of the territory without a Court mandate, alleging public order needs.

According to the Ministry of Economy, this law was conceived to counterfeit cyber-threats against critical infrastructures, espionage, activities of disinformation and fake news in electoral processes, and other cyberthreats like mobile phone hacking or personal data breaches.

Many organizations in Spain have complained about this legal decree because its relevance in the freedom and public services would have required longer debates involving all kinds of stakeholders in society to reach a consensus on the conditions of applicability of those measures that could leave a wide sector of the population without Internet and mobile phone services, without means to discriminate criminals from normal citizens or enterprises. This regulation allows the government (not a judge) to shut down Internet access, social networks and other communication services like websites, communication media channels, etc. in a censorship scenario much wider than the one foreseen in the EU regulation, that has already been widely criticised by the international Internet community. The complaints about the Spanish regulation state that it goes against the Spanish Constitution and the fundamental rights of all its citizens, because there are no means to control the exact number of citizens that could be left without communication.

3. REPORTED GOVERNMENTAL CENSORSHIP ACTIONS

The Catalan government organized a self-determination referendum to be held on October 1st of 2017 without authorization from the Spanish government. For this reason, the Spanish government launched a number of actions aimed to stop the spread of information about this referendum and to kidnap the applications that would support this democratic act.

The Electronic Frontier Foundation (EFF) is the leading international non-profit organization on the Internet. Created in the United States in 1990, it is globally recognized for positioning in many conflicts over the defence of digital rights, user privacy, and freedom of expression. EFF, amongst many other complainants in this sense, says the measures taken by the Spanish government are prohibited by the Universal Declaration of Human Rights. There is a common recognition that the censorship on the Catalan Internet has been disproportionate and in the following sections there are some details of the actions taken to censor those Internet sites and services by the Spanish government.

3.1 Websites

As a consequence of the court requirements promoted by the former Spanish government, many of the more than 140 censored domains and Internet services were blocked during months.

It began with the seizure of the referendum.cat domain, the official referendum website, on September 13 by the Guardia Civil (Spanish military police), pursuant to a warrant issued by the Supreme Court of Catalonia. Over the ensuring days this order was soon extended to a number of other and unofficial mirrors of that website, such as ref1oct.cat and ref1oct.eu, which were seized if they were registered as a .cat domain and blocked by ISPs if they were belonging to a different TLD (Top Level Domain). The fact that Spanish ISPs had already blocked websites such as Pirate Bay under court order, many years ago, enabled the blocking of additional websites to be rolled out swiftly due to the previous court resolution that created jurisprudence in Spain.

A few days after, one of these subsequent censorship orders was especially notable because it empowered the Guardia Civil to block not only a list of named websites, but also any future sites with content related to the referendum, publicized on any social network by a member of the Catalonian government. This order accelerated the blocking of further websites without any further court order. These apparently included the censorship of non-partisan citizen collectives, such as empaperem.cat and other non-profit organizations.

Facing those facts, clearly against the EU draft regulation, the Catalan government denounced the abuses and censorship in relation to Internet access committed by Spanish authorities, with the seizing or blocking of more than 200 web pages related to the self-determination referendum on Catalonia (*Generalitat de Catalunya* 2017):

> *"During the last days, the basic human rights of freedom of speech and freedom of press have been suspended in Catalonia. A part from censorship in media, following the Spanish Government instructions, a judge has ordered to shut down a number of web sites (e.g. referendum.cat, ref1oct.cat and garanties.cat) created by the Catalan Government to inform about the self-determination referendum we are going to celebrate on October the 1st and ordered the main telecom companies (Telefónica and Vodafone) providing access to Internet, to block the access of their users to mirrors of those sites hosted abroad (e.g. ref1oct.eu, among many others).*
> *Things are worsening with a number of officials of the Catalan Government and directors from a number of public and private agencies arrested. Among them, one member of our Chapter that is working at the registrar of the .cat TLD, Fundació puntCAT.*
> *A part from the serious political consequences of this critical situation, we express our serious concerns about the violation of ISOC principles for no censorship and open access to the Internet."*

