Review our Expected Standards of Behavior when participating in ICANN Meetings.

Go to:
http://go.icann.org/expected-standards

Review the ICANN Community Anti-Harassment Policy when participating in ICANN Meetings.

Go to:
http://go.icann.org/anti-harassment

Do you have a question or concern for the ICANN Ombudsman?

Email ombudsman@icann.org to set up a meeting.

ICANN

GAC Capacity Building Weekend

Saturday 17 & Sunday 18 September 2022
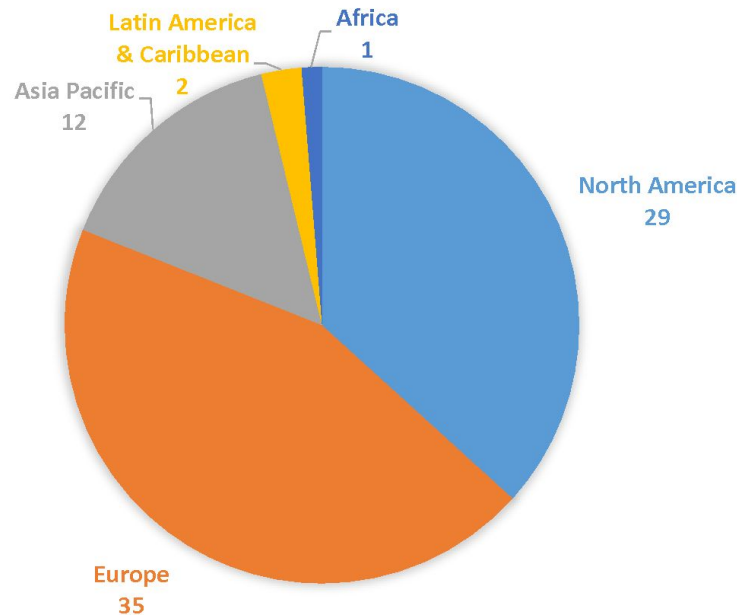
PART 7
DNS Roles and Responsibilities - GNSO Registries

2.6 Registries and Geo TLD Group

Samantha Demetriou, Rysg
Geo TLDs Excom

18 September 2022

I C A N N | G A C
Governmental Advisory Committee

ICANN 75
ANNUAL GENERAL
KUALA LUMPUR

Introduction to the RySG:
A Primer for GAC Members

2.6 Registries Stakeholder Group

Pie chart with the following data:
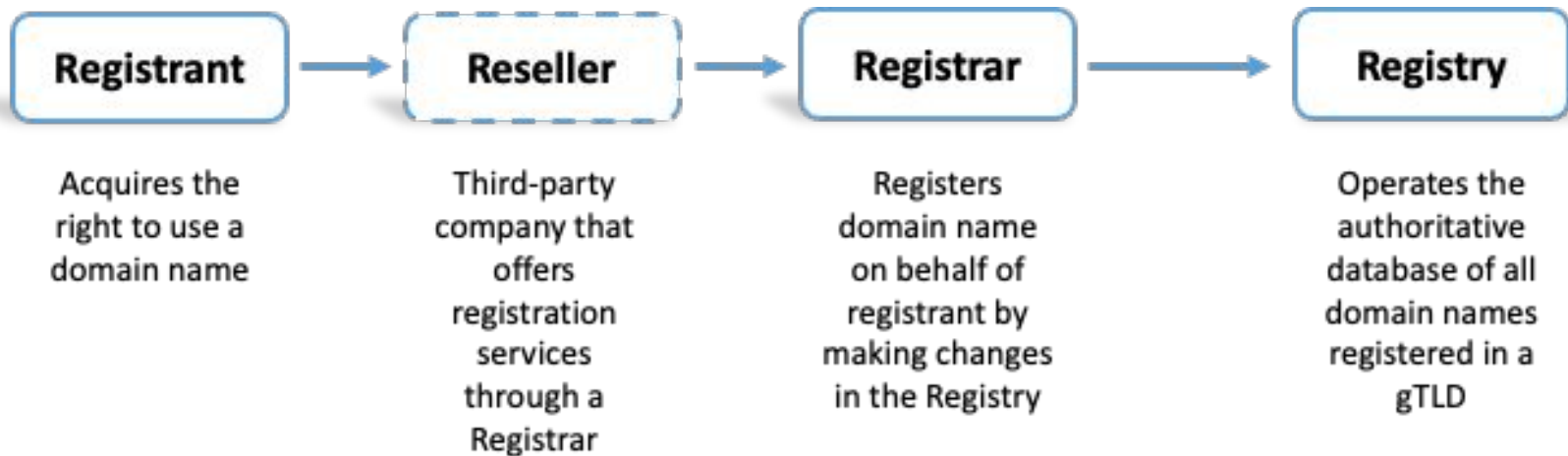- North America: 29
- Europe: 35
- Asia Pacific: 12
- Latin America & Caribbean: 2
- Africa: 1

