

# Fraud detection at EURid, an overview

ccNSO TechDay

2021.06.14

Jordi Iparraguirre

# Why is EURid into this?

We strive for a trusted  
.eu space

for users, businesses  
& consumers



# Basic framework

- We do not host content
- We do not want to be the resource used for causing harm
- We are not the police/judge of the Internet
- We verify registrant's Whois data
- But, can we walk an extra mile? → Prevent and mitigate abuse

If we are not the  
police/judge of the  
Internet, how can we  
prevent abuse?

What is abuse?



## Orange Extra Card

Increase the Welcome Interest of your Orange Accounts to %19 with Orange Extra!

[> Learn More](#)



19%  
Welcome Interest for  
ORANGE EXTRA

20%  
discount at  
ENUYGUN

20%  
discount at  
TRENDYOL



### Market Snapshot

Closing Change



### Calculator

- > Loan Calculator
- > ING Orange Calculator
- > Deposit Interest Calculator
- > Currency Converter

### 24 / 7 Banking

- > Online Banking
- > Mobile Banking
- > Telephone Banking
- > ATM
- > Instant PIN



Votre espace particulier

Votre espace professionnel

Accueil > Particulier > Formulaire de remboursement électronique - N 0062405129

### Confirmer vos informations

Nom complet ?

Prénom

Nom

Date de Naissance

Jour

Mois

Année

Adresse ?

Adresse



Code Postal

Téléphone ?

Mobile



### Vos coordonnées bancaire

Votre banque :

Choisissez votre banque

Valider

Un site de la direction générale des Finances publiques

we ship worldwide

TO ALL COUNTRIES & ALL DESTINATIONS

get free bonus

4 FREE VIAGRA PILLS FOR EVERYONE

Erection Powerpack  
only for

**\$74.95**

10 pills Viagra + 10 pills Cialis

Hurry up, time limited offer



BESTSELLERS

- ▶ Viagra
- ▶ Cialis
- ▶ Viagra Super Active+
- ▶ Levitra
- ▶ Viagra Professional
- ▶ Amoxicillin
- ▶ Viagra Super Force
- ▶ Pink Female Viagra
- ▶ Zithromax
- ▶ Cialis Super Active+
- ▶ Propecia
- ▶ Lasix
- ▶ Prednisolone
- ▶ Clomid
- ▶ Prozac
- ▶ **Cialis Professional**

- ANTI-ALLERGIC/ASTHMA
- ANTI-BIOTICS
- ANTI-DEPRESSANTS
- ANTI-DIABETIC
- ANTI-VIRAL
- ANXIETY/SLEEP AID
- BLOOD PRESSURE/HEART
- CANCER
- CHOLESTEROL
- EYE CARE
- GENERAL HEALTH
- MEN'S HEALTH
- MENTAL HEALTH/EPILEPSY
- PAIN RELIEF
- PETS
- SKIN CARE
- STOMACH
- STOP SMOKING
- VITAMINS/HERBAL SUPPLEMENTS
- WEIGHT LOSS
- WOMEN'S HEALTH

Limited period offer till stocks last

 <b>25% off</b> Viagra Erectile Dysfunction, Male Enhancement, Erection €1.03 <b>€0.77</b> <a href="#">ORDER NOW</a>	 <b>20% off</b> Cialis ED, Erectile Dysfunction, Erection €1.70 <b>€1.43</b> <a href="#">ORDER NOW</a>	 <b>15% off</b> Viagra Super Active+ Erectile Dysfunction, Male Enhancement, Erection €2.70 <b>€2.30</b> <a href="#">ORDER NOW</a>	 <b>10% off</b> Levitra Erectile Dysfunction, Erection, ED €2.02 <b>€1.82</b> <a href="#">ORDER NOW</a>
---	---	---	--

