Internet censorship in the Catalan referendum

Overview of how the state censored and how it got circumvented

Disclaimer

- I’m not a security specialist
- More a collection of public available information
- I wasn’t involved in any illegal activity, sorry only second-hand information
- I like to sleep in my own bed…

Outline

- Background
- Brief timeline
- How did net filtering work
- Notes about the “Where to vote” homepage
- Day of the referendum
- Conclusion
- Q&A

Background

- Own language
- Own culture
- One of the richest regions of Spain
- Long history of struggle to get more autonomy
- Referendum on 1st of October 2017

Background

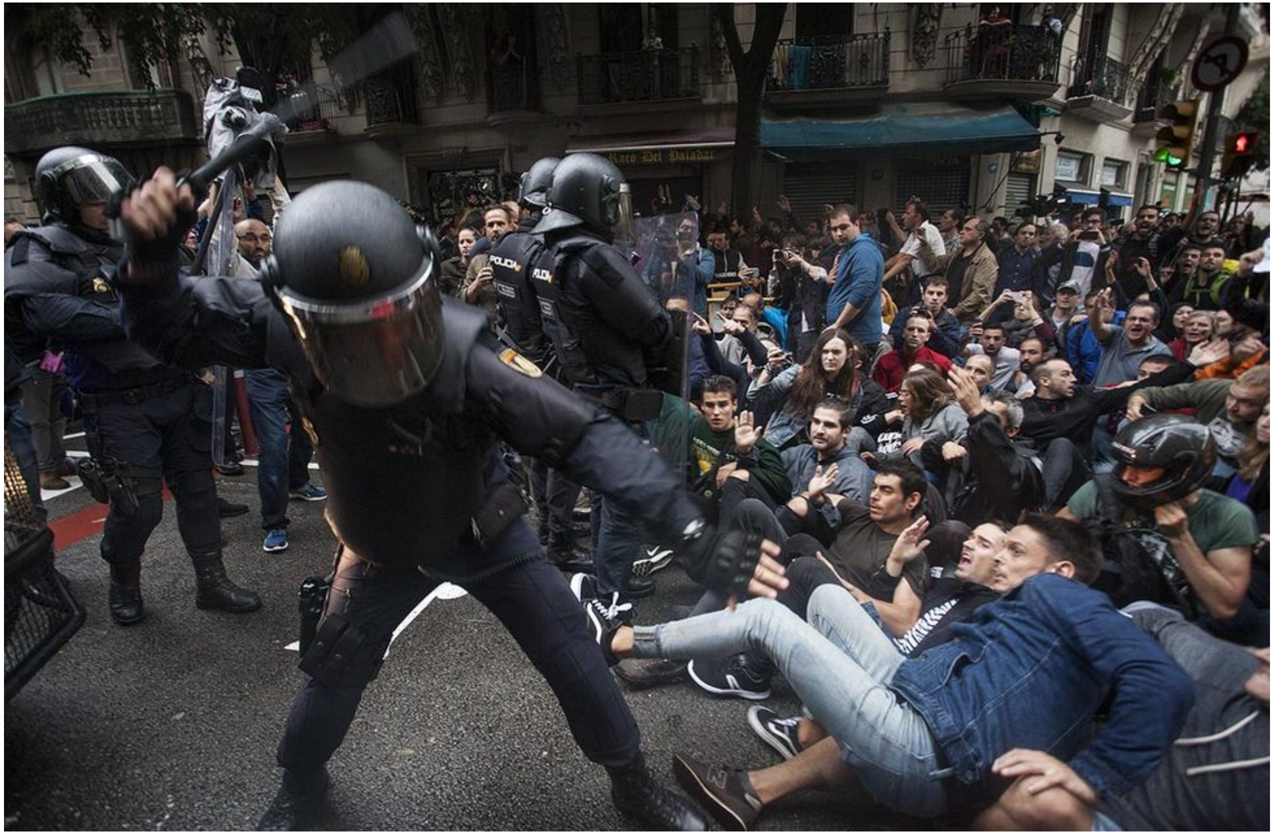
- **Internet censorship wasn't the only thing**
- **Pro-Referendum material was confiscated**
- **800+ injured by police on day of referendum**[1]

  One man lost his eye by a police rubber bullet
- **4 persons in prison without bail (incl. vice-president)**
- **President of Catalonia and 4 ministers in Brussels in exile**

More about police brutality: https://spanishpolice.github.io/

[1] https://www.hrw.org/news/2017/10/12/spain-police-used-excessive-force-catalonia