- The primary role of the RySG is to represent the interests of gTLD registry operators in the ICANN multi-stakeholder community

- All members must have a Registry Agreement with ICANN

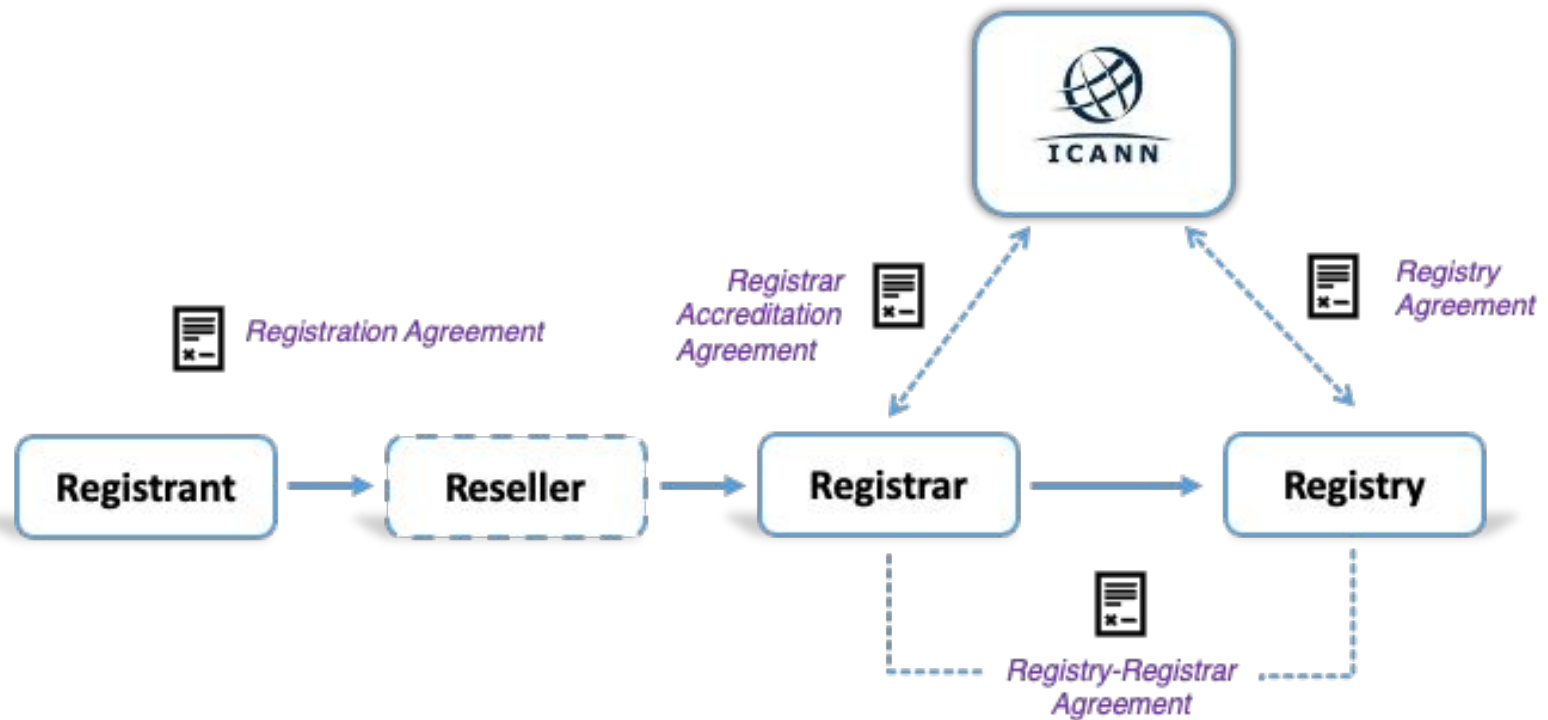- 82 members representing over 600 gTLDs

What is a gTLD Registry?

Registrant	Reseller	Registrar	Registry
Acquires the right to use a domain name	Third-party company that offers registration services through a Registrar	Registers domain name on behalf of registrant by making changes in the Registry	Operates the authoritative database of all domain names registered in a gTLD

What is a gTLD Registry?

gTLD Types and Business Models

Type of gTLD	Examples	Characteristics
Open Generic	.COM, .ORG, .XYZ, .CLUB	No registration restrictions
Niche Market	.DESIGN, .ART, .BOT	Target registrants in a specific market
Verified/Restricted	.BANK, .PHARMACY	Strict registration and verification requirements
Brand	.GOOGLE, .FOX, .AUDI	Only the company and its affiliates may register domains
Geo	.BERLIN, .CAPETOWN, .TOKYO	Support from governments, sometimes have a nexus requirement to register

Registries' Role in the ICANN Community

- Under our Registry Agreements (RA) with ICANN, all gTLD registries agree to abide by existing consensus policies and consensus policies developed in the future

- Compliance with the RA is enforced by ICANN Compliance

