



# DNS in times of COVID-19

## ccTLD experience

24 June 2020



[https://cdn.emojindex.com/emoji/seal/female\\_police\\_officer.png](https://cdn.emojindex.com/emoji/seal/female_police_officer.png)

- ★ **Please type your questions in Q&A pod.**
- ★ Text written in the chat will not be read aloud.
- ★ Chat sessions are archived.
- ★ Moderator and remote participation manager will manage the queue.
- ★ This meeting is governed under ICANN's Expected Standard of Behavior.

<http://www.icann.org/en/news/in-focus/accountability/expected-standards>



Alejandra Reynoso (.gt)

## Summary

- ★ ICANN 66 - Montréal
  - Plenary “DNS Abuse” ICANN 66
  - “DNS Abuse prevention system” by EURid (ccTLD news)
- ★ ICANN 67 - Cancún
- ★ ICANN 68 - Kuala Lumpur (virtual)
  - Emphasis COVID-19

## ★ Part 1 - [60 min] Impact of COVID-19

- TLD-OPS business continuity and disaster recovery playbook
- Running a ccTLD in crisis mode
- ccNSO Internet Governance Liaison Committee (IGLC) contribution on capacity building

## ★ 15 min break



## ★ Part 2 - [75 min] DNS Abuse

- What is DNS Abuse and why is it relevant to ccTLD managers?
- COVID-19 issues from an ICANN perspective
- Panel discussion

## TLD-OPS Business Continuity / Disaster Recovery Playbook.



Jacques Latour (.ca)



Régis Massé (.fr)



Alejandra Reynoso (.gt)



Barbara Povše (.si)



Patricio Poblete (.cl)

Running a ccTLD in crisis mode: from the 2019 political upheaval to the 2020 pandemic.



Pierre Bonis (.fr)

Internet Governance Liaison Committee (IGLC) contribution on capacity building.



*ccTLD Security and Stability Together*

A light gray, dotted world map serves as a background for the central text.

# **TLD-OPS** **DNS in times of COVID-19:** **the ccTLD experience**

**June 23, 2020**  
**ICANN68, Remote**

Jacques Latour, .ca (Chair)  
Régis Massé, .fr (Vice Chair)

# Ahhh!! Not another boring TLD-OPS update! Remote! In the middle of the night!!!!

- What can I do:
  - ~~A. Run away~~
  - ~~B. Sleep~~
  - ~~C. Daydream~~
  - ~~D. Play solitaire~~



E. The best you can do stay awake!

# DR/BCP - Drafting Team Status: Success

- Dirk Jumpertz, .EU, was unanimously approved as DR/BCP Drafting Team fearless leader and outstanding contributor to the DR/BCP plan :-)



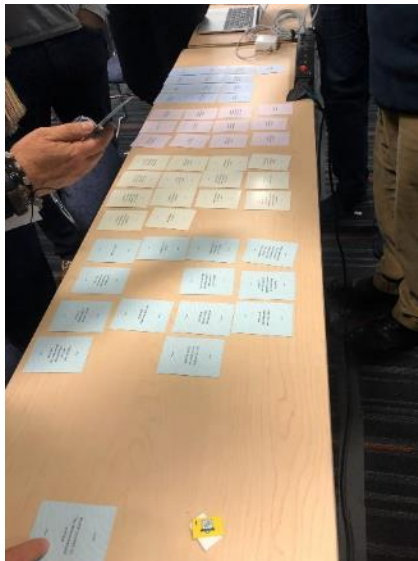


# DR/BCP Table Top eXercise (TTX) Workshop @ ICANN66 Montreal

- Simulate a registry compromise
- Test the DR/BCP Playbook against the scenario
- Update the DR/BCP Playbook against the gaps, observations and lessons learned
- ~30 different ccTLDs attended



# Even working during the break 😊



# Workshop Document Templates



TLD-OPS BCP/DR Workshop  
Document Templates  
ICANN 66



TLD-OPS BCP/DR Playbook  
Draft  
October 25, 2019



TLD-OPS BCP/DR Workshop  
OK Registry Overview  
ICANN 66

## Description of the OK Registry

are employed at "OK registry", the registry operator for the .ok ccTLD. OK known as Old Kontry, is a small European country with approximately 50k inhabitants. Because of its liberal policies, the .ok top level domain is quite popular and has 372.304 domain names registered as of November 1st 2019. .ok domain names are sold through a worldwide network of approximately 250 registrars.

OK is a unitary parliamentary constitutional monarchy. OK is not part of the EU.

OK is located in the capital and is part of the "University of OK", but is independent (management, financial and technical); the university is the legal authority though.

For DNS services, it utilizes the MegaRyCorp. Inc., a DE registry service provider. For other services, it utilizes in backend services for registries. 1 US anycast provider is



# Table Top Exercise (TTX)

## Scenario of the exercise

### ROUND 1: input

FRI, 05:00 PM

- a security researcher contacts the general manager of the registry operator that he found evidence on pastebin of an excerpt of a database that seems to point to the registry's extranet used by their registrars.
- the researcher checked the hashed passwords on pastebin and managed to quite easily "crack" some of the passwords. As expected "password123" is quite common. He confirms that he logged on to the registrar extranet at some specific times (he gives those times to the manager).
- the pastebin is still online and the researcher also found some evidence that someone is selling the credentials on the dark web.
- he believes there is sufficient evidence to assume someone hacked the registry and that the malicious actor has started to cash in on his handiwork.

*This is the initial information received by the registry. How will the manager react, what will he/she do? From here the manager must be fed with some additional information depending on his course of action. Remember to keep an eye on the clock. The participants have only 15 minutes per round.*

# Table Top Exercise (TTX)

## ROUND 2: input

FRI, 08:00 PM

- 3 hours have passed since the initial discovery
- someone tweets the link to another pastebin with the hashtag #freeDomains4All #longLive.OK; it's a copy of the original pastebin.
- the tweet gets picked up and retweeted; the hashtag is amended with #itWorks.

## ROUND 3: input

FRI, 10:00 PM

- 2 hours have passed
- the registry operator is contacted by the press, they want to know what's going on and ask for a formal statement.
- the registry operator's manager gets a phone call from the national television.
- the engineers are still looking into the matter, but haven't found yet where the leak came from.

## BONUS ROUND: input (10 minutes before the end of the round)

*To make the exercise extra interesting, additional information can be injected. In real life, events do not follow a predictable pattern, certainly not during a crisis. Bonus rounds only deliver additional information that needs to be parsed and acted upon before the end of the round.*

- the engineers have some good and some really bad news.
- they have found were the hackers had entered the system and traced what has changed.
- they also noticed that more than 50k additional domain names had been registered and an undefined number of existing domain names had been altered; some of them are high profile domain names.
- they suggest to roll back the DNS and reach out to the major Internet Service Providers to reload their resolvers

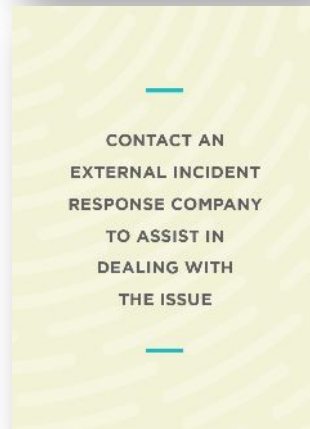
# Table Top Exercise (TTX)

## ROUND 4: input and final round

**SAT: 06:00 AM**

- 8 hours have passed
- the national CERT contacts the registry operator; they have received some intelligence about the origin of the attack
- the social media of the registry operator are bombarded with questions by concerned domain name holders and registrars
- the generic mailboxes have exploded with more than 5.000 email received
- the media contacts the registry operator again for updates and are asking why it is taking so long to fix the issue
- the relevant supervising ministry (e.g. telecommunications) is contacting the registry operator's general manager, they want status updates and a debriefing of the impact of the incident