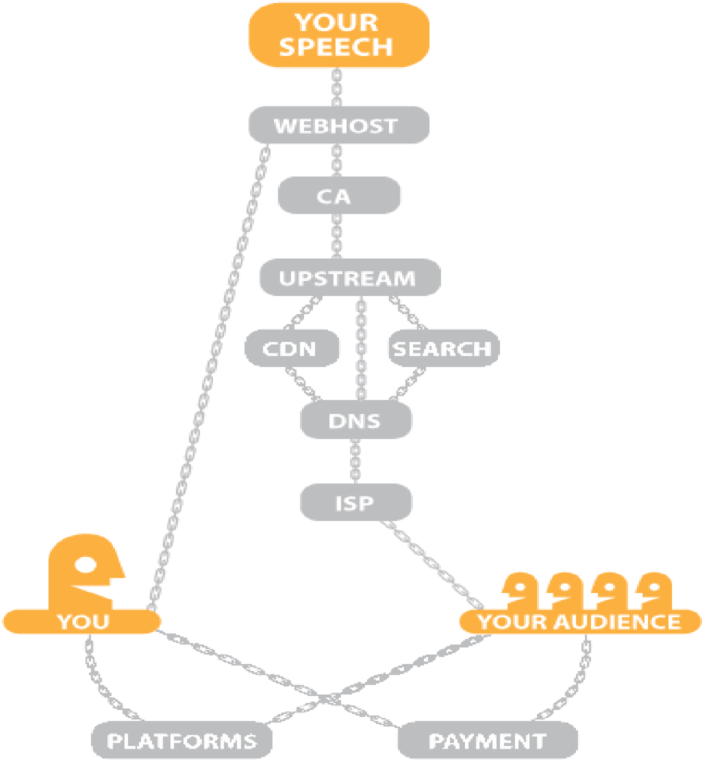
Spain is different



https://en.wikipedia.org/wiki/Catalan_independence_referendum,_2017

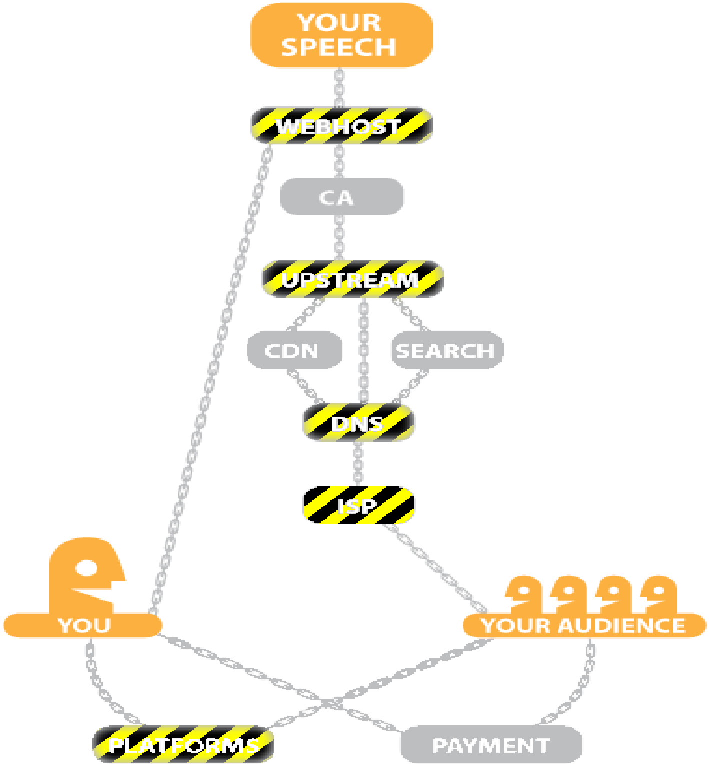
Let’s get technical

How internet censorship works



https://www.eff.org/free-speech-weak-link/

Spoiler alert!

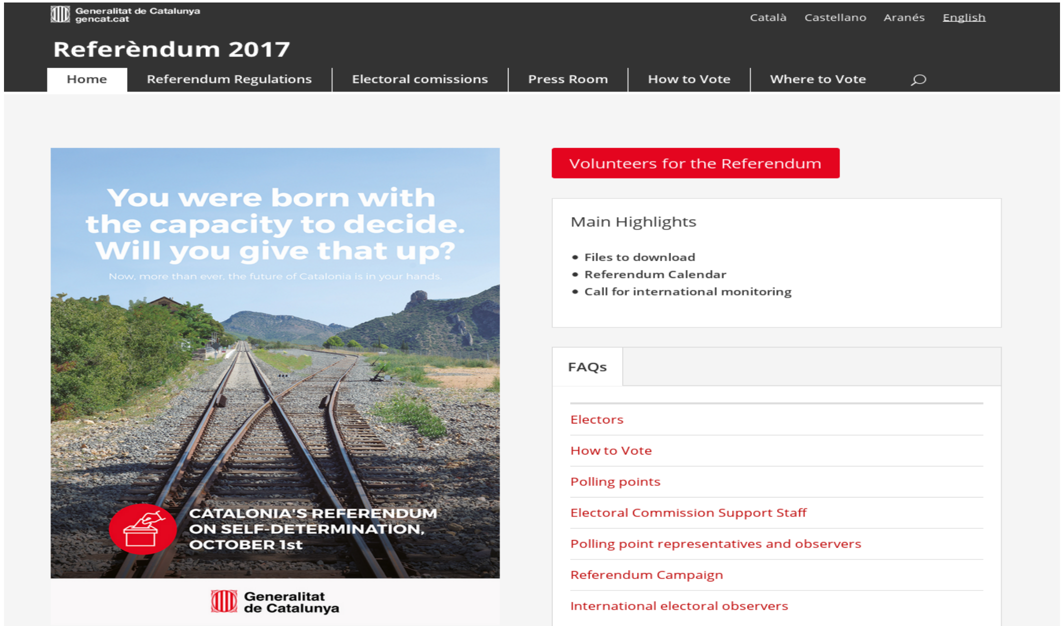


https://www.eff.org/free-speech-weak-link/

13th of September

- referendum.cat informs about the referendum

- Federal police enters web hosting provider CDMON



Referèndum 2017

You were born with the capacity to decide. Will you give that up?

Now, more than ever, the future of Catalonia is in your hands.

CATALONIA'S REFERENDUM ON SELF-DETERMINATION, OCTOBER 1st

Generalitat de Catalunya

Main Highlights

- Files to download
- Referendum Calendar
- Call for international monitoring

FAQs

Electors

How to Vote

Polling points

Electoral Commission Support Staff

Polling point representatives and observers

Referendum Campaign

International electoral observers

- Mirror ref1oct.cat appears, later ref1oct.eu

Brief timeline

- 14th of September: two more official websites seized
- 16th of September: On a judge order ISPs start to block home pages
- Activity starts to create mirrors of the official websites

20th of September

- **Spanish state took over control of the Catalan treasury**
- **Federal police will be sleeping in ships in Catalan ports**
- **A total of 14 arrests by federal police**
- **Several high-ranking officials of Catalan government and civil servants**

  Members of the Center of Telecommunications and Technology (CTTI)

  Group of hacktivists took over using TOR, signal, anonymous SIM cards, bitcoin... [1]
- **Also arrested the technical director of Fundació .cat**

[1] https://www.vilaweb.cat/noticies/els-hackers-que-van-fer-possible-el-cens-universal/

Fundació .cat

- Top Level Domain operator of .cat
- At 15th of September it got a first court order to shut down ref1oct.cat
  - In total 3 court orders with list of domains
  - Resolve .cat domains to police server
- ..but also to begin to block “all domains that may contain any kind of information about the referendum”.
- Places burden of blocking domain names on the registry operator.