The complaint was addressed to the Vice President of the EC and Commissioner in digital matters, Andrus Ansip, highlighting articles 3 (3) of Regulation EU 2015/2120 of the European Parliament and of the Council, dated November 25, 2015, and Directive 2002/21/EC, dated March 7, 2012, which regulate open Internet access. The Generalitat (Catalan government) emphasized that the Spanish government, the Prosecutor's Office and the Spanish law enforcement authority (Civil Guard and

National Police) have violated those EU regulations with their actions against the PuntCAT Foundation (.cat TLD Registry) and the order and requirement to suspend access to any page with domain .cat related to the referendum.

The Spanish authorities also issued an order sent to telecommunications operators to block access to these pages, as well as any domains that are published or published on the social networks of members of the government. This order and its associated requirement were strongly refused by ISOC (Internet SOCiety: worldwide association of internet users with regional chapters) in a press release issued by its Regional Bureau Director for Europe, Frédéric Donck (Donck 2017):

"Measures restricting free and open access to the Internet have been reported in Catalonia. There have been reports that major telecom operators have been asked to monitor and block traffic to political websites, and following a court order, law enforcement has raided the offices of the .CAT registry in Barcelona, examining a computer and arresting staff.

We are concerned by reports that this court order would require a top-level domain (TLD) operator such as .CAT to begin to block "all domains that may contain any kind of information about the referendum". We do not see it as the expertise and mandate of TLD operators within the Internet's ecosystem to engage in monitoring and blocking of content outside of receiving judicial requests related to specific domains.

The Internet Society promotes the open development, evolution, and use of the Internet for the benefit of all people throughout the world. As such, we believe actions that impede the ability of any local community to use the Internet freely are unacceptable. The court's ruling vis-à-vis .CAT has a disproportionate chilling effect on free expression, and an unjust impact on the ability of Catalan-speaking persons to create, share, and access content on the Internet.

We are concerned that network blocking practices are multiplying as a way for countries to police online content around the globe.

Shutdowns should not become 'the new normal'. In an Internet Society paper released on this issue earlier this year [English, French and Spanish versions], we stressed that network blocking measures are generally ineffective, and tend to create collateral damage, including the overblocking of lawful content and expression. We have joined with over 130 human rights organizations and over 50,000 concerned citizens across the world to urge government to Keep the Internet On.

We hope to see a return to free and unfiltered Internet in Catalonia in the near future and call on all parties to commit to upholding freedom of expression and dialogue in this challenging time."

3.2 Using DNS to censor websites registered in the .cat TLD

EFF and Public Knowledge released a white paper titled "Which Internet Registries Offer the Best Protection for Domain Owners?" (Jeremy Malcolm, 2017b). In that paper they describe that ICANN (EFF, n.d.) has a policy and a working group aimed to request TLD registries to close domain registrations that may be attempting action against trademark or copyright registered by other organisations. This policy group has very good control of the traditional TLDs (.com, .org, .net, etc.) but they are not so active in the country code TLD or even less on the newly defined TLDs (.info, .education, etc.). In this scenario, in practice, only the registries are responsible for closing a registered domain site, based on the above-mentioned criteria foreseen in the EU draft regulation, such as registered trademark or copyright protection, but also on malicious practices, like malware distribution, scam, phishing (requested by APWG (APWG 2019) to ICANN (Trendacosta, Harmon and Gagliano. 2020), or illegal or terrorist content distribution.

Coming back to the Catalan case, following the attempts to block the referendum information and voting service sites, the owners of those sites were creating alternative sites on HSPs in different ISPs, outside of the country, that were out of the jurisdiction of the Spanish authorities. The URLs were also registered in different TLD under control of organizations legally bound to other countries. In many cases also, the officers involved in the referendum votes collection used direct IP addresses to access the replicated service providers, due to the manipulation of the URL resolution tables made by the telecom operators in the DNS servers offered as default ones to their Spanish customers, making the domains unreachable for them.