# DR/BCP Playing Cards – Big Success!

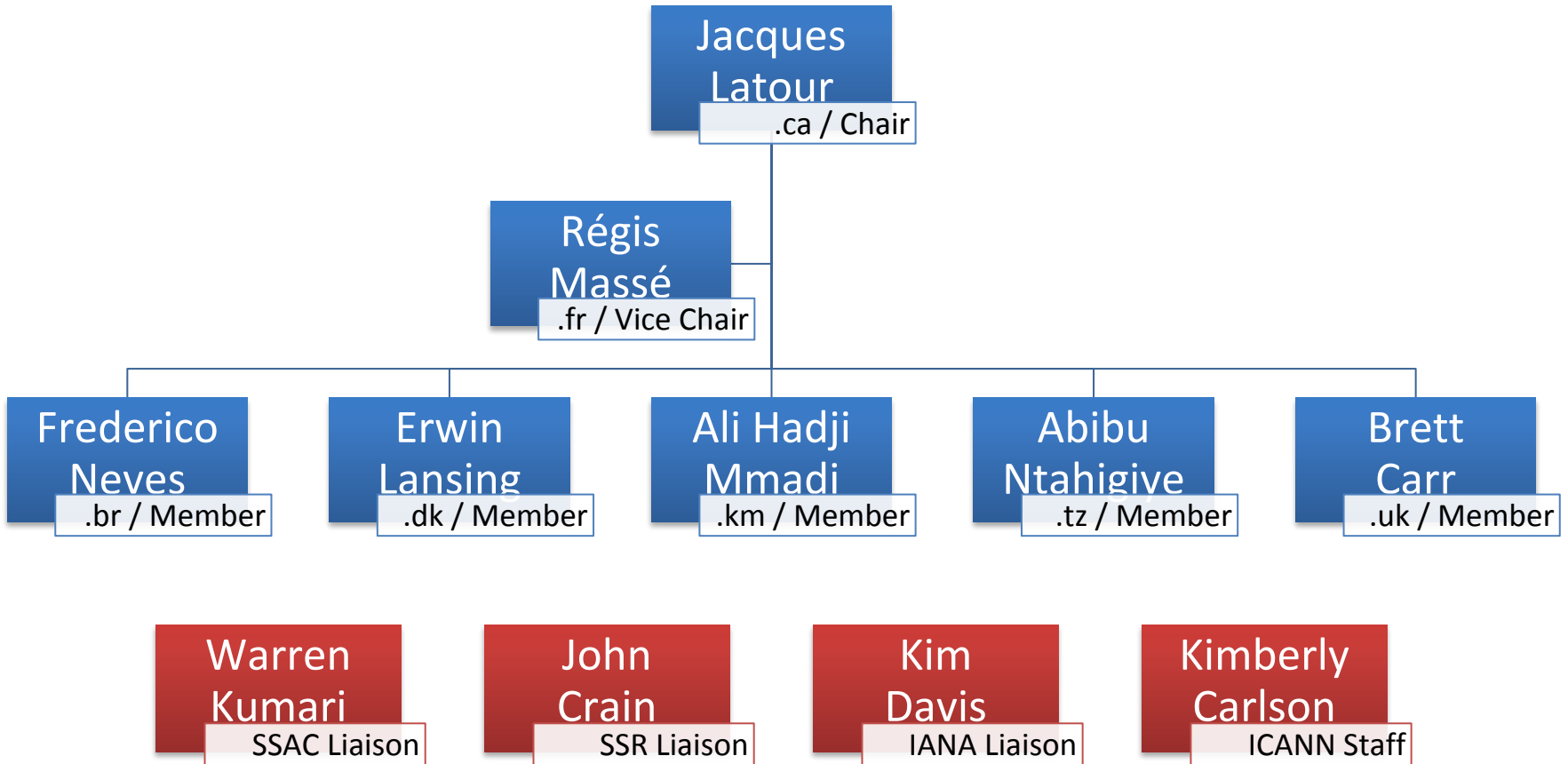


# DR/BCP Playing Cards – Big Success!

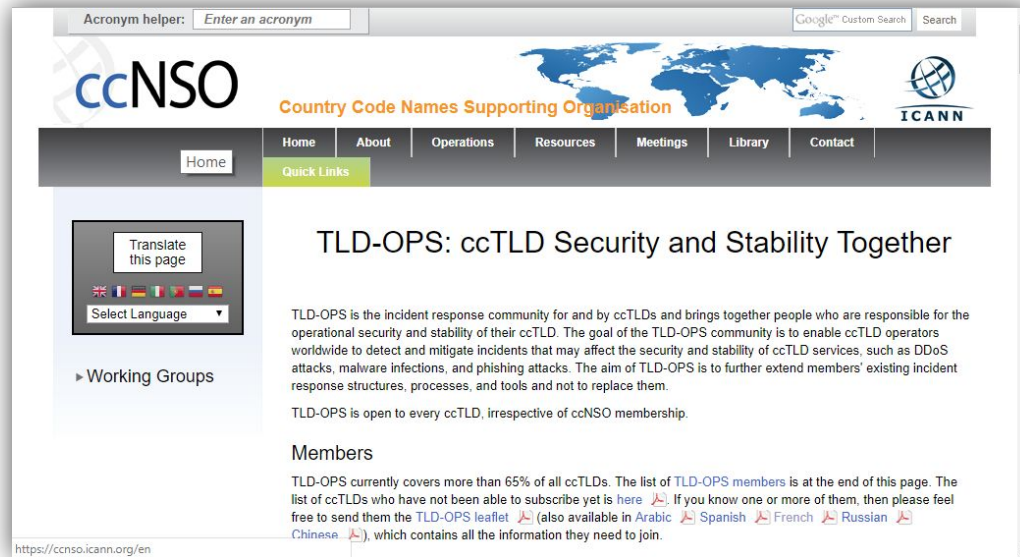




# TLD-OPS Standing Committee



# Ressources & Contacts



<http://ccnso.icann.org/resources/tld-ops-secure-communication.htm>

Jacques Latour  
Standing Committee Chair  
+1.613.291.1619  
jacques.latour@cira.ca



ccTLD Security and Stability Together



Régis Massé  
Standing Committee Vice Chair  
+1.6.83.12.43.49  
regis.masse@afnic.fr



ccTLD Security and Stability Together



TLD-OPS Standing Committee





*ccTLD Security and Stability Together*



**Thank you!**

ccNSO

## TLD-OPS Business Continuity / Disaster Recovery Playbook.



Jacques Latour (.ca)



Régis Massé (.fr)



Alejandra Reynoso (.gt)



Barbara Povše (.si)

# Part 1 - Impact of COVID-19

- ★ Fri 06/Mar - Guatemala declares state of calamity. 🤔
- ★ Wed 11/Mar Exercise: One page Business Continuity Plan. 😎
- ★ Fri 13/Mar - 1st COVID-19 case in Guatemala. 😨
- ★ Mon 16/Mar - Schools and universities closed. 😱
- ★ Tue 17/Mar - All operations are being done remotely. 😐 → 😊
- ★ Documentation is being built: 📜
  - Business Continuity Plan - 76 pages so far 📄
    - Risk Assessment & Management of 18 risks
    - 11 BC Plans - Most likely to happen
    - 4 Protocols
  - Procedures - 51 pages so far 📄

.gt

# Part 2 - Impact of COVID-19

- ★ Information Security Policies for the Registry based on ISO27001
- ★ Tue 17/Dec 19: Registry.si Team used TLD-OPS Playbook - and played a game 🧐
- ★ Thu 27/Feb 20 - 1st BCP: Epidemic
- ★ Fri 13/Mar - Slovenia declares state of calamity.
- ★ Mon 16/Mar - Schools and universities closed.
- ★ Mon 17/Mar - All operations are being done remotely.
- ★ No major issues,  
still developing BCM and different BCPs 📄



## TLD-OPS Business Continuity / Disaster Recovery Playbook.



Jacques Latour (.ca)



Régis Massé (.fr)



Alejandra Reynoso (.gt)



Barbara Povše (.si)



Patricio Poblete (.cl)

Running a ccTLD in crisis mode: from the 2019 political upheaval to the 2020 pandemic.



Pierre Bonis (.fr)

Internet Governance Liaison Committee (IGLC) contribution on capacity building.

# Running a ccTLD in **Crisis** mode: From the political upheaval of **2019** to the pandemic of **2020**



Patricio Poblete  
ccNSO Members Meeting  
ICANN68  
June 24, 2020






**From October 18, 2019,  
people in Chile participated in  
huge protests against social  
inequality and in demand of  
political reforms**

**This lasted  
until the end of the year**

An aerial photograph of a massive crowd gathered in a city street, likely during a protest or march. The crowd is dense and fills the lower half of the frame. In the background, there are several tall buildings, including one with a '4G LTE Claro' sign and another with a 'Canon' sign. A river or canal is visible in the foreground, with a bridge crossing it. The overall scene is one of a large-scale public gathering in an urban setting.