Fundació .cat

- On 17th of September inform ICANN about the warrant[1]
- On 20th of September Technical Director gets arrested
- Retained under custody for 2 ½ days
- Accusation of

  misappropriation of public funds

  perversion of justice

  disobedience

- Reasons for now unclear, awaiting to see proofs provided by the prosecutor

[1] https://twitter.com/puntcat/status/909525852446187521/photo/1

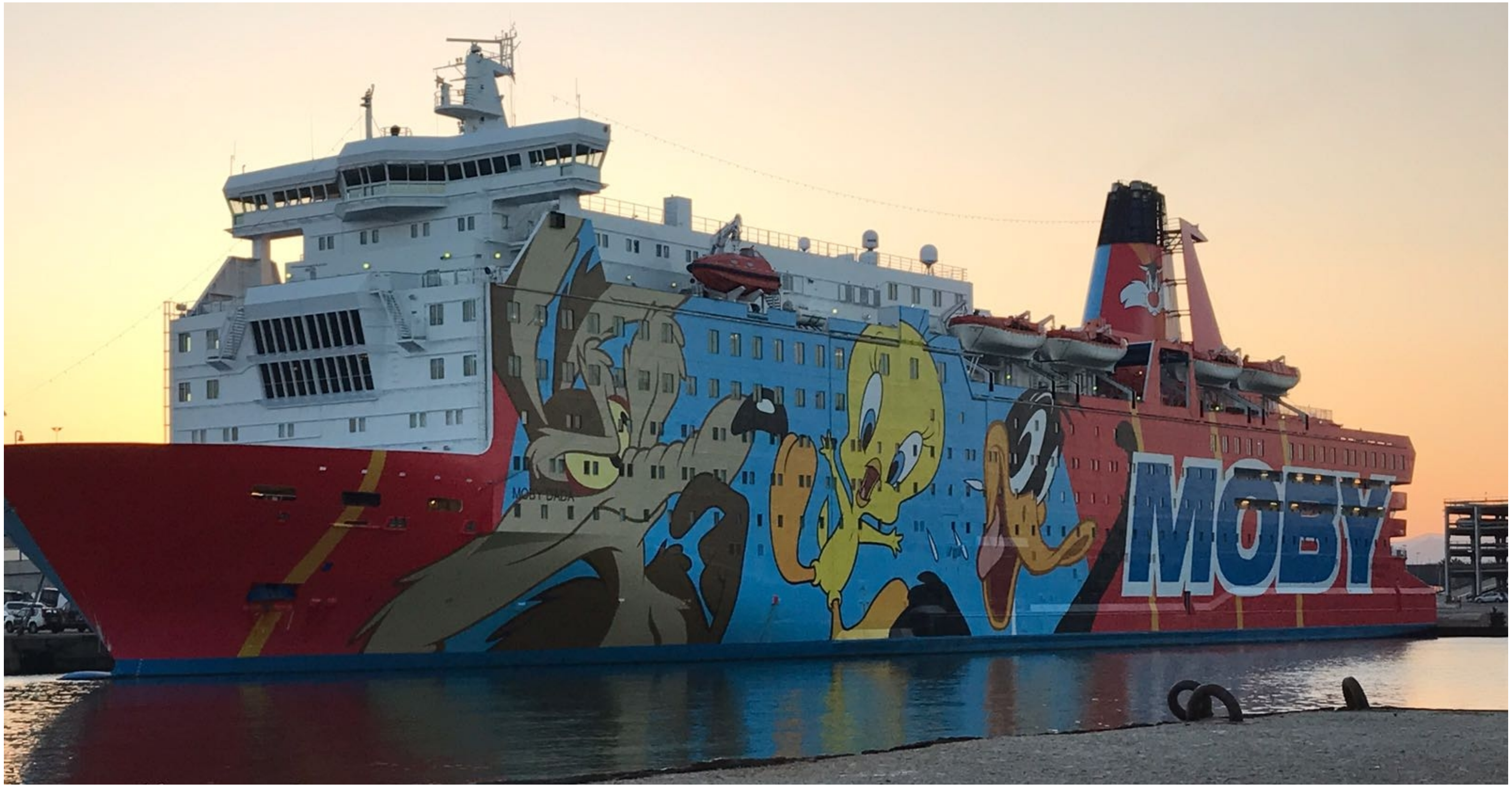
Mirrors

- Massive amounts of mirrors appeared in the next days
- Exact number difficult to know but easily over 100
- Mirror in the TOR network - http://usxzmlnuzt4oioe7.onion/
- Funny names like

  www.guardiacivil.sexy

  www.piolin.cat

Tweety?



22nd of September

- Police raids a house near Valencia
- Accusation of being head of a group organized to mirror the referendum website via: https://github.com/GrenderG/referendum_cat_mirror
- Search warrant included order to change passwords + security questions for github, facebook, twitter, mail, etc

22nd of September

- Police took (illegally) control over open sessions in the browser
- He was able to recovered them a few days later
- Accused of disobedience (6 months – 4 years of prison)

- More then 15 people were cited to declare

Censor methods

Analysis of the censor methods

- Open Observatory of Network Interference (OONI) reports 25 websites blocked [1]
- Other sources talk about 70 websites blocked [2]
- Some media reports talk about 140 blocked websites [3]
- Mirrors of official websites
- Political organisations, Yes-Campain websites

  enpaperem.cat, ...

[1] https://ooni.torproject.org/post/internet-censorship-catalonia-independence-referendum/

[2] https://www.nodo50.cat/

[3] https://www.media.cat/wp-content/uploads/2017/12/Informe_1-O_ENG.pdf

Analysis of the censor methods

- **Up to now seen**
  - Webhosting seized
  - Redirection of .cat domains to “police landing page” by the TLD name server
- **Methodes used by ISPs**
  - DNS tampering
  - HTTP blocking
- **Different blocking methods used by different ISPs**

Filter techniques by ISPs [1, 2, 3]

- **DNS tampering**

  Orange (France Telecom Spain), Vodafone, Euskatel

- **Deep Package Inspection (DPI)**

  Movistar (Telefónica)