Most Popular Products

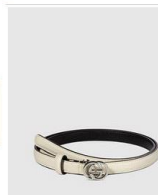
 Viagra Professional Erectile Dysfunction, Male Enhancement, Erection <b>€0.65</b> <a href="#">ORDER NOW</a>	 Amoxicillin Antibiotic, Bacterial Infections <b>€0.45</b> <a href="#">ORDER NOW</a>	 Viagra Super Force Erectile Dysfunction, Male Enhancement, Erection <b>€3.83</b> <a href="#">ORDER NOW</a>	 Pink Female Viagra Female Enhancement, Female Libido, Decreased Libido <b>€0.65</b> <a href="#">ORDER NOW</a>
 Zithromax Bacterial Infections <b>€0.68</b> <a href="#">ORDER NOW</a>	 Cialis Super Active+ ED, Erectile Dysfunction, Erection <b>€2.69</b> <a href="#">ORDER NOW</a>	 Propecia Hair Loss, Male Pattern Baldness, Androgenetic Alopecia <b>€0.50</b> <a href="#">ORDER NOW</a>	 Lasix Diuretic, Heart Failure, Edema <b>€0.26</b> <a href="#">ORDER NOW</a>
 Prednisolone Asthma, Uveitis, Psoriasis, Gangrenosum <b>€0.32</b> <a href="#">ORDER NOW</a>	 Clomid Ovulatory Failure, Induce Ovulation, Ovarian Stimulation <b>€0.68</b> <a href="#">ORDER NOW</a>	 Prozac Depression, Antidepressant, Obsessive-Compulsive Disorder <b>€0.44</b> <a href="#">ORDER NOW</a>	 Cialis Professional ED, Erectile Dysfunction, Erection <b>€4.26</b> <a href="#">ORDER NOW</a>



## CATÉGORIES

- Gucci Femme écharpes Et Foulards
- Gucci Femme Ceintures
- Gucci Femme Chaussures
- Gucci Femme Joaillerie
- Gucci Femme Lifestyle
- Bags & Luggage
- Gucci Femme Montres
- Gucci Femme Petite
- Maroquinerie
- Gucci Femme Portefeuilles
- Gucci Femme Sacs à Main
- Gucci Homme Ceintures
- Gucci Homme Chaussures
- Gucci Homme Cravates