The .cat top-level domain was one of the preferred domains to be used for the registration of the domains used in the advising of the referendum and its practical implementation because it was one of the top-level domains approved by ICANN in 2004 for the promotion of Catalan language and culture. It is operated by a non-governmental, non-profit organization, the puntCAT Foundation. Due to the commitment of that registry with the Catalan culture, the Spanish authorities didn’t expect them to accept the interception of the domains with the required due diligence, and for this reason the LEA executed the seizure of computers at the puntCAT Foundation offices that host the .cat TLD Registry. Nevertheless, since the operations of the domain registry services are handled by an external provider, .cat domains not connected with the October 1 referendum, including EFF's little-known Catalan language website eff.cat (Malcolm 2017a), were not affected by the seizure.

At the time, many experts expressed their deep concerns about the use of the domain name system to censor content in general if it doesn’t follow, at least, internationally well-defined criteria, such as those collected in the EU draft regulation, preventing the application of the censorship criteria for the prosecution of enemies of a national government, that in international laws would not be considered illegal, even when such seizures are authorized by a court, as happened here. There are two particular factors that compound those concerns in this case:

- First, the content in question here is essentially political speech, which the European Court of Human Rights has ruled as deserving of a higher level of protection than some other forms of speech. Even though the speech concerns a referendum that has been ruled illegal, the speech does not in itself pose any imminent threat to life or limb.
- The second factor that especially concerns experts here is that the seizure took place with only 10 days remaining until the scheduled referendum, making it unlikely that the legality of the domains' seizures could be judicially reviewed before the referendum was scheduled to take place. The fact that such mechanisms of legal review would not be timely accessible to the Catalan independence movement, and that the censorship of speech would therefore be de facto unreviewable, it should have been another reason for the Spanish authorities to exercise restraint in this case.

In general, blocking the domains by the registry could be faster than going through the HSP, because it is part of the responsibility of the registry to guarantee that the domains are not used for criminal acts according to international law and policies. This mechanism has been created to protect the citizens or organisations from being robbed or attacked to their assets in general (e.g. illegal website shops). But when the reasons to seize a domain are just allegations of sedition or any other form of unlawful or controversial speech between political parties, domain name intermediaries should not be held responsible for the content of websites that utilize their domains, and this is clearly stated in the EU new draft regulation.

The seizure of .cat domains is a worrying signal that the Spanish government gives priority to its own interests in quelling the Catalonian independence movement above the human rights of its citizens to access a free and open Internet, and we join ordinary Catalonians in condemning it.

3.3 Mobile voting app

Moreover, a separate court order was obtained requiring Google to remove a voting app from the Google Play app store. The order also required Google to remove any other apps developed by the same developer without further instructions to discriminate its potential illegality. Some activists, violating such orders by setting up mirrors, reverse proxies, or alternative domains for blocked content, were summoned to court to face criminal charges. One of these activists also had his GitHub and Google accounts seized.

Even if the blocking of electoral information pursuant to these court orders was legitimate and proportionate (there is a general consensus in ISOC and other Internet NGO that it was not), it was inevitable that the implementation of the orders would result in over-blocking and censorship of lawful content. An example of this was the blocking of the domain gateway.ipfs.io. This domain is the main webserver for the InterPlanetary File System (IPFS), an experimental Internet protocol for distributed storage of information. Although some information on the October 1 referendum was hosted on this distributed filesystem, this was a tiny proportion of the information that was blocked. On the territory, on the day of the referendum itself, the Internet was shut down at polling places in an effort to prevent votes from being transmitted to returning officers.

4. CENSORSHIP IMPLEMENTATION METHODOLOGY

Following the Court requirement, the Spanish police, the main Telecom operators (TOs) (Censura1oct 2017) and some alternative DNS providers were required to censor some online content. Censorship targeted official Catalan government websites (i.e. government censoring other government, including unrelated sites, like the Catalan public healthcare date requesting service, as just an example of the collateral effects of the indiscriminate attack).