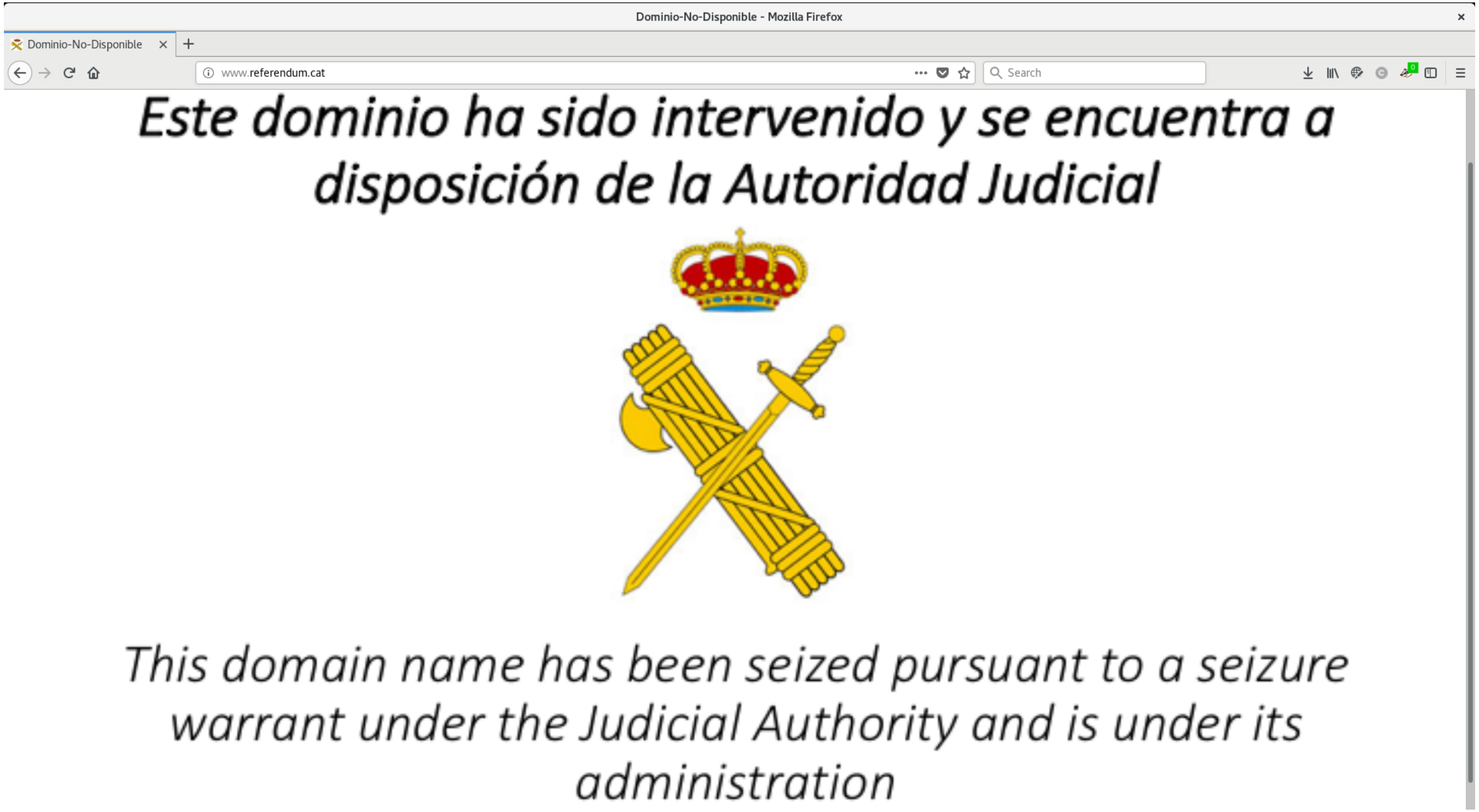
- **Smaller ISPs which connect to larger ones are affected as well**
- **Some small independent ISPs were not affected**

[1] https://censura1oct.github.io/en/2017/09/16/methods_en.html

[2] https://ooni.torproject.org/post/internet-censorship-catalonia-independence-referendum/

[3] https://www.qurium.org/alerts/spain/blocking-techniques-catalunya

Analysis of the censor methods



Este dominio ha sido intervenido y se encuentra a disposición de la Autoridad Judicial

This domain name has been seized pursuant to a seizure warrant under the Judicial Authority and is under its administration

DNS tampering

- ISP’s DNS server resolves URL to police “landing page”

- Change your DNS resolver address
- In case of an original Vodafone router, ask them to disable their DNS proxy
- Alternatively use a VPN

Deep Package Inspection

- HTTP blocking
- Match between the IP addresses and host name in the HTTP GET request
- A regular expression was used to filter host names

Deep Package Inspection

- **Example www.ref1oct.eu**
- **regular expression**

  *.www.ref1oct.eu → did not work

  *.ref1oct.eu → did work
- **Website used cloudflare CDN**

  Two IP addresses from cloudflare were used for matching

  → if you used a different cloudflare IP it worked

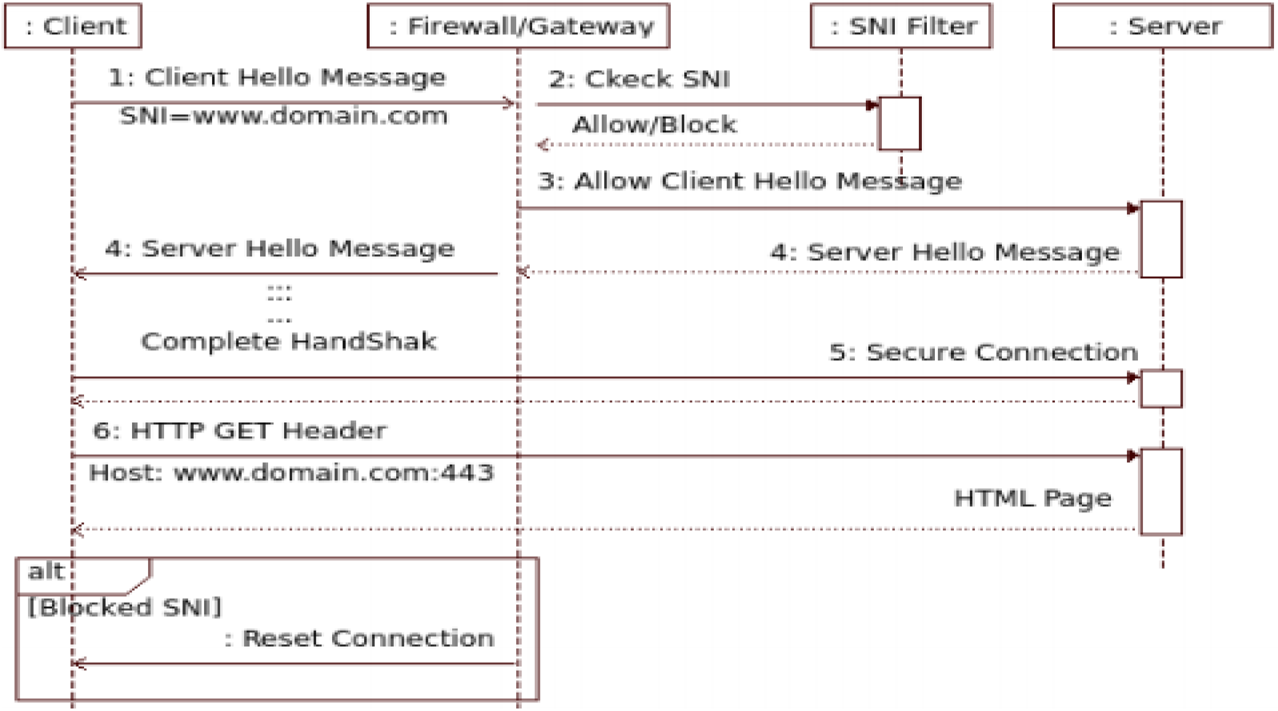
Server Name Indication (SNI)