- ICANN's Bylaws define what can and cannot be the subject of consensus policies, which is critically important in providing a minimum of business certainty

- ICANN policies and contractual changes often have a direct and material impact on our registry operations and businesses

ICANN
ANNUAL GENERAL
75
KUALA LUMPUR

gTLD Registries and DNS Abuse Mitigation

Domain Name System (DNS) Abuse

Internet Abuse is an overarching and broad problem relating to all aspects of the internet and how it is used, accessed and delivered.

- Abuse on major social media platforms (Facebook, TikTok)
- Abuse of major Marketplaces (Amazon, Ebay etc.)
- Abuse of services (Website creators e.g. Wix or Squarespace, hosting companies, email providers)

DNS Abuse* is a subset of 'Internet Abuse' specifically concerning abuse of the Domain Name System itself.

The Registries Stakeholder Group (RySG) and our members acknowledge our important role in the mitigation of DNS Abuse; however, we cannot alone be seen as a solution to all Internet Abuse

A Registry's role must be appropriate to the abuse identified and our response must be tempered to consider the broader consequences of our actions

*for more info see: https://dnsabuseframework.org/

ICANN ANNUAL GENERAL 75
KUALA LUMPUR

Registry Remediation - Overview

A registry operator has a very limited set of tools we can use to mitigate DNS Abuse*