There were many massive  
peaceful marches

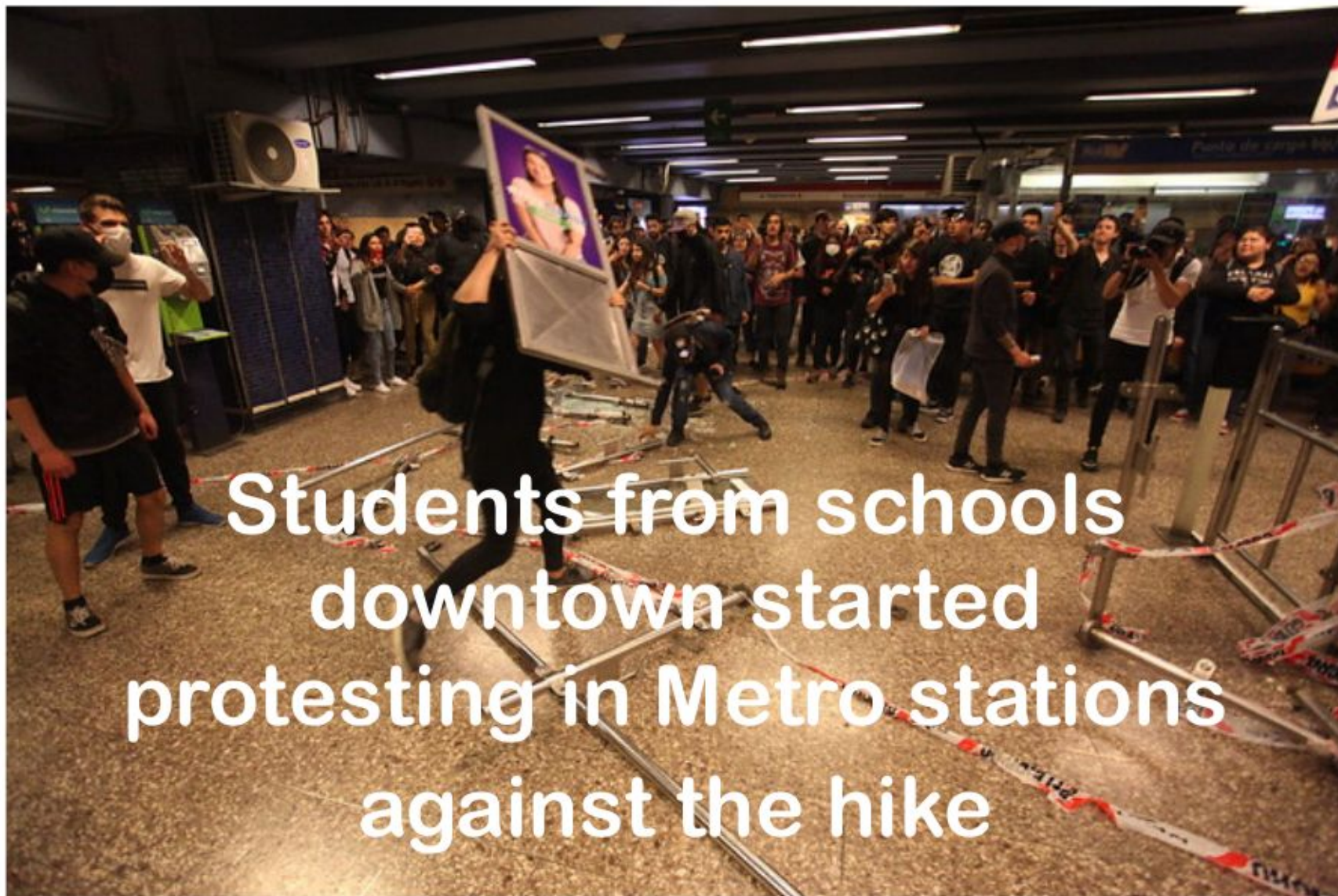


But also  
violent  
protests,  
arson and  
looting



And many cases of police abuse and violation of human rights

**It all started when  
the Metro fare in Santiago  
was raised  
from 800 to 830 pesos  
(an increase of 4 cents US)**



Students from schools  
downtown started  
protesting in Metro stations  
against the hike



Protests were violently repressed by the police



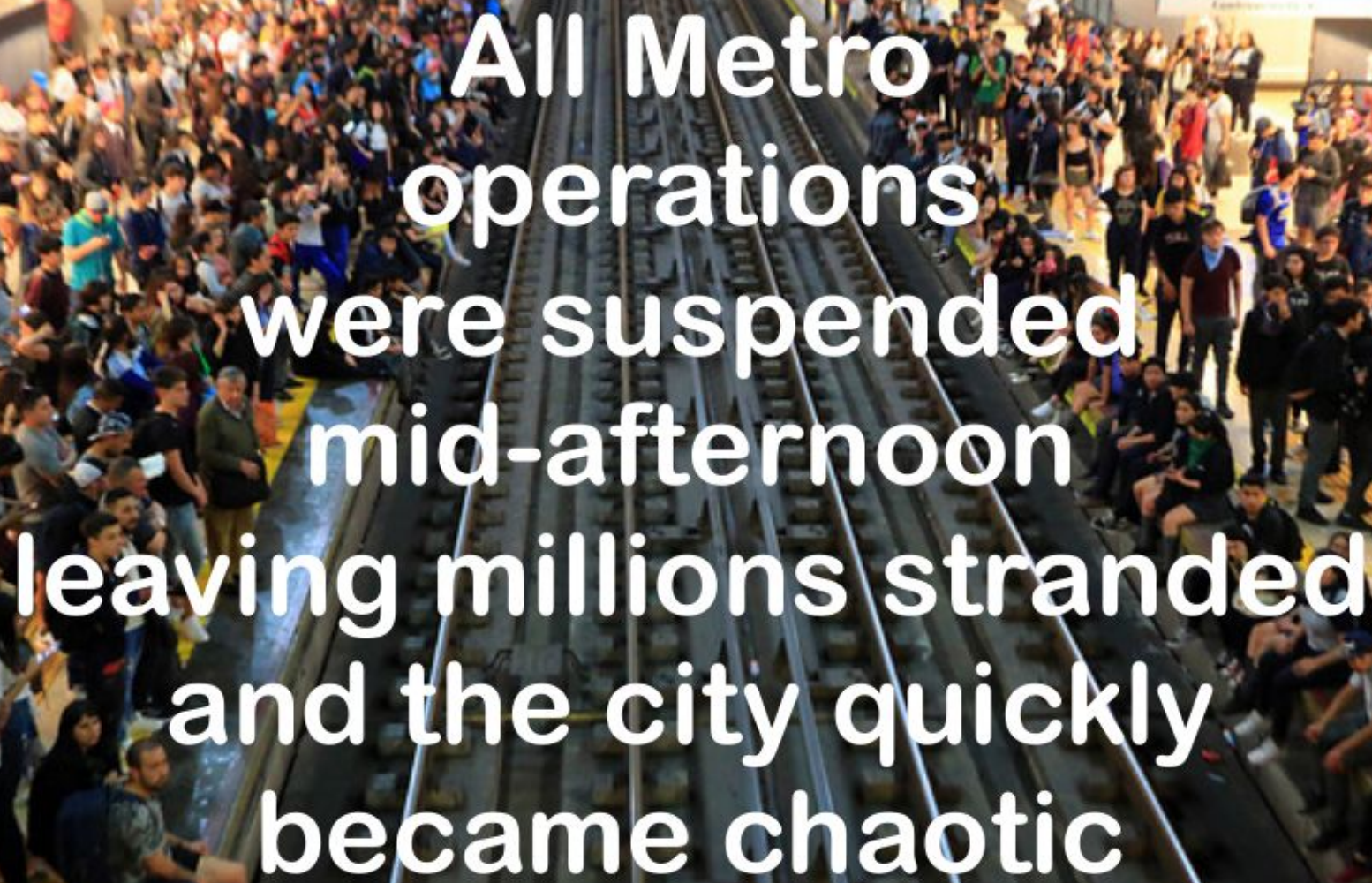




Many turnstiles were  
vandalized

Trains were stopped by people sitting at the edge

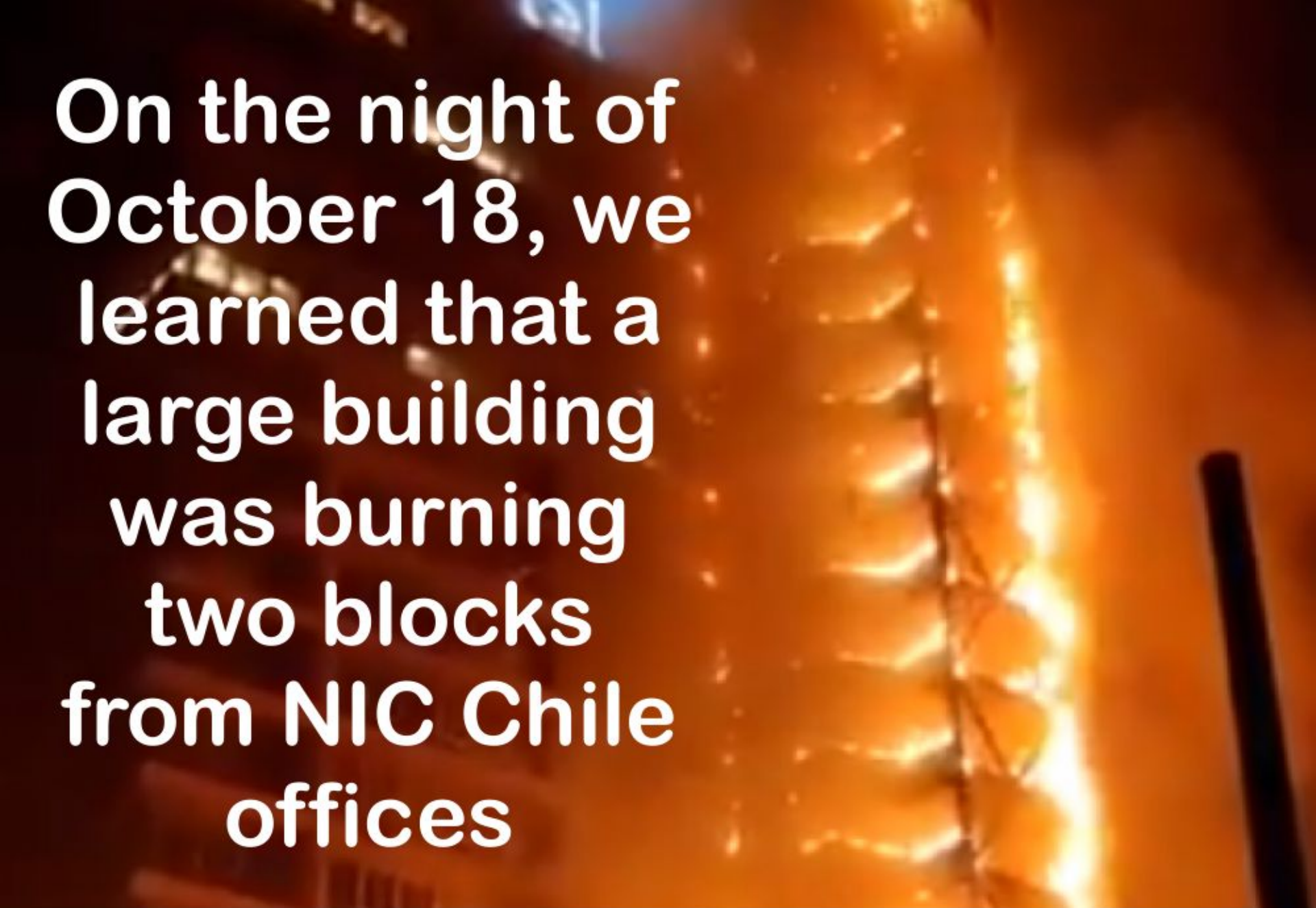


A high-angle photograph of a crowded subway station. The tracks run down the center, flanked by platforms. People are sitting on the floor, some on the tracks, and others are standing. The scene is chaotic and crowded.