- HTTPS – HTTP traffic is encrypted

  TCP Host parameter not readable by DPI

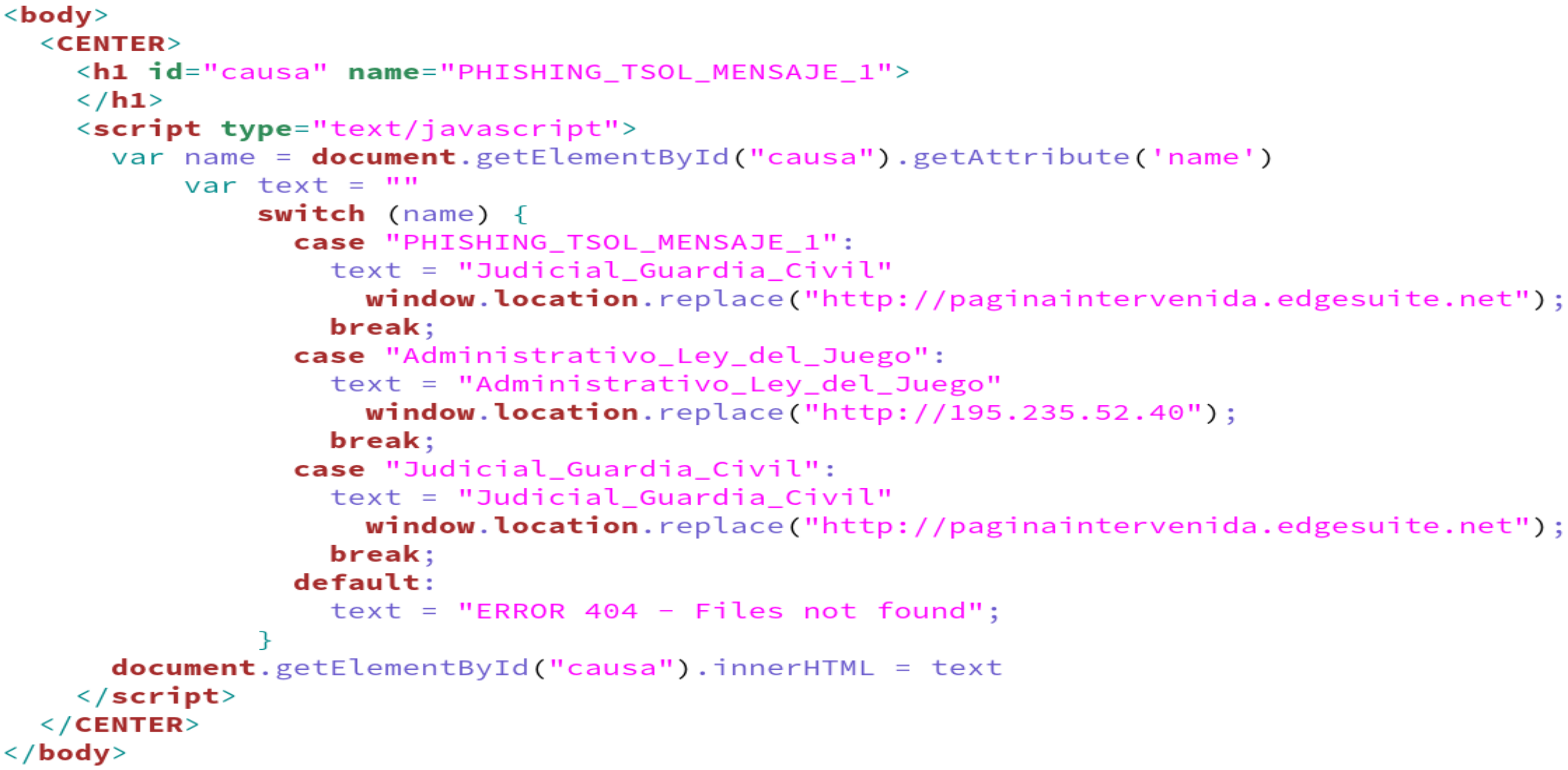
- Multiple URLs resolve to the same IP address
- Host names can have different TLS certificate
- SNI gives a hint to the host which certificate is required
- Used by all state-of-the art browsers

Server Name Indication (SNI)



https://hal.inria.fr/hal-01202712/file/Im2015-Presentation-Slides.pdf

Deep Packet Inspection (DPI)



```
<body>
  <CENTER>
    <h1 id="causa" name="PHISHING_TSOL_MENSAJE_1">
    </h1>
    <script type="text/javascript">
      var name = document.getElementById("causa").getAttribute('name')
          var text = ""
              switch (name) {
                case "PHISHING_TSOL_MENSAJE_1":
                  text = "Judicial_Guardia_Civil"
                    window.location.replace("http://paginaintervenida.edgesuite.net");
                  break;
                case "Administrativo_Ley_del_Juego":
                  text = "Administrativo_Ley_del_Juego"
                    window.location.replace("http://195.235.52.40");
                  break;
                case "Judicial_Guardia_Civil":
                  text = "Judicial_Guardia_Civil"
                    window.location.replace("http://paginaintervenida.edgesuite.net");
                  break;
                default:
                  text = "ERROR 404 - Files not found";
              }
      document.getElementById("causa").innerHTML = text
    </script>
  </CENTER>
</body>
```

Deep Packet Inspection (DPI)

- When filter gets activated HTTP 403 is returned
- Replaces the content with the police picture
- Several landing pages for different issues → reuse of exising infrastructure

Deep Packet Inspection (DPI)

- **DPI hold state for 10 seconds, so:**

```
function input {
        sleep 11
        echo "GET / HTTP/1.1"
        echo "Host: guardiacivil.sexy"
        echo
        echo
}
input | nc guardiacivil.sexy 80
```