- Registry actions 'interrupt' the resolution/functioning of the domain
- Most 'common' request is for the 'Suspension' of a domain
- Registry action does **_NOT_** delete, remove or change content
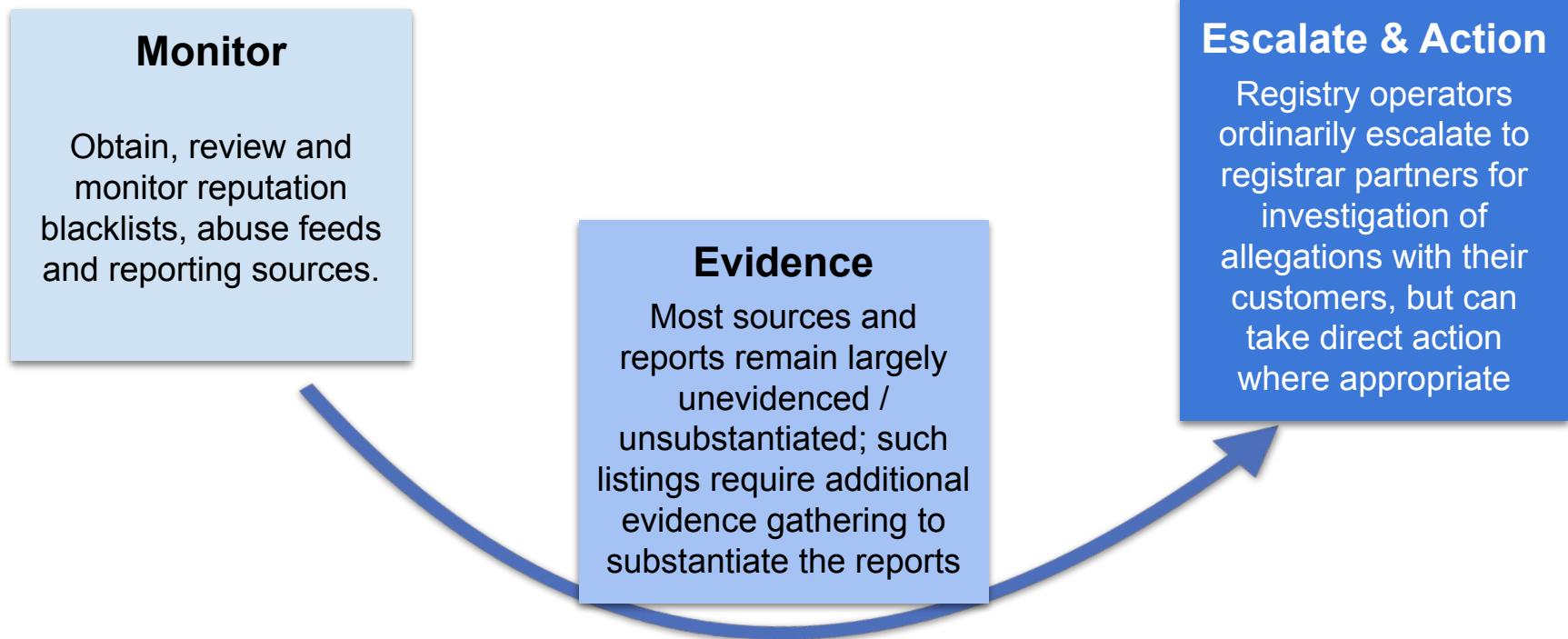- Suspension only removes one means by which content may be accessed

Registry action can have very broad effect :

- Websites (ICANN.org)
- Emails (person@icann.org)
- Applications (e.g. apple.news)
- Platforms (e.g. Facebook, TikTok, Twitter , Amazon, Ebay etc.)

* See RYSG Paper / Internet & Jurisdiction Policy Network Paper on Available Registry Actions)

General Registry DNS Abuse Process

Monitor

Obtain, review and monitor reputation blacklists, abuse feeds and reporting sources.

Evidence

Most sources and reports remain largely unevidenced / unsubstantiated; such listings require additional evidence gathering to substantiate the reports

Escalate & Action

Registry operators ordinarily escalate to registrar partners for investigation of allegations with their customers, but can take direct action where appropriate

Evolving Understanding & Efforts

RySG / CPH resources for review

- Framework on Domain Generating Algorithms (DGAs) Associated with Malware and Botnets
- CPH Guide to Abuse Reporting
- Trusted Notifier Framework

Supported Third Party Initiatives

- Internet and Jurisdiction Policy Network (https://www.internetjurisdiction.net/)
- Top DNS (https://international.eco.de/topics/names-numbers/topdns/)
- DNS Abuse Institute (https://dnsai.org)
- NetBeacon - (https://netbeacon.org/)