All Metro  
operations  
were suspended  
mid-afternoon  
leaving millions stranded  
and the city quickly  
became chaotic

# Dozens of Metro stations were destroyed by fire





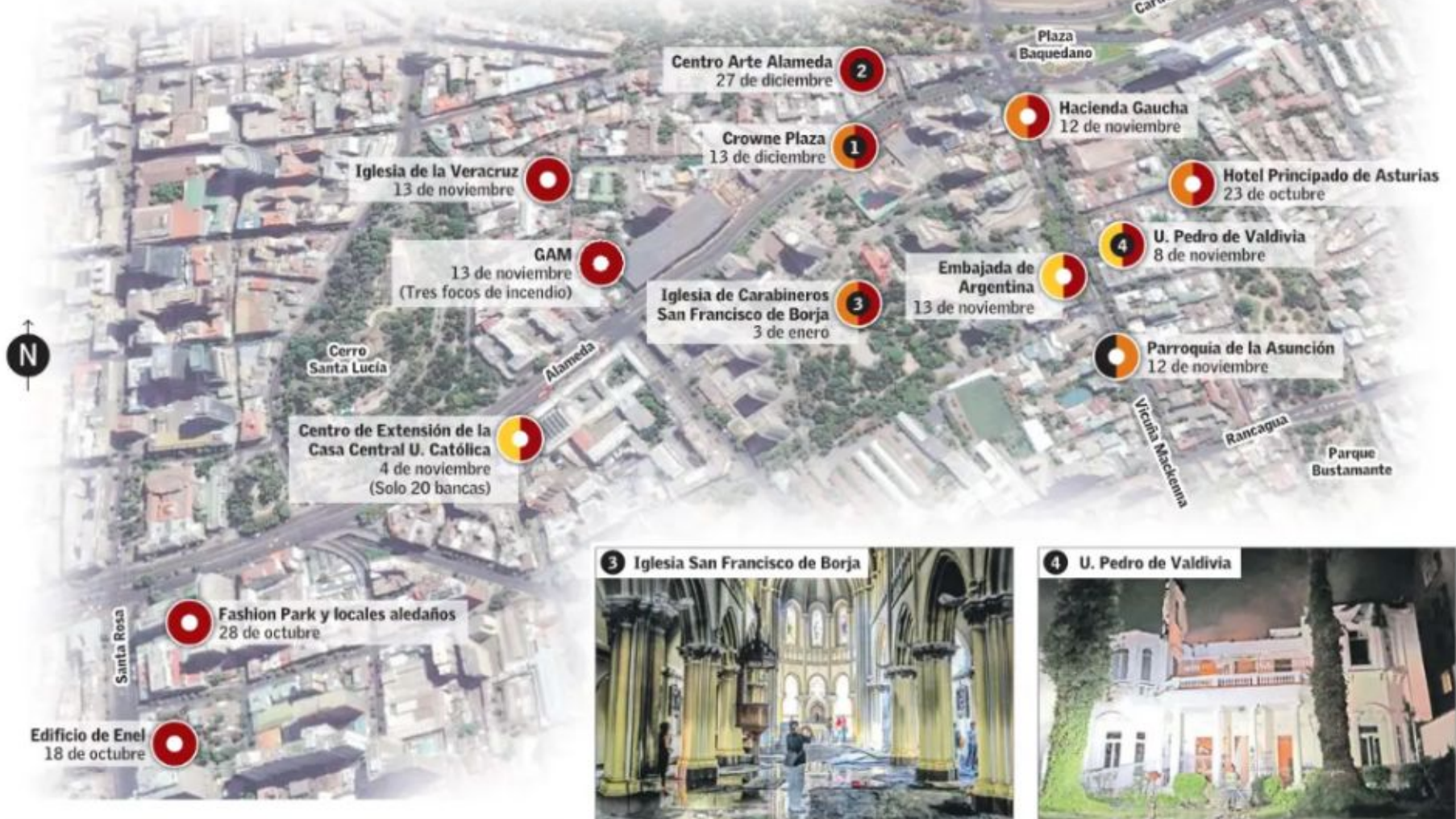
On the night of  
October 18, we  
learned that a  
large building  
was burning  
two blocks  
from NIC Chile  
offices