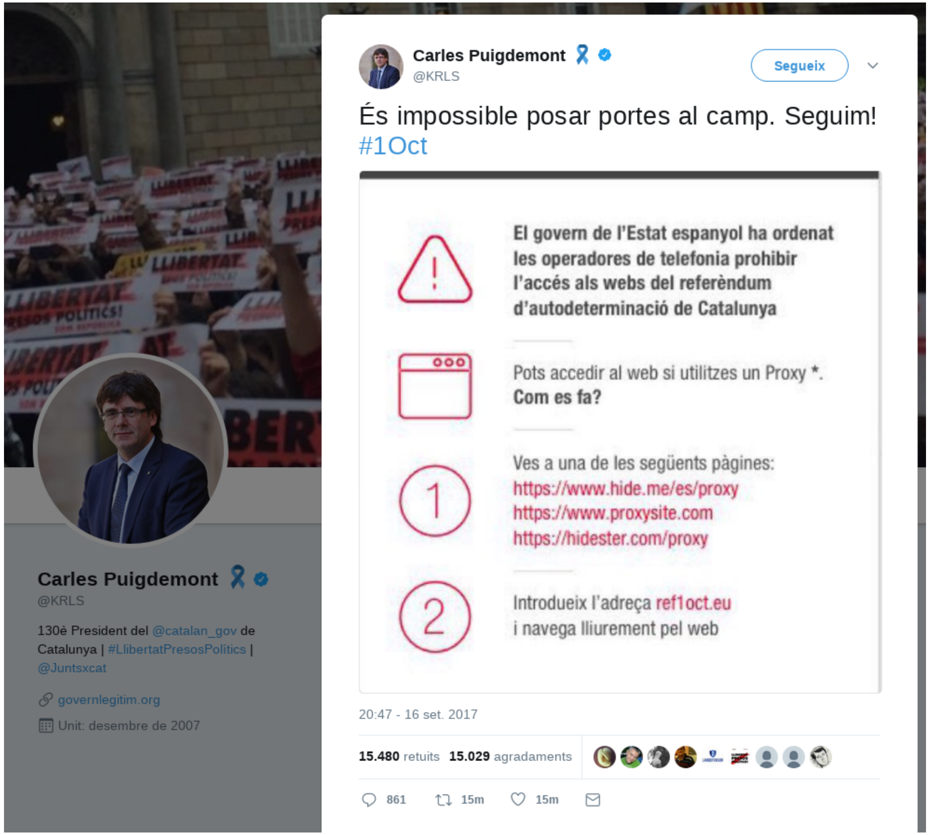
DPI conclusions

- Add a different cloudflare IP to resolve the domain
- Delay the HTTP GET for 11 seconds
- Use a VPN

Censorship conclusions

- Technically circumvent censorship is easy
- As long as you don’t have to educate 5.3 million voters

- ISPs did not communicate to the users
- Choose your ISP wisely, you might get around censorship (!)



Carles Puigdemont
@KRLS
Segueix

És impossible posar portes al camp. Seguim! #1Oct

El govern de l’Estat espanyol ha ordenat les operadores de telefonia prohibir l’accés als webs del referèndum d’autodeterminació de Catalunya

Pots accedir al web si utilitzes un Proxy *. Com es fa?

1 Ves a una de les següents pàgines:
https://www.hide.me/es/proxy
https://www.proxysite.com
https://hidester.com/proxy

2 Introdueix l’adreça ref1oct.eu
i navega lliurement pel web

20:47 - 16 set. 2017

15.480 retuits 15.029 agradaments

861 15m 15m

Carles Puigdemont
@KRLS

130è President del @catalan_gov de Catalunya | #LlibertatPresosPolítics | @Juntsxcat

governlegitim.org

Unit: desembre de 2007

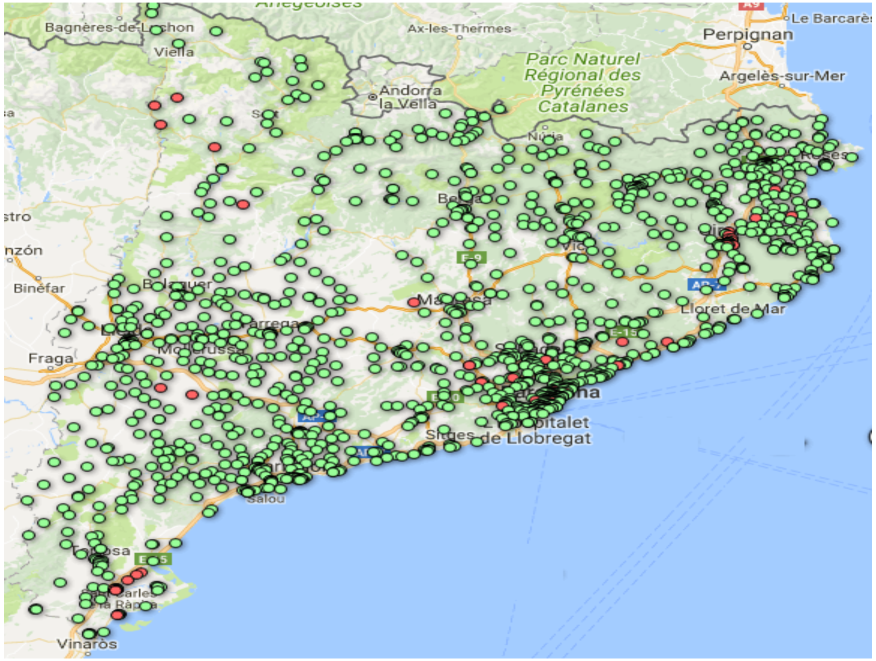
https://twitter.com/KRLS/status/909126641145798656

Where to vote website

Where to vote?

- Spanish post service denied to send information
- Census of 5.3 million voters
- 1000+ polling stations

- It was foreseen that the official homepage will be blocked
- Website must be easily clone-able



https://www.vilaweb.cat/noticies/referendum-1-octubre-1o-votacio-cens-electoral-guia-meses-participacio/

Where to vote?

- 21st of September - Published the web to search your polling station
- Get's blocked the next day
- Telegram and Twitter bot
- Android App is published in the google play store

  Pulled out of GooglePlay on 29th of September

Where to vote?