Other websites hosted in Spain or domain names managed by organizations in Spain were also physically disabled. As criticised by some agents about the content of the EU regulation to prevent dissemination of terrorist information, in this case, when the IP address offered by the hosting service to the sites being censored, was shared with other legal sites, all the sites sharing that same IP were blocked, i.e. those with legal content hosted in the same hosting facility. Moreover, in some cases where dynamic IP balancing was used, all the customers of the HSP were blocked for some hours.

Since the court requirement was only accepted in Spain, the recommendations to reach the censored domains by the interested Spanish citizens and the referendum officers, were:

- Use any IP belonging to Cloudflare (anti-DDoS service) for the censored domains, except those explicitly excluded by the TO.
- In some cases, the censorship only was effective in the WWW service, i.e. subdomains like info.refoct.eu were still accessible from DNS resolution servers.
- The most extended solution was to use VPN tunnel, allowing users requesting censored pages to access them from PROXY VPN servers located outside Spain.

The consequence of the court order was the blocking of at least 25 sites related to the Catalan referendum by means of DNS tampering and HTTP blocking. The evidence of that is based on OONI (Open Observatory of Network Interference) Probe network measurements, collected from three local networks. OONI (Lundström and Xynou 2017) data shows that these sites were blocked for several days.

To ensure that voters could participate, even if their appointed voting stations were shut down by the police, the Catalan government announced the application of an open census policy in the morning of the referendum. According to this policy, voters were offered the opportunity to choose any voting station in the country. However, the central system that validated that the voters were in the census was taken down by Amazon during the first hours of the day. Google was also previously ordered to take down a voting app, that provided information about the polling stations for the Catalan independence referendum.

Despite all the attempts to block the process, alternative servers to count votes were deployed and the referendum (1-O) was held. Polling stations officers reported that they had difficulty accessing the Internet at the polling stations, but there are not metrics data to confirm whether throttling or an Internet blackout took place.

To collect evidence showing whether and how sites associated with the Catalan referendum were blocked, OONI Probe tests were run in Catalonia. Those probes showed which ASNs were using DNS tampering, which HTTP blocking and which were "just" seized directly at the registrar of the corresponding TLD (.cat Foundation) for every domain being requested to be censored. In the latter case, the Registrar redirected the censored domains to a generic website created by Akamai Technologies (http://paginaintervenida.edgesuite.net/) by means of the DNS.

5. CONCLUDING REMARKS

The Spanish authorities took several kinds of actions to prevent the dissemination of information and the operation of some services associated with a dispute between governments, which is not recognized as one of the criteria for censoring Internet content. Those actions ranged from registrar seizure of domains at DNS level, modification of DNS tables by the telecom operators and even DDoS attacks perpetrated with the support of spontaneous actors (like in the case of Estonian network take-down by Russian citizens many years ago).

There is a lack of international consensus about what kind of information has to be blocked on Internet, without regard for the civil rights of freedom and opinion.

Provided the global reach of information in Internet, it should be created an international organisation to collect and resolve the complaints about illegal or harmful content for citizens, taking a decision about the need to remove that information or service from the network, and ask the relevant operators to do it immediately. This approach has been proposed and some pilot implementations have been set up in agreement between ICANN and APWG on the basis of protecting from abusive use of copyright-protected information in some URL sites.

REFERENCES

Anti-Phishing Working Group, Inc. (APWG). 2019. Home Page. https://apwg.org.

Censoring webpage, shown in place of censored content. http://paginaintervenida.edgesuite.net/.

Censura1oct. 2017. “Com funciona la censura en línia: Metods.” GitHub, September 16, 2017. https://censura1oct.github.io/en/2017/09/16/methods_en.html.

Cory, Nigel. 2016. “How Website Blocking is Curbing Digital Piracy Without Breaking the Internet.” Information Technology & Innovation Foundation, August 22, 2016. https://itif.org/publications/2016/08/22/how-website-blocking-curbing-digital-piracy-without-breaking-internet.

Cory, Nigel. 2018. “The Normalization of Website Blocking Around the World in the Fight Against Piracy Online.” The Normalization of Website Blocking Around the World in the Fight Against Piracy Online. Information Technology and Innovation Foundation, June 12, 2018. https://itif.org/publications/2018/06/12/normalization-website-blocking-around-world-fight-against-piracy-online.