-  Profanación
-  Destrozos
-  Saqueo
-  Incendio

Fecha del primer incidente

 **U. San Sebastián**  
27 de diciembre  
(Controlaron fuego al interior)

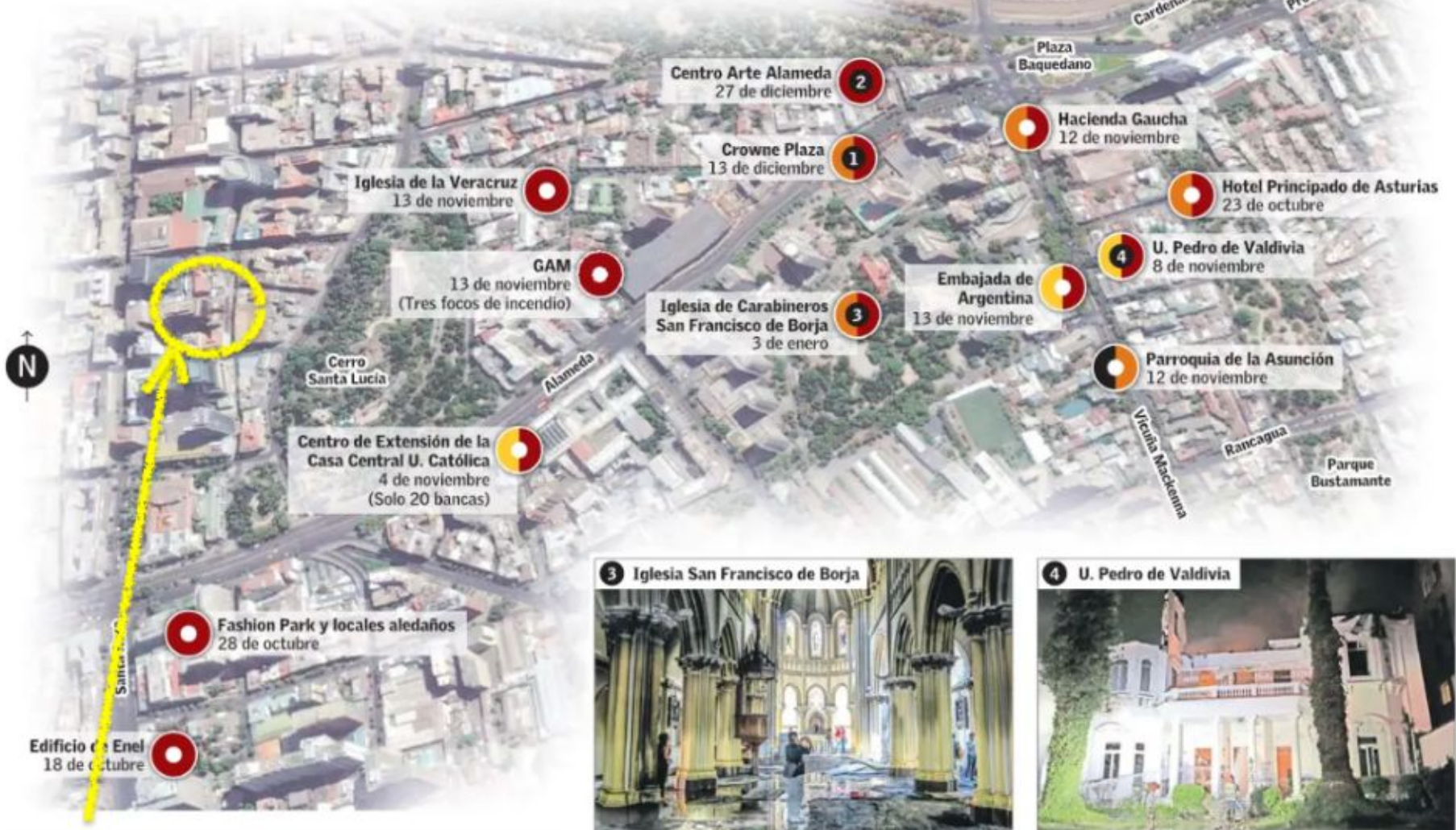





- Profanación
- Destrozos
- Saqueo
- Incendio

Fecha del primer incidente

**U. San Sebastián**  
27 de diciembre  
(Controlaron fuego al interior)





**Our neighborhood often  
resembled a battlefield.**

**Our priorities:  
Keep our people safe  
&  
Keep our services operating  
normally, as much as possible**



# Domain name resolution was not at risk



NIC Chile

Netnod

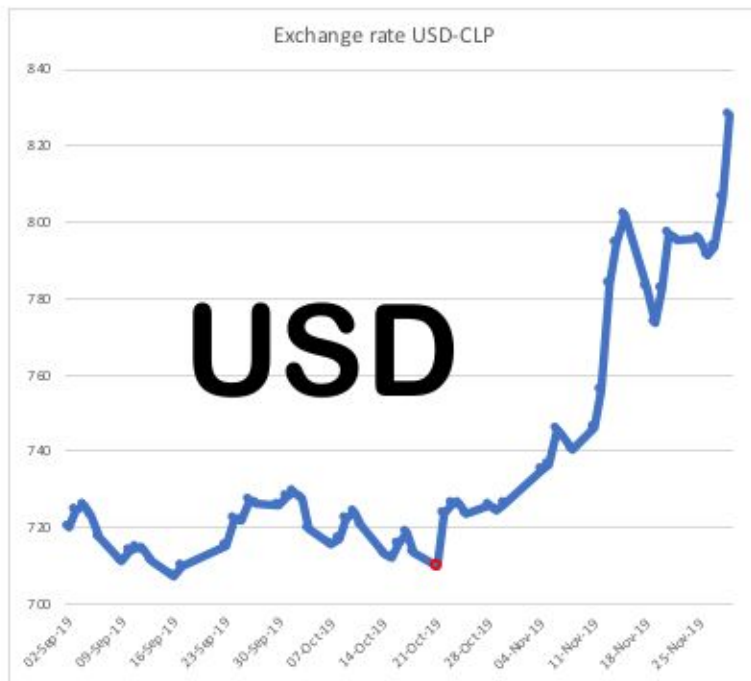
CIRA

PCH

Map data ©2020 Terms of Use

**Registry and registrar services were distributed in several data centers, some outside Santiago**

# The economy felt the impact



**Anticipating customers could have trouble paying for renewals, we temporarily suspended deactivating unpaid domains**

**We dropped that measure after seeing that renewals seemed normal**

**We decided to have most of our staff  
work from home**

**But we were not ready to do it for  
everyone. Some had to come to the office**

**Help desk phones could only be  
answered from the office**

**Accounting transactions had to be filed  
daily and involved submitting paperwork**




Public transportation was unreliable and often unavailable

Some of our staff lived close enough to arrive on foot, if needed

For others, we hired taxi services

Workdays often had to be cut short because of unsafe situations nearby



**We temporarily relocated  
some of our staff involved in  
filing accounting information  
to emergency offices at the  
university campus, far from  
the epicenter of the revolt  
and close to where the  
paperwork needed to be  
submitted**

**Communicating with our users was key**

**We issued almost daily announcements of our hours of help desk operation, through our web site, twitter and Facebook**

**We also reminded them that all online services continued operating normally**

**Good internal communications were also crucial**

STARBUCKS COFFEE

FERIA CHILENA DEL LIBRO

By year end, most businesses had adapted





## **We learned some lessons:**

**When the COVID-19 crisis came, we were much better prepared**

**Our help desk staff could take calls from anywhere with their laptops**

**We had purchased equipment to support work from home for everybody**

**The university administration accepted electronic submissions for (almost) all accounting transactions, and kept improving**

**Very important:  
support people working from home**

**Keep improving their workspaces at home**

**Via Zoom: morning “coffee breaks”  
and afternoon “active breaks” with a  
physical trainer**



**Working at home, juggling domestic tasks and  
homeschooling children is very stressful  
Much more so if close family or friends fall ill**

**We provide psychological counseling for  
everyone who needs it**

**Never let a good crisis go to  
waste**

**You'll be better prepared for  
the next one**

**Thanks!**

## TLD-OPS Business Continuity / Disaster Recovery Playbook.



Jacques Latour (.ca)



Régis Massé (.fr)



Alejandra Reynoso (.gt)



Barbara Povše (.si)



Patricio Poblete (.cl)

Running a ccTLD in crisis mode: from the 2019 political upheaval to the 2020 pandemic.



Pierre Bonis (.fr)

Internet Governance Liaison Committee (IGLC) contribution on capacity building.

# Capacity building : Effects of the lockdown on ccTLDs ?

---

ICANN68 | Pierre Bonis (IGLC Chair)

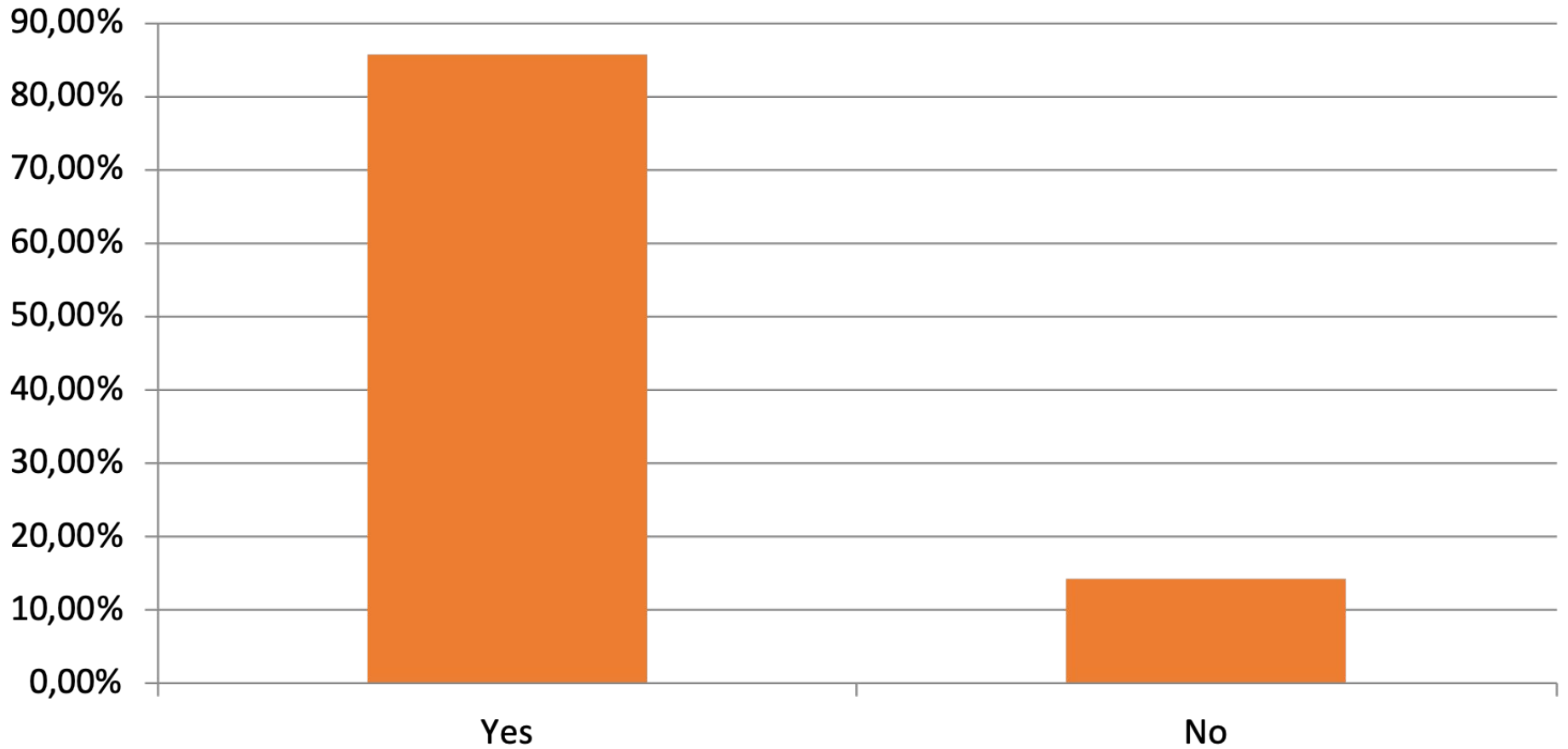
# Which of the IGF topics relevant to ccTLDs are being addressed?