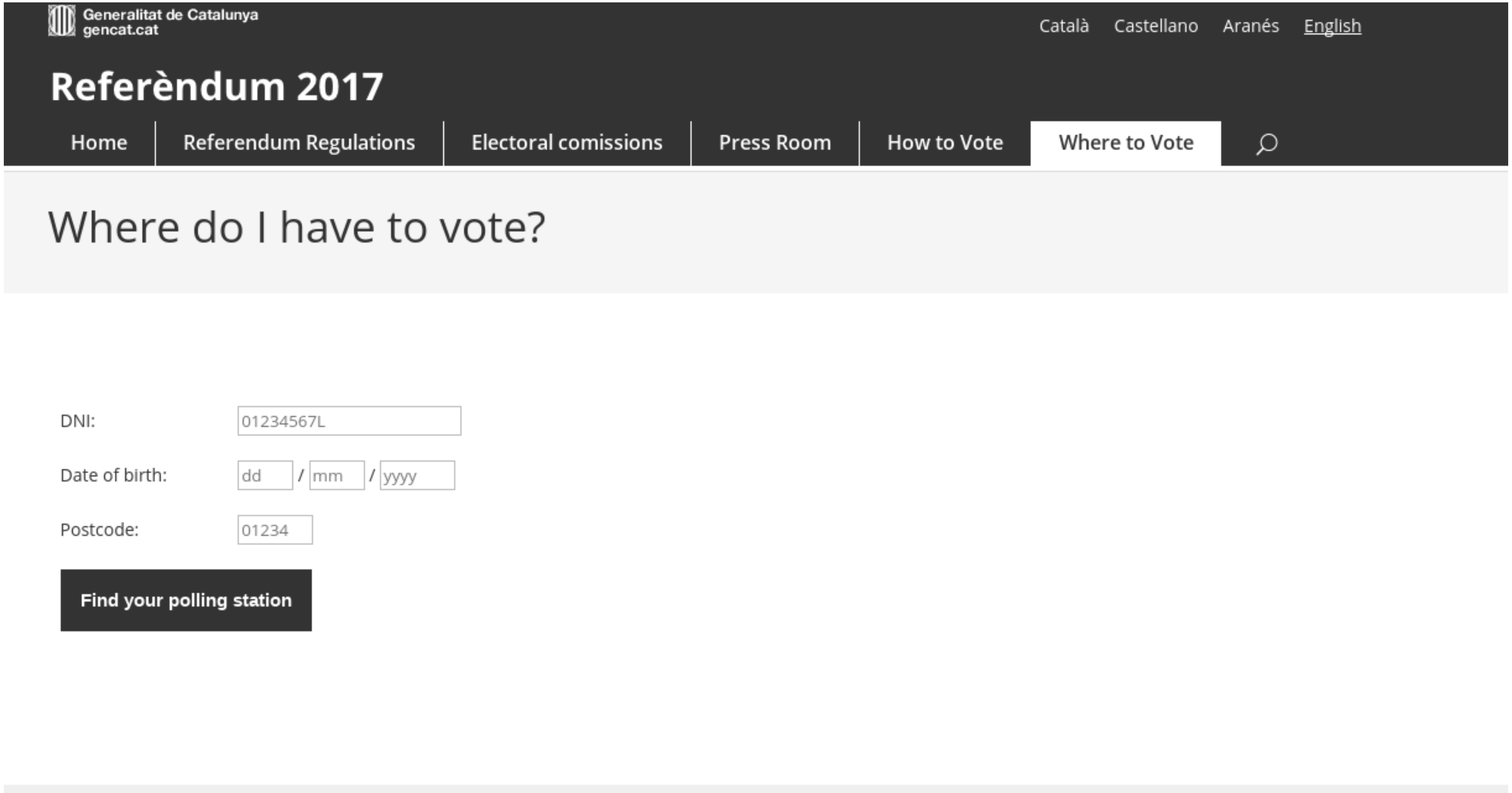
- **Many clones appear**
- **Web get’s published in IPFS**

    https://gateway.ipfs.io/ipns/QmZxWEBJBVkGDGaKdYPQUXX4KC5TCWbvuR4iYZrTML8XCR

- **gateway.ipfs.io got blocked for around one week by Telefónica**
- **Impact on unrelated content**

    But ipfs.io still possible

Where to vote?



Referèndum 2017

Where do I have to vote?

DNI: 01234567L

Date of birth: dd / mm / yyyy

Postcode: 01234

Frontend is the backend [1, 2]

- Census of 5.3 million voters stored in several encrypted files on the web server
- “ID[3..8] + date of birth + postcode” are hashed 1714+1 times with SHA256
- The first 4 hex values used to identify the encrypted file
- Collisions group persons in files

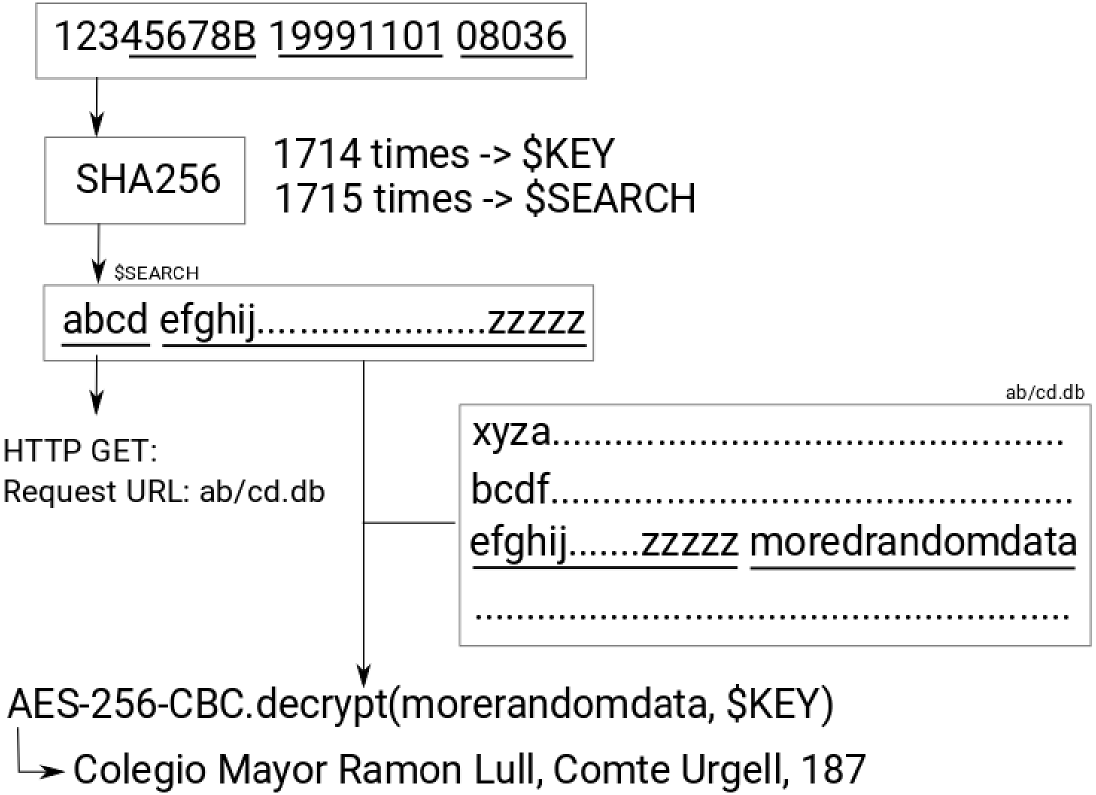
[1] http://www.entredevyops.es/posts/referendum-votar.html

[2]https://hackernoon.com/is-sensitive-voter-data-being-exposed-by-the-catalan-government-af9d8a909482

Frontend is the backend

- Each file has around 70 entries
- Part of the SHA256 hash matches an entry
- The entry contains the polling station encrypted with AES-256-CBC

Frontend is the backend



12345678B 19991101 08036

SHA256

1714 times -> $KEY
1715 times -> $SEARCH

$SEARCH

abcd efghij.....................zzzzz

HTTP GET:
Request URL: ab/cd.db

ab/cd.db

xyza...
bcdf..
efghij.......zzzzz moredrandomdata
....