Current efforts underway

- Spec 11(3)b Voluntary reporting (with ICANN invitees soon)
- Malicious vs Compromised work (SSAC and ccNSO invitees)

ICANN 75
ANNUAL GENERAL
KUALA LUMPUR

ICANN - 4 year retrospective on DNS Abuse
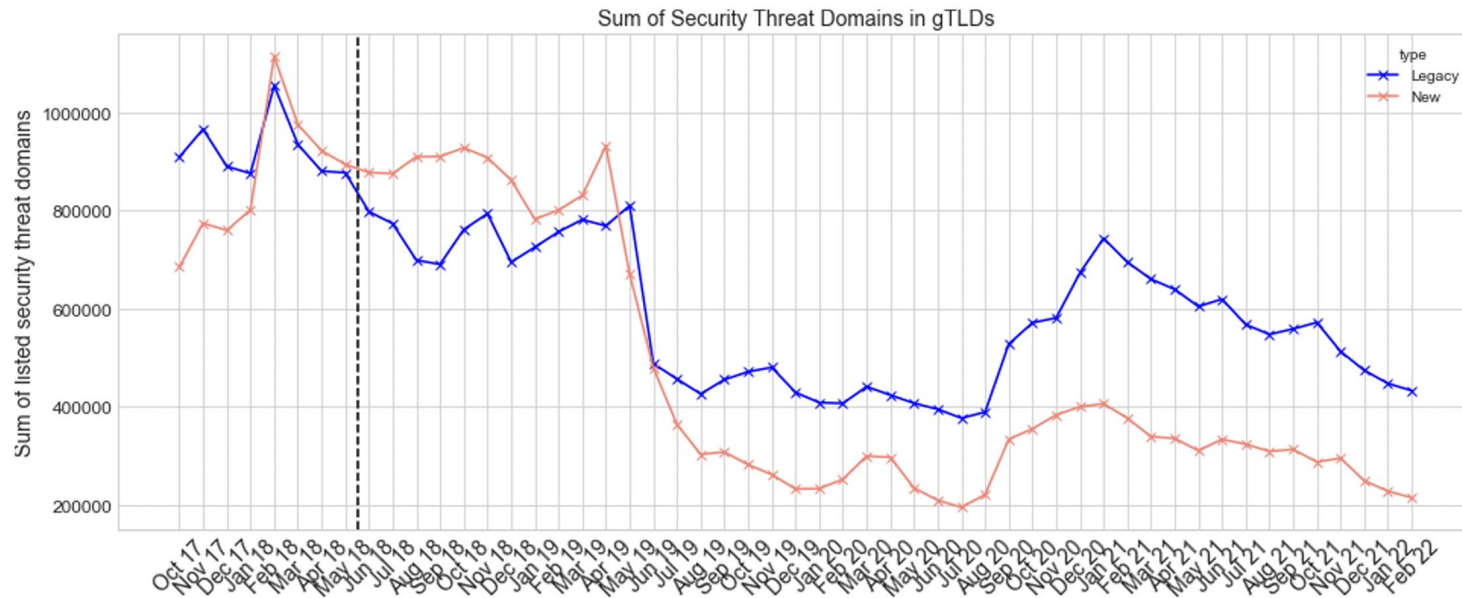

Sum of Security Threat Domains in gTLDs

Figure 2 - Sum of absolute counts of security threat domains across threat gTLD types over time

Source: https://www.icann.org/en/system/files/files/last-four-years-retrospect-brief-review-dns-abuse-trends-22mar22-en.pdf

ICANN | GAC

| 15

2.6 Registries Stakeholder Group

Please reach out with any questions!