# A quick survey among IGLC members

Answers from AF, AP, EU and NA regions. extracts

## My ccTLD currently performs capacity building activities.





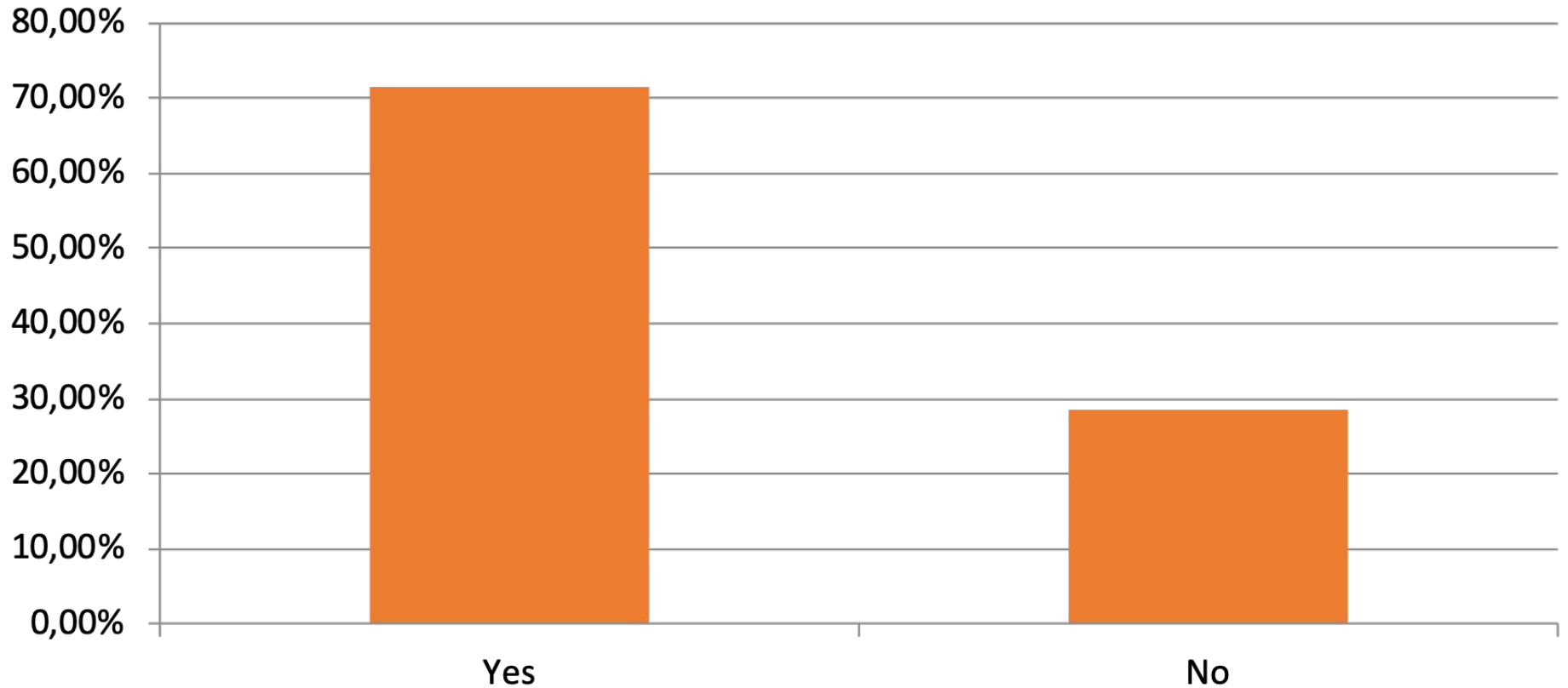
## Why are we into capacity building activities? (some answers)


- It's our mission (in our bylaws).
- It's expected from our stakeholders.
- It's a way to promote the usage of domain names
- to develop commercial services
- allow the staff and the Registry itself to achieve its goals
- To ensure the smooth functioning of the domain name system.

# To whom is it targeted?

- internal staff
- potential future registrants
- government
- registrars
- registrants

## Did you notice an increase in capacity building activities by your registry, during the COVID-19 pandemic?





# Expectations from stakeholders during the crisis (discussion, not in the survey)

- Cybersecurity advices and training
- Online presence (registering, website building...)
- How to fight abuse on the Internet? (especially COVID-19 related)...

# The impact of the lock down

- Obviously, most of in praesentia events were cancelled but :
  - Webinars enormous success
  - Guides, publications from ccTLDs were searched and (sometimes) read.
  - Support had to answer questions in a more “capacity building” approach, and less “technical support”, for those who run a support not only to the registrars but also to the registrants

# Any lessons to learn?

- Greater audience online (huge load for the staff, but easier to attend for the audience).
- In times of fear and questions, ccTLDs are even more seen as a neutral and professional source of expertise (even from the press !)
- How can we build on that ?

You have the  
floor!



## TLD-OPS Business Continuity / Disaster Recovery Playbook.



Jacques Latour (.ca)



Régis Massé (.fr)



Alejandra Reynoso (.gt)



Barbara Povše (.si)



Patricio Poblete (.cl)

Running a ccTLD in crisis mode: from the 2019 political upheaval to the 2020 pandemic.



Pierre Bonis (.fr)

Internet Governance Liaison Committee (IGLC) contribution on capacity building.





[https://www.pepperlaw.com/resources/jpg/blog\\_post\\_photo\\_5231.jpg](https://www.pepperlaw.com/resources/jpg/blog_post_photo_5231.jpg)

**15  
minutes**



Nick Wenban-Smith (.uk)  
Moderator of Panel

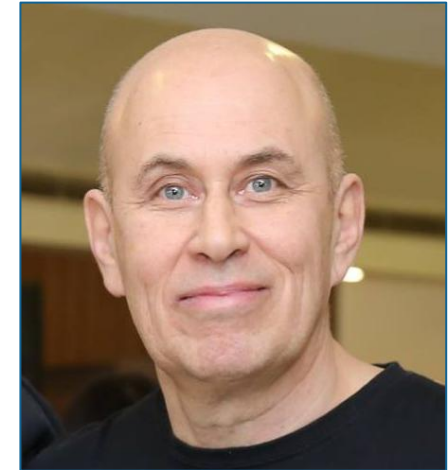


John Crain (ICANN Org.)  
COVID-19 related issues

## Regional Organizations



Barrack Otieno (AFTLD)



Leonid Todorov (APTLD)



Peter Van Roste (CENTR)



Ignacio Estrada (LACTLD)

# DNS Abuse: Introduction and relevance to ccTLDs

It seems obvious, but ...

- What is illegal offline is illegal online
- There are specific examples of use of domain names which are universally agreed as “abusive”\*
  - Phishing
  - Malware distribution
  - Pharming
  - Botnets
  - Spam (when as a vector for the above)
- \*See Internet and Jurisdiction Operational Approaches, Norms, Criteria and Mechanisms

# DNS Abuse: Introduction and relevance to ccTLDs

What is more difficult is when it is alleged that a domain name has been used to commit a crime ...

- In which jurisdiction?
- What type of crime?
- Child Sexual Abuse Material is illegal everywhere, so what is the justification for any ccTLD to tolerate having a domain name associated with such content?
- So now it is ok for the registry to have policies in relation to content ...

# DNS Abuse: Introduction and relevance to ccTLDs

There is no universal standard!

- Incitement to violence, terrorism
- Sales of counterfeit medicines – cures for Covid 19
- Infringement of intellectual property
- Political dissent
- Freedom of expression, criticism of a company or religion
- Propagation of “harmful” material: anti-vaccination

Registries are policing the internet!



# DNS Abuse: Introduction and relevance to ccTLDs

Why is this important for ccTLDs?

- ccTLDs uniquely connect to their countries/ territories
- We pride ourselves on our diversity and independence
- Nobody tells us what to do ...

# DNS Abuse: Introduction and relevance to ccTLDs

Why is this important for ccTLDs?

- We are expected to add value and to protect our communities
- (Especially in times of crisis)
- If we cannot perform some basic functions competently then that opens to the door to a number of undesirable outcomes ...
  - Legislation ...
  - Regulation ...
  - Direct intervention ...
  - Loss of role ...





**ICANN**

**VIRTUAL POLICY FORUM**

**68**

COVID-19, What we see

John Crain

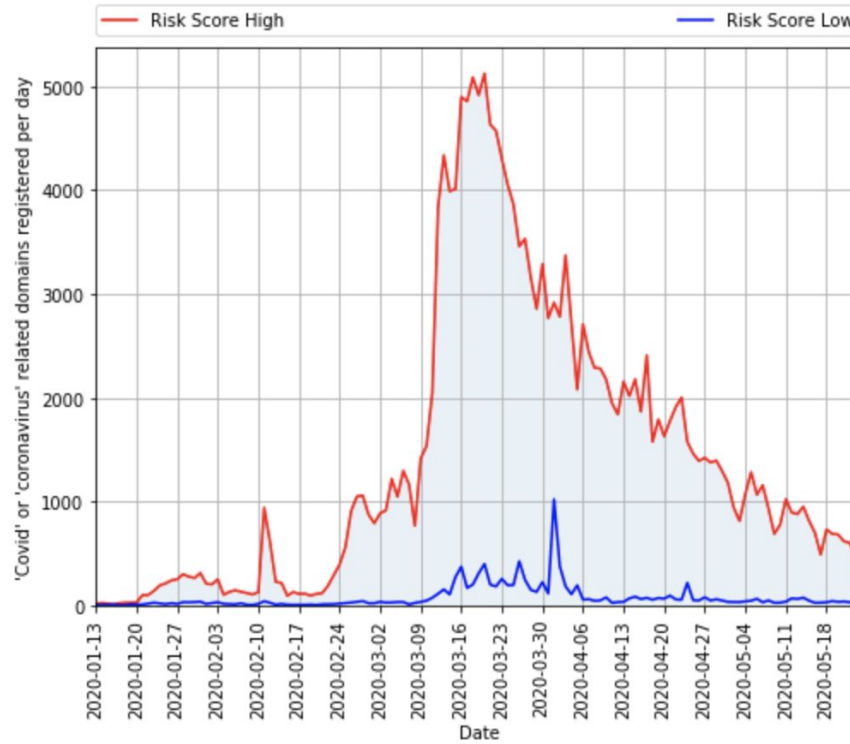
[john.crain@icann.org](mailto:john.crain@icann.org)

ICANN SSR

- Big events have associated bursts of domain name registration
- COVID-19 no different
  - The extra related stress, worry and working from home makes it the perfect storm