AES-256-CBC.decrypt(morerandomdata, $KEY)

Colegio Mayor Ramon Lull, Comte Urgell, 187

Is this secure?

- Brute force attack possible
- Dates and post codes allows to group for divide-and-conquer
- Letter in DNI works as a checksum

Conclusion

- It’s possible to get a reduced number of DNIs per post code and birth of date
- How valid is the data obtained? DNI is a public data.

- Data was stored encrypted on the server which allowed for an easy to clone website
- Alternatives like adding a salt is not feasible
- Any ideas?

30th of September

- **Federal police took control over Center of Telecommunications and Technology (CTTI)**

  All entities of the Catalan government have access to internet via CTTI

- **Probably start to monitor IPs mostly of the future polling stations**

Day of the referendum

Day of the referendum

- People occupied the polling stations since the day before
- Hundreds gathered in front of the polling stations
- Ballots and ballot boxes arrived early in the morning

Day of the referendum

- **Global census, everybody could go to any polling station**

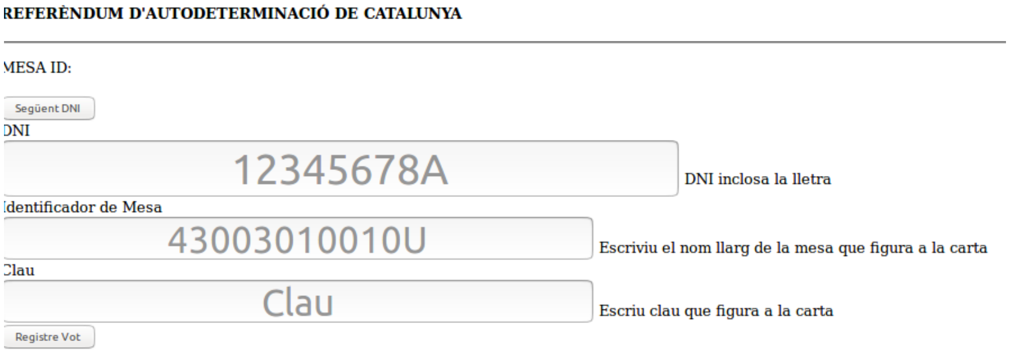
  It was foreseen that the police will close-down polling stations by force

- **Register polling place via ID + password**

  Password used for authentication and encryption

- **Enter the DNI to register the voter in a centralized database**

- **Tight time-frame, from 9:00 to 20:00**



REFERÈNDUM D'AUTODETERMINACIÓ DE CATALUNYA

MESA ID:

DNI: 12345678A — DNI inclosa la lletra

Identificador de Mesa: 43003010010U — Escriviu el nom llarg de la mesa que figura a la carta

Clau: Clau — Escriu clau que figura a la carta

Day of the referendum

- **Polling stations internet connection was through CTTI**

    Some cut off from the net

    Some TOR blocked

    Reports of blocked IPs

- **Some polling stations had alternative access to the net**
- **In many polling station people used their cellphones/4G APs/Wifi from neighbors to register voters**

    Different IPs blocked by different ISPs

Day of the referendum

- **Global home page registremeses.com**

  Used cloudflare

  Was blocked within minutes

  Used IP addresses directly
- **Reverse proxies shield the central server**
- **Reverse proxies were taken down constantly in the first hours through DDOS attacks**
- **New proxies were communicated via hotline/instant messaging**

  After few minutes DDOS attack for new IP was in place

Day of the referendum

- **Whenever a new IP address was used, polling place needs to re-register**

  Possibility of social hacking

  No secure communication channel between polling place responsible and hotline

Day of the referendum

- **DDOS attack organized via Forum “Foro Coches” [1]**

  “I want to remind you that to DDOS something that is illegal, it is not illegal!”

- **IP addresses got published**
- **Updates on not reachable IP addresses**
- **Evidence of SYN-Flood attack**

  DDOS techniques were used, not just users sitting in front of their computer

- **Port knocking was introduced to mitigate the attack**
- **Foro Coches and others got attacked by hacker groups [2]**

[1] https://www.qurium.org/alerts/spain/blocking-techniques-catalunya

[2] https://www.naciodigital.cat/noticia/140059/aixi/es/van/fer/ciberatacs/contra/referendum

Conclusion

- **Attacks on the**

  Net infrastructure

  Filtering techniques

  Distributed Denial Of Service attacks

- **Voting could take place**
- **Central server was the weakest point of the system**

  Would it be possible to build something like this in a decentralized manner?

Aftermades

- **Participation of referendum was 43.03%**

  2.044.038 – Yes to independence

  177.000 – No, and 44.913 Vote “en blanc”

- **10th of October – website of Assemblea Nacional Catalan (ANC) shut down again**
- **30th of October – several websites of the catalan government got shut down**

- **19th of December ANC took legal actions against the blockage of their website**

Conculsion

- Maybe the biggest case of internet censorship in European Union so far
- Government tried to load censorship responsibility to top-level-domain registrar
- Huge repression against creators of mirrors
- Unconventional data-storage might need a deeper look

- Although repression on the street and censorship on internet, the Spanish state wasn't able to stop the referendum.

International reaction

- **Internet society**

  https://www.internetsociety.org/news/statements/2017/internet-society-statement-internet-blocking-measures-catalonia-spain/

- **Electronic Frontier Foundation**

  https://www.eff.org/deeplinks/2017/09/cat-domain-casualty-catalonian-independence-crackdown

- **Julian Assange**

  https://www.rt.com/news/405119-assange-catalonia-internet-war/

- **Peter Sunde**

  https://twitter.com/brokep/status/909685207497879554

- **…**

Questions?

Thanks a lot!

- Mercè Molist (@mercemolist)
- Daniel Morales (@GrenderG)
- Lluis from guifi.net
- People from sobtec.cat
- Hackmeeting Madrid
- And many more...