## Promotions du mois de février



370552 AP00N 9022 Ceinture  
Fine En Cuir Avec Boucle  
Double G  
~~€220.72~~ **€84.55**  
Economie : 62%



309900 BMJ1G 9022 Ceinture  
Très Fine Microguccissima  
Avec Boucle éperon  
~~€233.18~~ **€84.55**  
Economie : 64%



282349 A150N 7523 Ceinture  
Fine En Cuir Verni Avec  
Boucle Motif  
~~€240.30~~ **€84.55**  
Economie : 65%



309900 BMJ1G 1000 Ceinture  
Très Fine Microguccissima  
Avec Boucle éperon  
~~€186.90~~ **€84.55**  
Economie : 55%

## Produits Phares

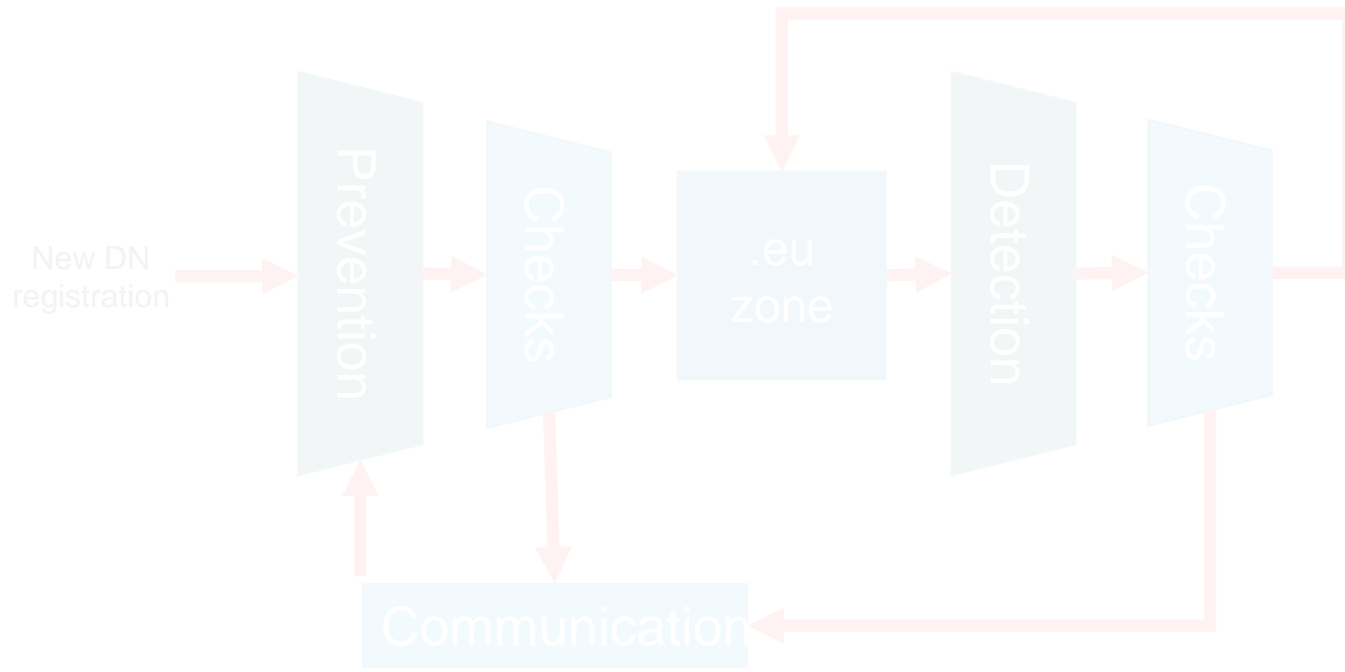


Prevent and mitigate  
abuse

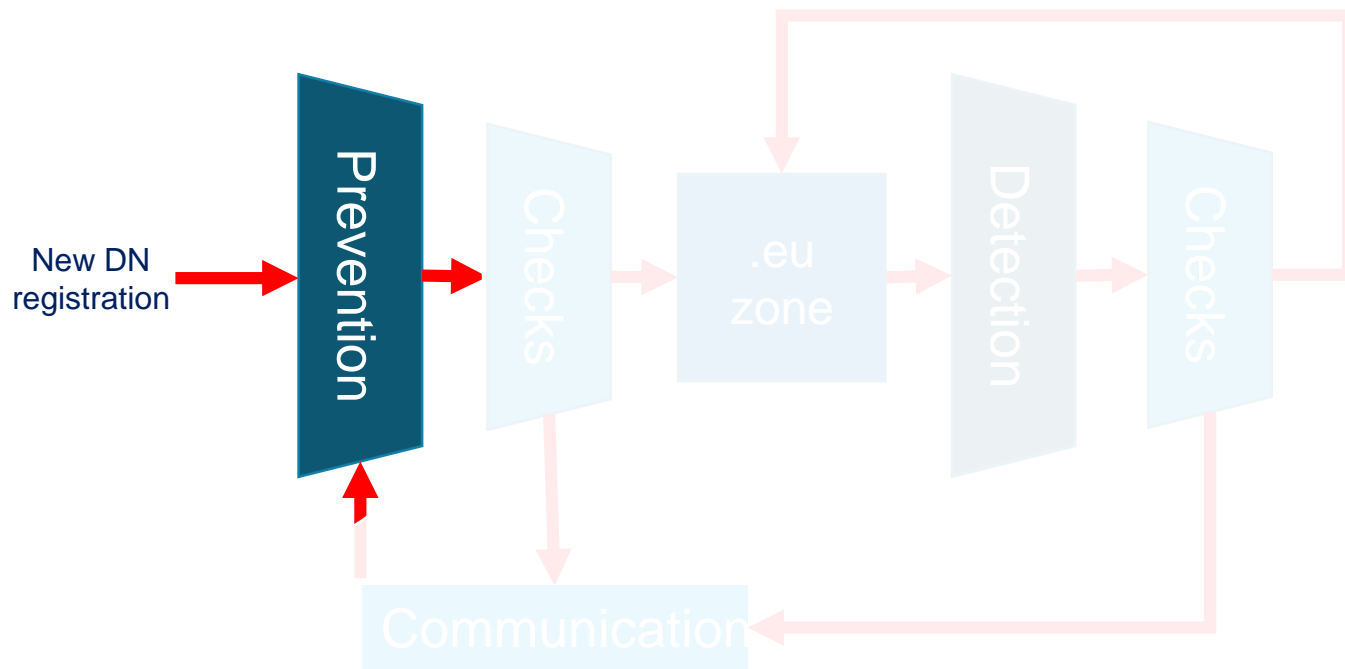
Concept

Three overlapping circles are positioned at the bottom of the slide. The leftmost circle is a medium blue, the middle one is a lighter blue, and the rightmost one is a very light blue, almost white. They overlap in the center.