TLP: White

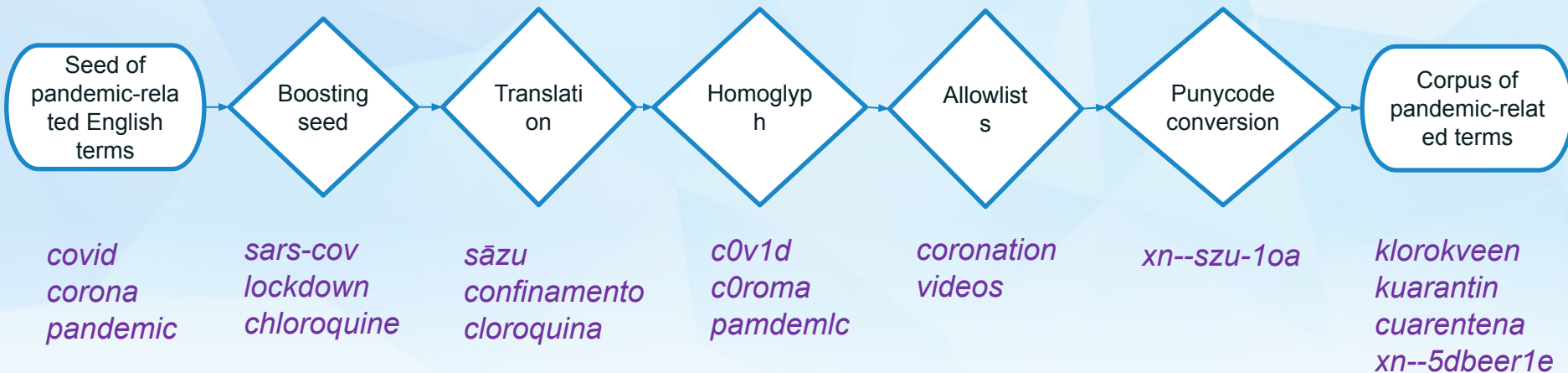
## Domain trends update



(Source: [John Conwell](#), DomainTools)

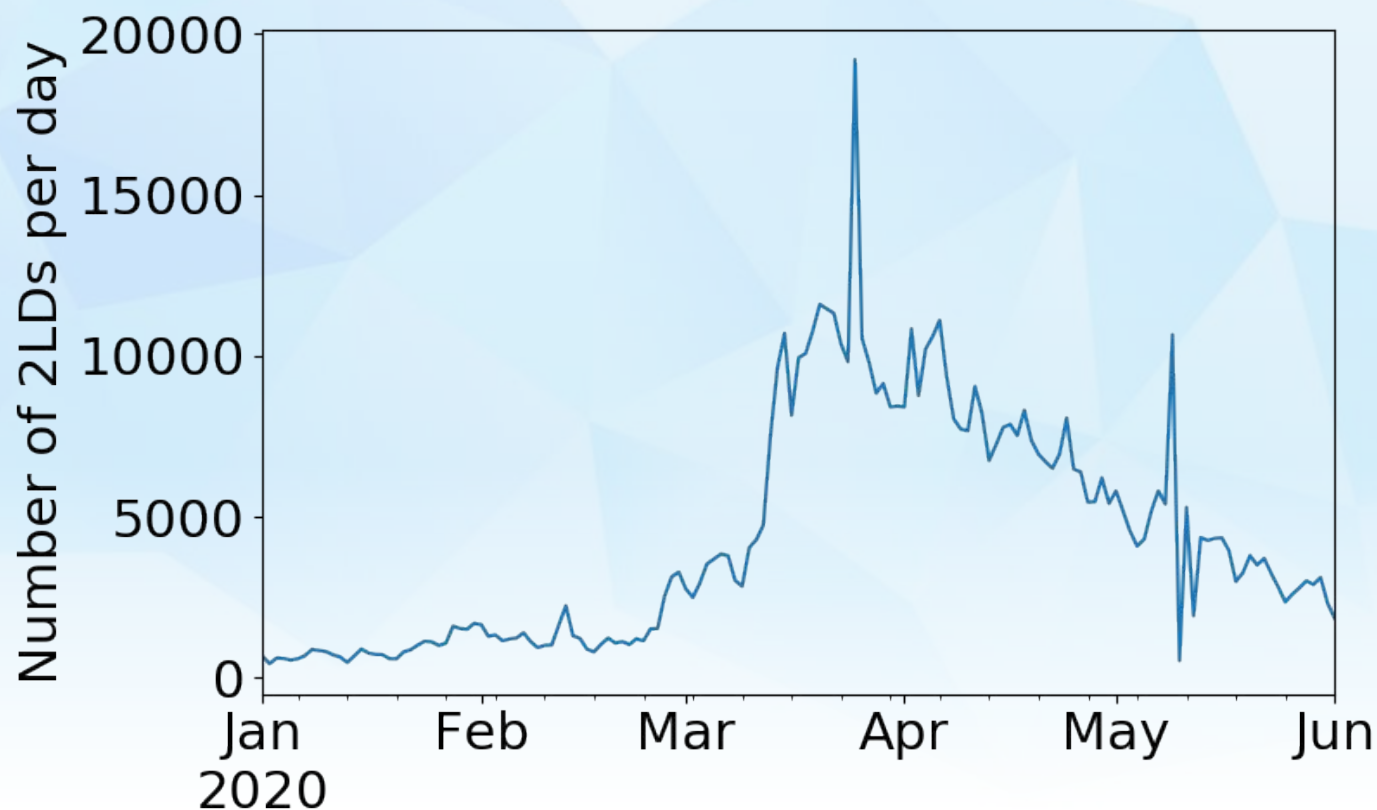
# How does our identification approach work?

- Our approach for identification:
  - Pandemic-related keyword search within zone files (gTLDs + a few ccTLDs)



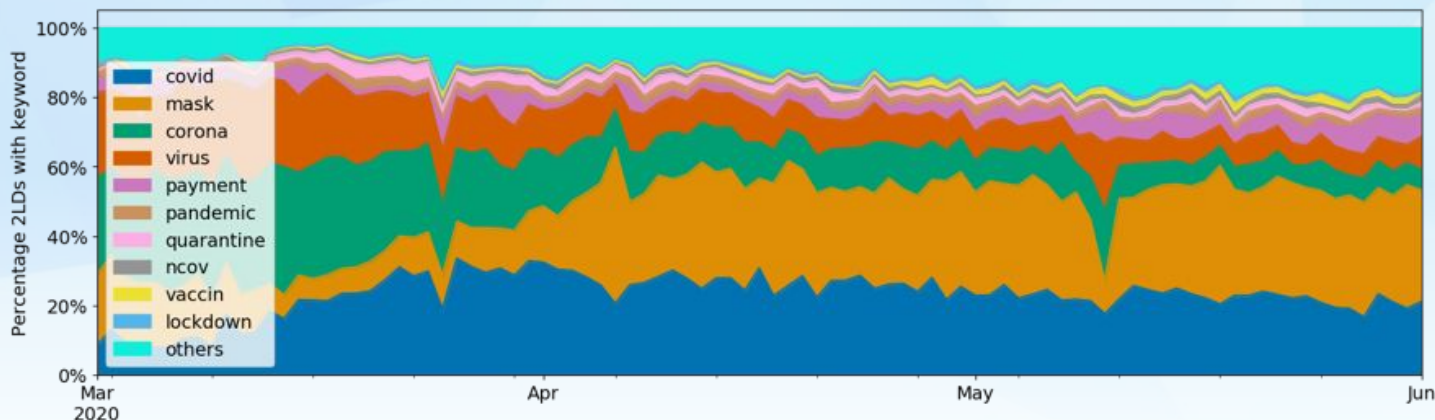
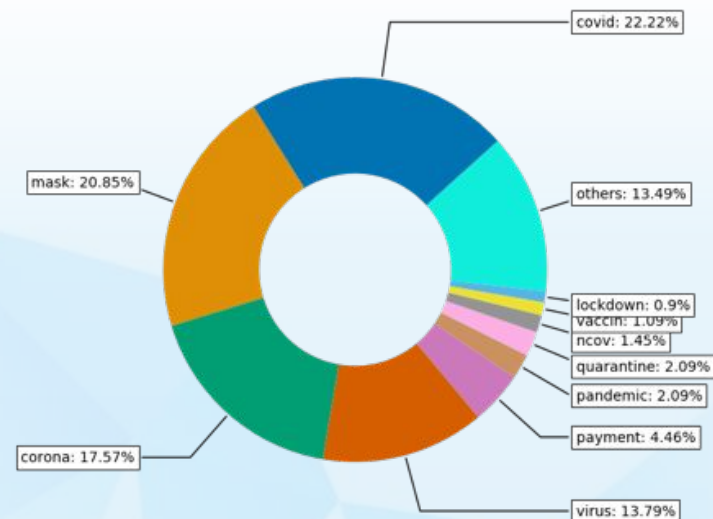
# How many domains have we identified?

- 662,111 domains were identified since January 2020



# What keywords do these domains contain?

- Most of the domains related to 3 keywords
  - 4 keywords account for 73% of the domains
  - Different keywords categories:
    - Disease name (covid, ncov, sars, ...)
    - Pandemic countermeasures (mask, lockdown, quarantine,...)
    - Collateral (zoom, webex, conference, ...)
  - Significant number of domains matches non-English terms



Language	%Domains
English	94,21%
German	2,13%
French	1,26%
Spanish	0,71%
Dutch	0,68%
Turkish	0,59%
Italian	0,14%
Hindi	0,11%
Malay	0,08%
Japanese	0,04%
Portuguese	0,02%
Chinese	0,02%

This is “data”, **not** “intelligence”

There will be benign domains, unrelated domains, defensive registrations, parked domains... along with anything malicious

What **evidence** can we find, do we trust it?