Donck, Frédéric. 2017. “Statement About the Political Situation in Catalonia.” Internet Society (ISOC): Catalonia Chapter, September 20th, 2017. http://isoc-cat.blogspot.com.es.

European Commission. 2018. *Proposal for a Regulation of the European Parliament and of the Council on Preventing the Dissemination of Terrorist Content Online.* (COM 2018) 640 final. https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-preventing-terrorist-content-online-regulation-640_en.pdf.

European Parliament. 2018. “Legislative Train Schedule: Preventing the Dissemination of Terrorist Content Online.” Last modified September 2018. https://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-preventing-the-dissemination-of-terrorist-content-online.

Generalitat de Catalunya. 2017. “La Generalitat denuncia els abusos i la censura de l’Estat en matèria d’accés a Internet al Vicepresident de la Comissió Europea.” SmartCatalonia. September 26, 2017. http://smartcatalonia.gencat.cat/ca/detalls/noticia/generalitat_denuncia_abusos_censura_estat_acces_internet.

Internet Corporation for Assigned Names and Numbers (ICANN). 2020. “Uniform Rapid Suspension.” https://www.icann.org/resources/pages/urs-2014-01-09-en.

Lundström, Tord and Maria Xynou. 2017. “Evidence of Internet Censorship during Catalonia's Independence Referendum.” Open Observatory of Network Interference (OONI), October 3, 2016. https://ooni.torproject.org/post/internet-censorship-catalonia-independence-referendum/.

Malcolm, Jeremy. 2017a. “.cat Domain a Casualty in Catalonian Independence Crackdown.” Electronic Frontier Foundation (EFF), September 21, 2017. https://www.eff.org/es/deeplinks/2017/09/cat-domain-casualty-catalonian-independence-crackdown.

Malcolm, Jeremy. 2017b. “Which Internet Registries Offer the Best Protection for Domain Owners?” Electronic Frontier Foundation, August 2, 2017. https://www.eff.org/wp/which-internet-registries-offer-best-protection-domain-owners.

Masih, Niha, Shams Irfan, and Joanna Slater. 2019. “India's Internet Shutdown in Kashmir Is the Longest Ever in a Democracy.” *The Washington Post*, December 16, 2019. https://www.washingtonpost.com/world/asia_pacific/indias-internet-shutdown-in-kashmir-is-now-the-longest-ever-in-a-democracy/2019/12/15/bb0693ea-1dfc-11ea-977a-15a6710ed6da_story.html.

Robinson, Gavin. 2018. “The European Commission’s Proposal for a Regulation on Preventing the Dissemination of Terrorist Content Online.” *Eurocrim* 4, 234-40. https://doi.org/10.30709/eucrim-2018-024.

Shahbaz, Adrian. 2018. “The Rise of Digital Authoritarianism.” Freedom House. https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism.

The Guardian. 2020 “*The Guardian* View on Internet Censorship: When Access Is Denied | Editorial.” January 1, 2020. https://www.theguardian.com/commentisfree/2020/jan/01/the-guardian-view-on-internet-censorship-when-access-is-denied.

Trendacosta, Katharine, Elliot Harmon, and Cara Gagliano. 2020. “ICANN.” Electronic Frontier Foundation. Accessed April 8, 2020. https://www.eff.org/issues/icann.

United Nations (UN) General Assembly. 2018. *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression.* A/73/348. https://undocs.org/pdf?symbol=en/A/73/348.

Valdés Cortés, Margarita. 2000. “Internet Censorship Around the World.” Internet Archive, January 3, 2000. http://www.isoc.org/inet2000/cdproceedings/8k/8k_4.htm.

Wikipedia. 2019. “Internet Censorship and Surveillance by Country.” Accessed October 14, 2019. https://en.wikipedia.org/wiki/Internet_censorship_and_surveillance_by_country.

Wikipedia. 2020. “Internet Censorship.” Accessed February 14, 2020. https://en.wikipedia.org/wiki/Internet_censorship.