Samantha Demetriou, Chair: sdemetriou@verisign.com

Beth Bacon, Vice Chair Policy: beth@pir.org

Alan Woods, Vice Chair Administration: alan@identity.digital

Karen Day, Treasurer: karen.day@sas.com

2.6 Geo TLD Group

Promoting local digital Identities for
Cities, Regions, Languages and Cultures on the Internet

GAC Capacity building workshop
ICANN75 - Sunday 18 September

2.6 Geo TLD Group

the **geoTLD.group** represents the interests of geographic top-level domains representing a city, region, language or culture.

the geoTLD.group is member of the Registries Stakeholder Group within ICANN

the geoTLD.group is an international not-for-profit membership association

geoTLD.group members

[Europe] .alsace .amsterdam .barcelona .bayern .berlin .brussels .bzh .cat .cologne .eus .frl .gal .hamburg .koeln .london .madrid .nrw .paris .ruhr .saarland .scot .stockholm .swiss .tirol .vlaanderen .wien
[Africa] .africa .capetown .durban .joburg
[America] .boston .miami .nyc .quebec
[Asia Pacific] .melbourne .sydney .tokyo

2.6 Geo TLD Group

2.6 Geo TLD Group

geoTLDs

digital Identities for
Cities, Regions, Languages and Cultures on the Internet

geoTLDs belong to the gTLDs
per ICANN Registy contract geoTLDs are bound to the policies set by the
ICANN community

the typical geoTLD is operated on behalf of their local government (by
contract or formal assignment) or with the explicit support (letter of support)
of a local/relevant government

Proximity
there are 69 geoTLDs delegated, characterised by the **proximity** to the
community they serve

2.6 Geo TLD Group

DNS Abuse: responsible management by geoTLDs

Contractual obligations and local cooperation
- per ICANN contract geoTLDs actively monitor for DNS abuse cases
- many are also community TLDs
  - Specification 12 Registry Agreement (eligibility requirements, usage restrictions and proactive enforcement)
- several geoTLD Registry operators have additional obligations or agreements with their local government

low number of abuse cases reported by geoTLD.group members

< 0'01% of total number of registered names. Mostly infections undetected by registrant

Proximity!
- smaller zones - less attractive for wrongdoers
- due to their specific local character 'weird' registrations easily stand out
- some geoTLDs require a presence or existing link with their community
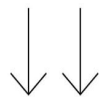- geoTLD Registries invested in the prestige of their communities

ICANN
ANNUAL GENERAL
75
KUALA LUMPUR

2.6 Geo TLD Group

PUNTU .EUS

We have working agreements with the **Basque Government** official Cybersecurity institutions: **Basque Cybersecurity Center** (developing strategies to enable protection for .EUS) and **IZENPE** (free official SSL certificate for he .EUS domain names). Active members of the **Cybersecurity Basque Cluster** and the **Global Cyber Alliance**.
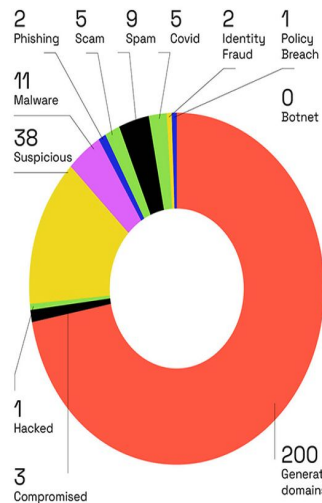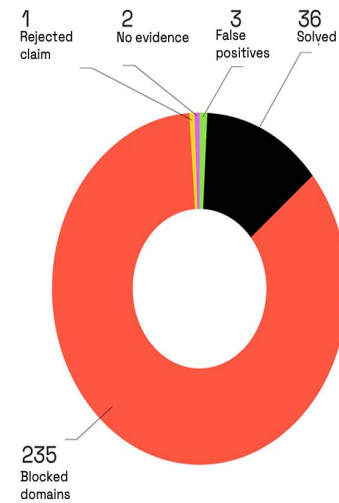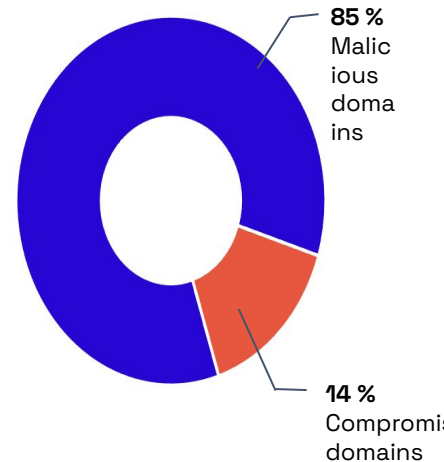
DETECTED RISKS