# API calls – VirusTotal



Siôn Lloyd



11 engines detected this domain



Registrar  
undefined

Creation Date  
5 days ago

Last Updated  
5 days ago



Community Score

DETECTION	DETAILS	RELATIONS	COMMUNITY
AlienVault	Malicious		CyRadar Malicious
Emsisoft	Phishing		ESET Phishing
Fortinet	Phishing		G-Data Phishing
Google Safebrowsing	Phishing		Kaspersky Phishing
Netcraft	Malicious		Sophos AV Malicious
Spamhaus	Phishing		ADMINUSLabs Clean
AegisLab WebGuard	Clean		Antiy-AVL Clean
Artists Against 419	Clean		Avira (no cloud) Clean
BADWARE.INFO	Clean		Baidu-International Clean
BitDefender	Clean		BlockList Clean





# API calls - AlienVaultOTX

SUBSCRIBE (40) ADD TO GROUP DOWNLOAD EMBED CLONE SUGGEST EDIT



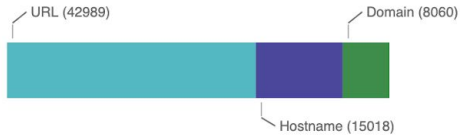
## CCTC Top Indicators

MODIFIED 18 MINUTES AGO by Joshua\_saxe | Public | TLP: Green

GROUPS: COVID19 Cyber Threat Coalition Vetted, CYBSEC-TIA, Public Library Threat Intelligence

Report Spam [Twitter] [Facebook] [Google+] [LinkedIn]

Indicators of Compromise (66067) Related Pulses (2215) Comments (0) History (0)



TYPES OF INDICATORS

Show 10 entries

Search:

TYPE	INDICATOR	TITLE	ADDED	ACTIVE	RELATED PULSES
domain	tempattidurpasien.com		Jun 3, 2020, 2:17:16 PM	●	0
URL	https://t.co/GppF0yYNAN		Jun 3, 2020, 2:17:16 PM	●	1
URL	https://movemycouch.com/404.shtml		Jun 3, 2020, 2:17:16 PM	●	0
URL	http://www.meduchet.com/crm/21138163051d1d676653c26.71326395install...		Jun 3, 2020, 2:17:16 PM	●	0
URL	https://secure.runescape.com-un.ru/m=weblogin/loginform194,533,474,814...		Jun 3, 2020, 2:17:16 PM	●	0

# API calls - phishtank

PhishTank is operated by [OpenDNS](#), a free service that makes your Internet safer, faster, and smarter. [Get started today!](#)

Signed in: [sionlloyd](#) | [My Account](#) | [Sign Out](#)



[Home](#) [Add A Phish](#) [Verify A Phish](#) [Phish Search](#) [Stats](#) [FAQ](#) [Developers](#) [Mailing Lists](#) [My Account](#)

## Submission #6604832 is currently ONLINE

Submitted May 31st 2020 9:02 PM by [N1Antifraude](#) (Current time: Jun 1st 2020 11:17 AM UTC)

https://[REDACTED]



Verified: **Is a phish** [Next unverified phish >](#)

As verified by [paulch](#) [NotBuyingIt](#) [Vasily1](#) [emidaniel](#) [Romantic kiss](#) [PhishKiller73](#)

Is a phish **100%**

Is NOT a phish 0%

[Screenshot of site](#)

[View site in frame](#)

[View technical details](#)

[View site in new window](#)


[Something wrong with this submission?](#)

  
Bancolombia  
Sucursal Virtual Personas

Inicio de sesión

Usuario

Si no tienes un usuario asignado ingresa con tu documento de identidad

 Ingresa tu usuario



# API calls – google safe browsing



## The site ahead contains malware

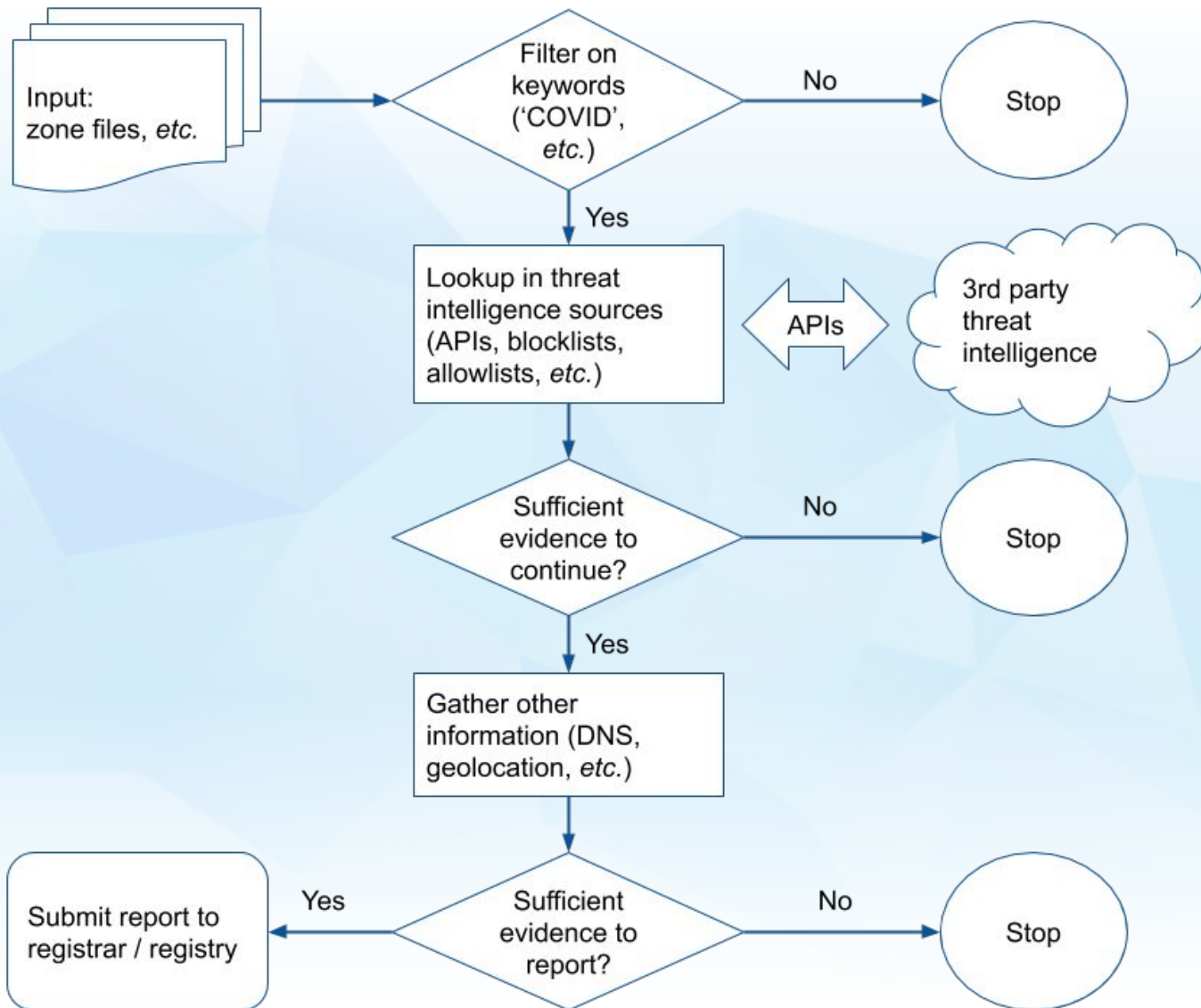
Attackers currently on **malware.testing.google.test** might attempt to install dangerous programs on your computer that steal or delete your information (for example, photos, passwords, messages, and credit cards).

Automatically report details of possible security incidents to Google. [Privacy policy](#)

[Details](#)

[Back to safety](#)

# Reporting Data Flow



Roughly an order of magnitude lost at each gate:

- Thousands of registrations per day
- Some reports on hundreds
- Sufficient evidence on tens

# Conclusion

There is definitely bad stuff out there!

BUT; it is not anywhere near the levels that some figures would suggest



Nick Wenban-Smith (.uk)  
Moderator of Panel

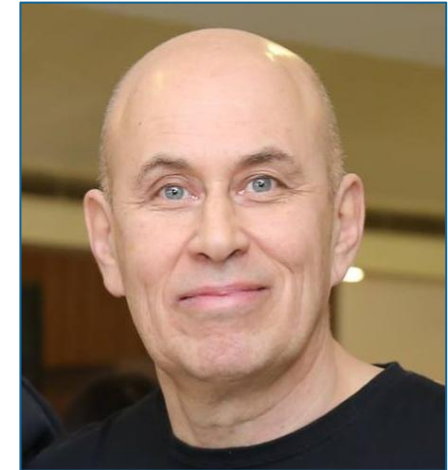


John Crain (ICANN Org.)  
COVID-19 related issues

## Regional Organizations



Barrack Otieno (AFTLD)



Leonid Todorov (APTLD)



Peter Van Roste (CENTR)



Ignacio Estrada (LACTLD)



**ICANN** | **68**  
VIRTUAL POLICY FORUM



**Thank you!**

24 June 2020



[https://cdn.emojidex.com/emoji/seal/female\\_police\\_officer.png](https://cdn.emojidex.com/emoji/seal/female_police_officer.png)

- ★ **Please type your questions/comments in chat:**
  - Please use brackets around your question/comment:
    - **<QUESTION> <QUESTION>**
    - **<COMMENT> <COMMENT>**
  - Text outside these brackets will be considered part of “chat” and will not be read aloud.
  - Chat sessions are archived.
  
- ★ Moderator and remote participation manager will manage the queue.
  
- ★ This meeting is governed under ICANN’s Expected Standard of Behavior:

<http://www.icann.org/en/news/in-focus/accountability/expected-standards>