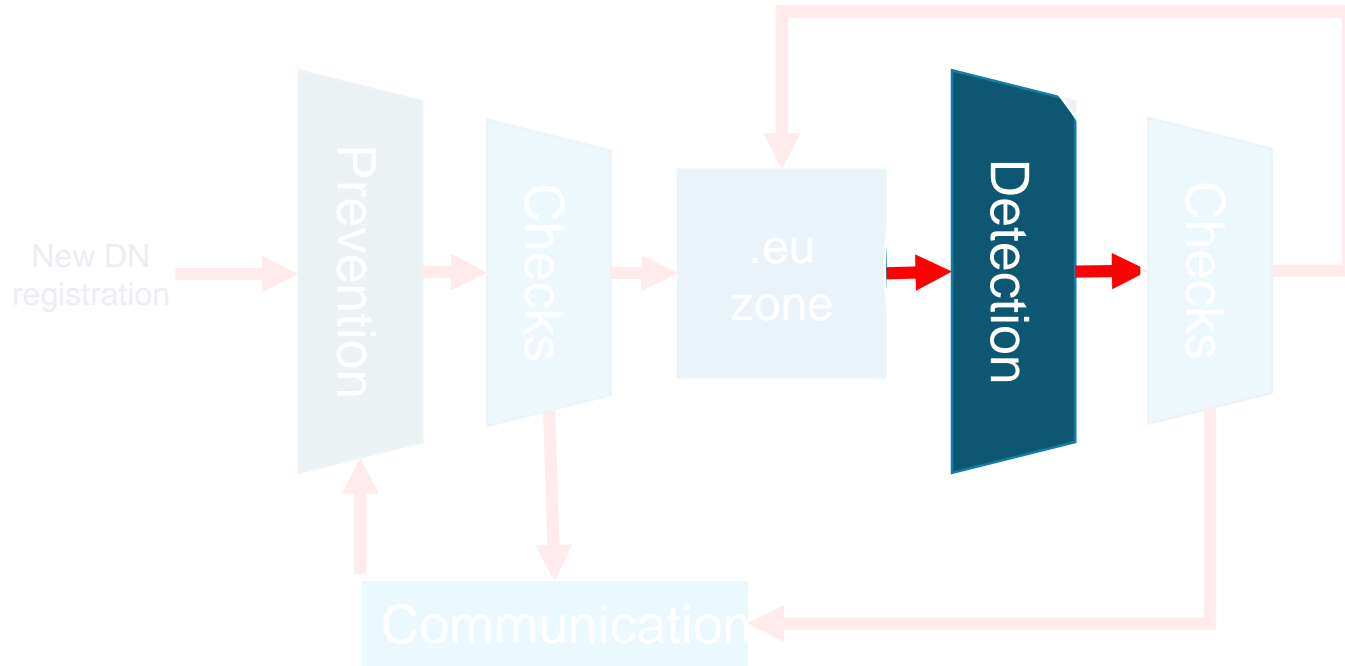
# We act at different levels



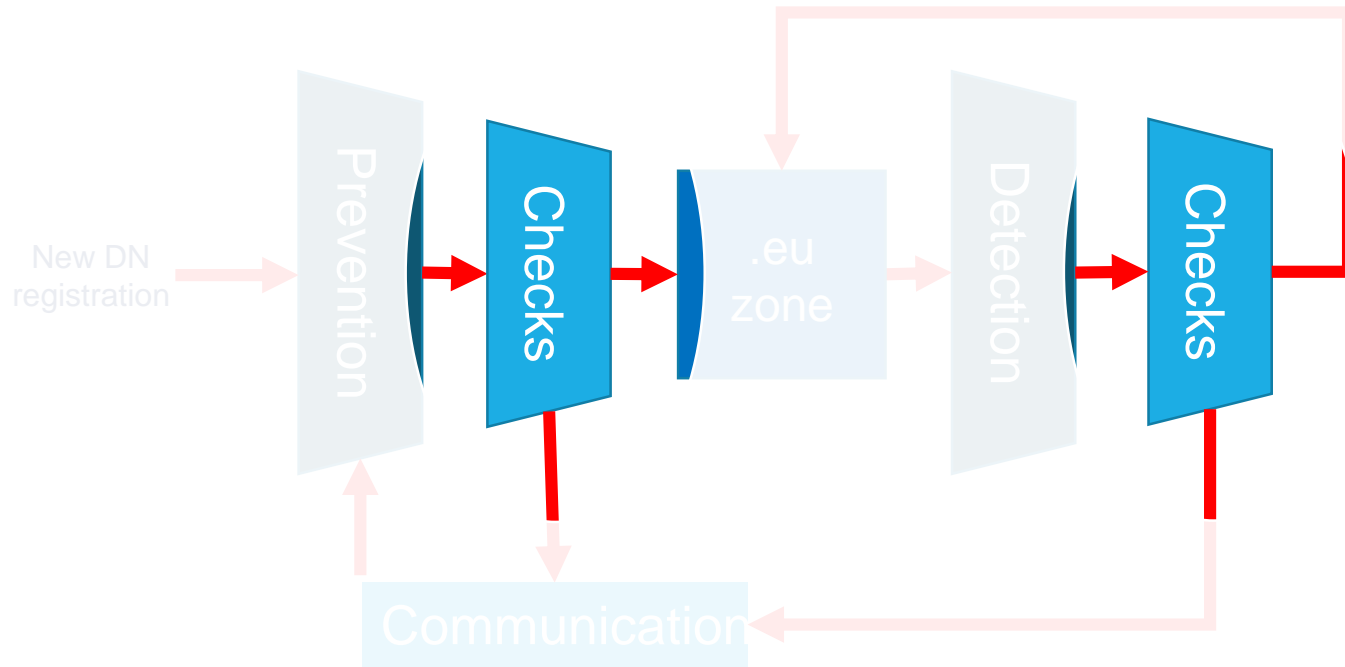
# 1. Prevention: APEWS



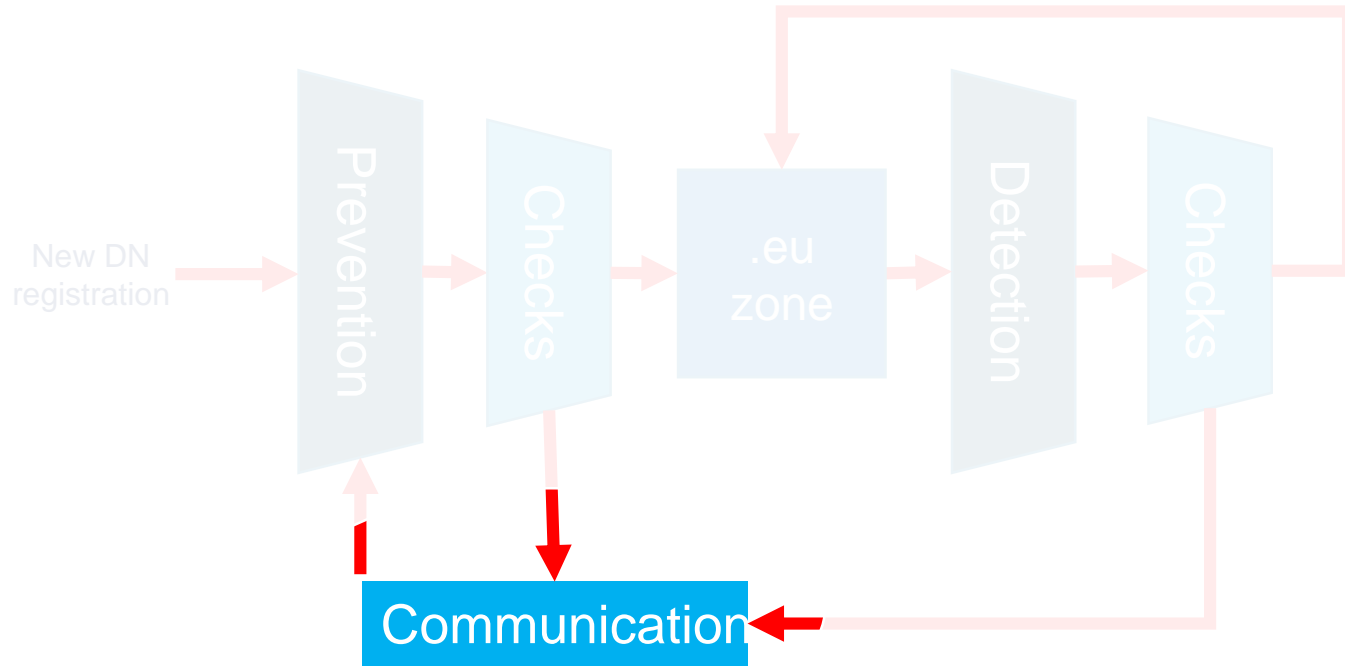
## 2. Detection: Post delegation



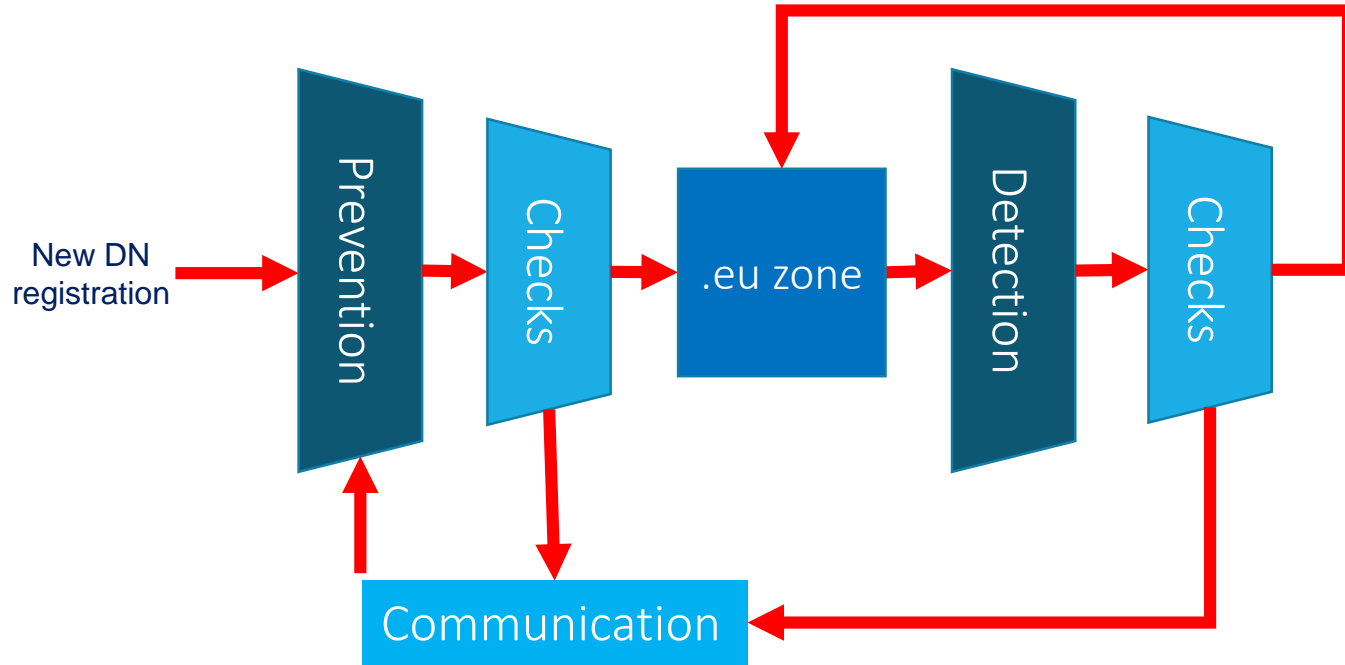
# 3. Checks: WhoisQuality & KYC



# 4. Communication: Share findings



# We act at different levels



Prevent and mitigate  
abuse

Practice

Three overlapping circles are positioned at the bottom of the slide. The leftmost circle is a medium blue, the middle one is a lighter blue, and the rightmost one is a very light blue, almost white. They overlap in a way that creates a sense of depth and movement.



# 1. APEWS

## **A**buse **P**rediction and **E**arly **W**arning **S**ystem

Award winning machine learning system

Domain name is registered but **NOT** (yet) delegated

Pre-delegation Machine-Learning checks

Suggests, before delegation, allegedly abusive domains

- Using domain registration data
- Mixed with external intelligence (experts' confirmed abuse lists)

# 1. APEWS

Domain name delegation is stopped

- We ask registrant for evidence of correct registration data
- We do human review of each case
- Now, with KYC (eIDAS and MRZ), we automate it and increase certitude

APEWS development started in 2016 after negotiation with the EC  
In production since January 2020