277

0.02% of 13.083 DUM

CASES DETECTED BY TYPE

2 Phishing
5 Scam
9 Spam
5 Covid
2 Identity Fraud
1 Policy Breach
0 Botnet
11 Malware
38 Suspicious
1 Hacked
3 Compromised
200 Generated domains

CASE RESOLUTION BY TYPE

1 Rejected claim
2 No evidence
3 False positives
36 Solved
235 Blocked domains

MALICIOUS vs COMPROMISED

85 % Malicious domains

14 % Compromis[ed] domains

WHAT DO WE DO?

Our main task is to ensure your digital security. Using the Abuse IQ system we continuously monitorize .EUS websites. As a result, we detect bad behaviours on the web pages and anticipate risks and threats.

We block the **malicious domain names.** These are domain names registered with bad intent.

We help fix **compromised domain names.** These are domain names attacked by a third party.

CYBERSECURITY REPORT 2021

ICANN ANNUAL GENERAL **75** **KUALA LUMPUR**

Stéphane Bondallaz

La lutte contre la cybercriminalité au travers des noms de domaine Internet en droit suisse

Les mesures qui peuvent être prises à l'égard des noms de domaine Internet sont essentielles pour lutter contre la cybercriminalité. Si cette lutte ne trouve pour l'heure qu'un appui limité dans les instruments internationaux, le droit suisse des noms de domaine prévoit des mesures efficaces avant tout contre le « phishing » et la diffusion de « malware ». Une protection au travers des noms de domaine contre des atteintes illicites peut par ailleurs être mise en œuvre dans le cadre de procédures administratives ou judiciaires ordinaires de droit suisse.

Catégories d'articles : Contributions
Domaines juridiques : Droit administratif

[26] Il convient de signaler que l'enregistrement et/ou l'utilisation abusive de noms de domaine en violation de droits attachés à des signes distinctifs peuvent être soumis au service de règlement des différends prescrit par l'ODI pour le ccTLD « .ch » (art. 45 al. 2 ODI et 28 al. 3 LTC)[33] et à ceux imposés par l'ICANN pour le gTLD « .swiss » (art. 14 al. 1 ODI), services qui ont développé un corpus juridique particulier de droit international des marques applicable aux noms de domaine[34].
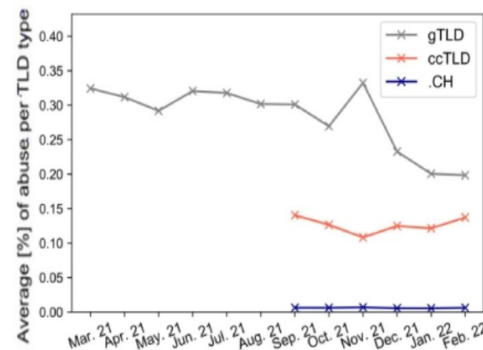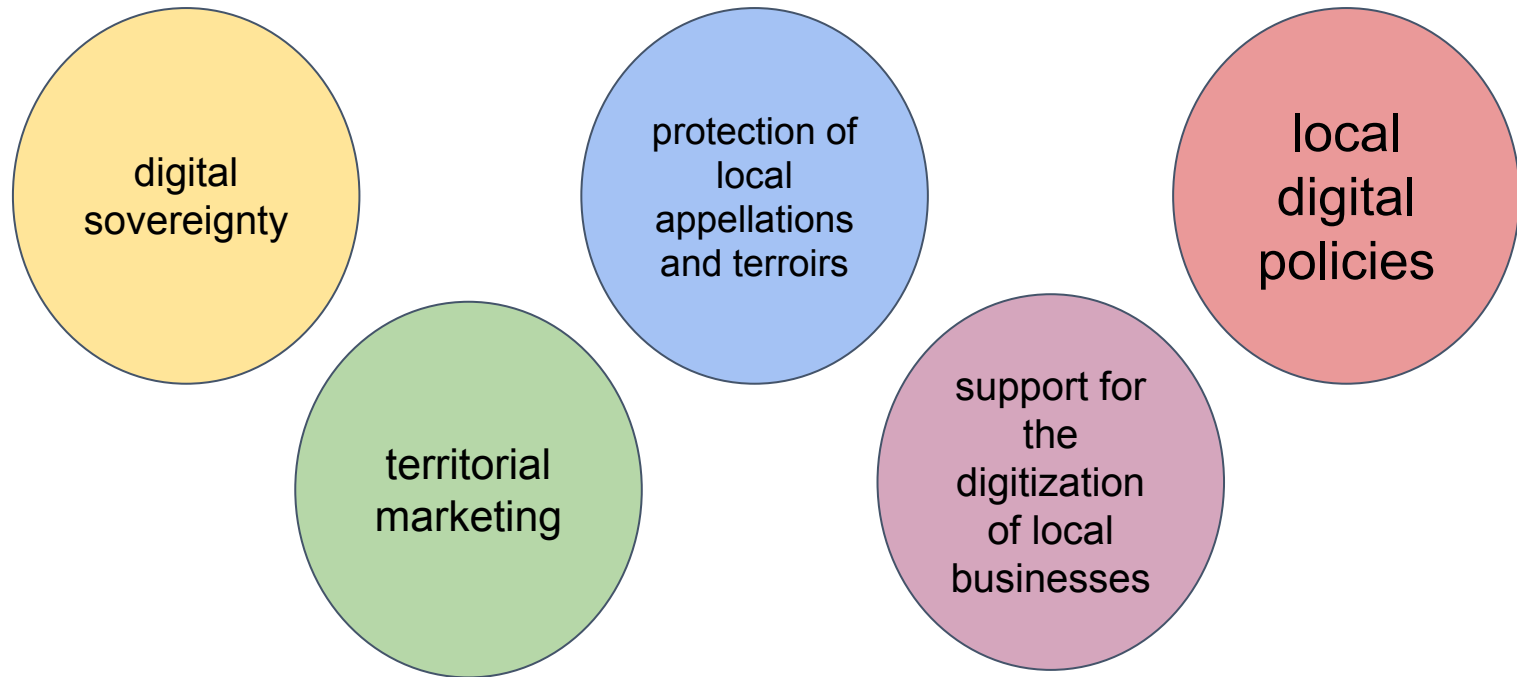
5. Conclusion

[60] Le Conseil fédéral s'est montré extrêmement diligent et novateur en développant dans l'ODI un arsenal d'outils et de mesures qui permettent une lutte efficace et rapide contre la cybercriminalité dans les domaines Internet gérés par la Confédération. Les domaines « .ch » et « .swiss » figurent ainsi parmi les plus sûrs au monde, ce qui contribue à renforcer la confiance des usagers dans les contenus et services en ligne qui y sont accessibles.

Opportunities : next round

Local public authorities are waiting for the next round

digital sovereignty

territorial marketing

protection of local appellations and terroirs

support for the digitization of local businesses

local digital policies

2.6 Geo TLD Group

Thank you for your attention!

website www.geoTLD.group

contact office@geoTLD.group

Join our community outreach session!

DNS Abuse: Responsible management by geoTLDs

Wednesday 21 September, 09:00 MYT (UTC+8)

Conference Hall 1

ICANN
ANNUAL GENERAL 75
KUALA LUMPUR