# 1. APEWS

APEWS uses different ML algorithms

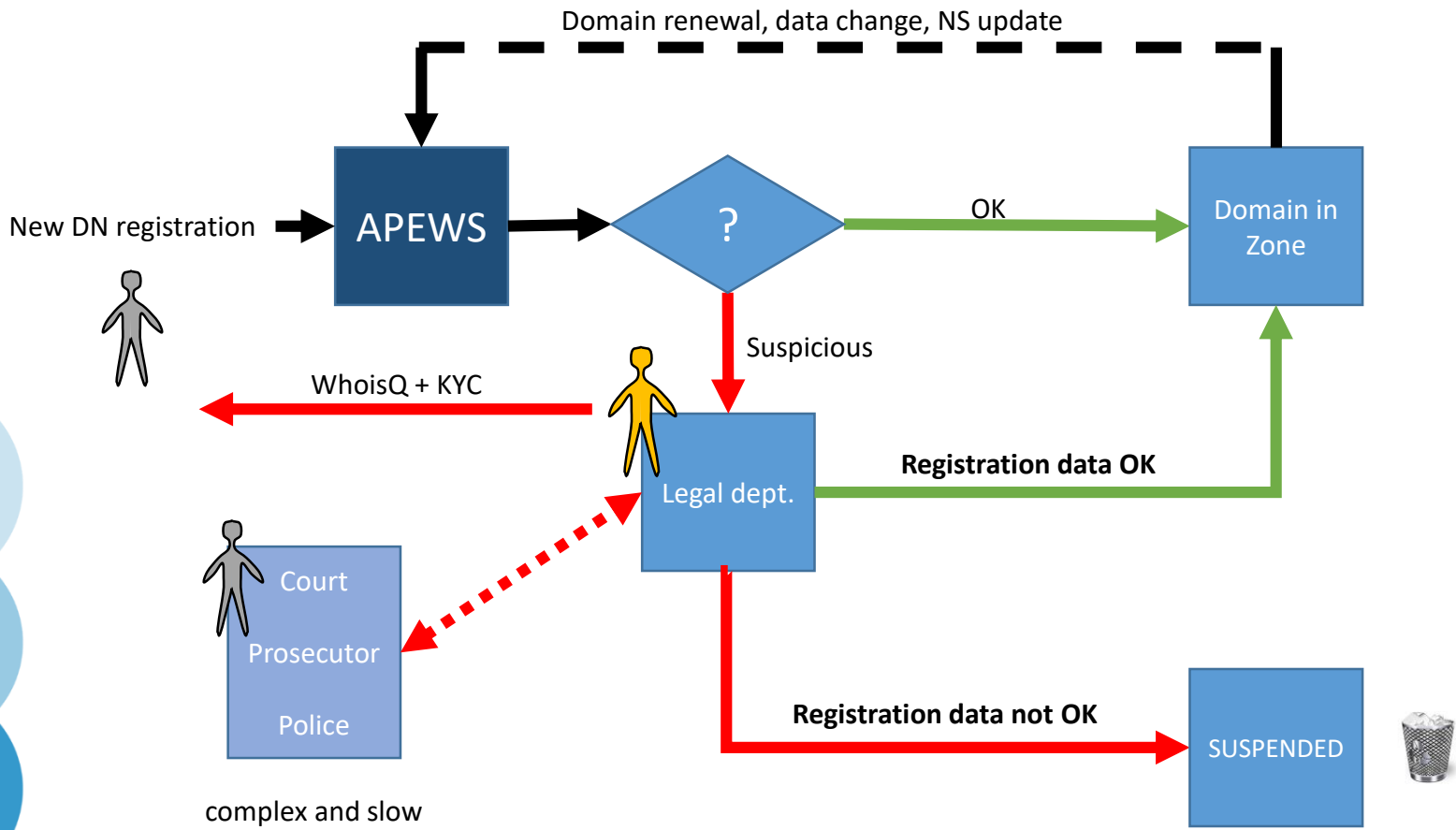
APEWS re-trains itself regularly

Academic papers:

<https://eurid.eu/en/news/identification-of-malicious-dns/>

Combined with a rule-based system

- Eg. Stop COVID19 related domains (EC request)



# 2. Post-delegation checks

Domain name is registered **AND** delegated

Looks for allegedly abusive domains

- DNs delegated in the last 24h
- DNs delegated a few weeks ago
- Ad-hoc list of domains, at any time

# 2. Post-delegation checks

Analyze DN itself (look for certain brands, keywords, ...)

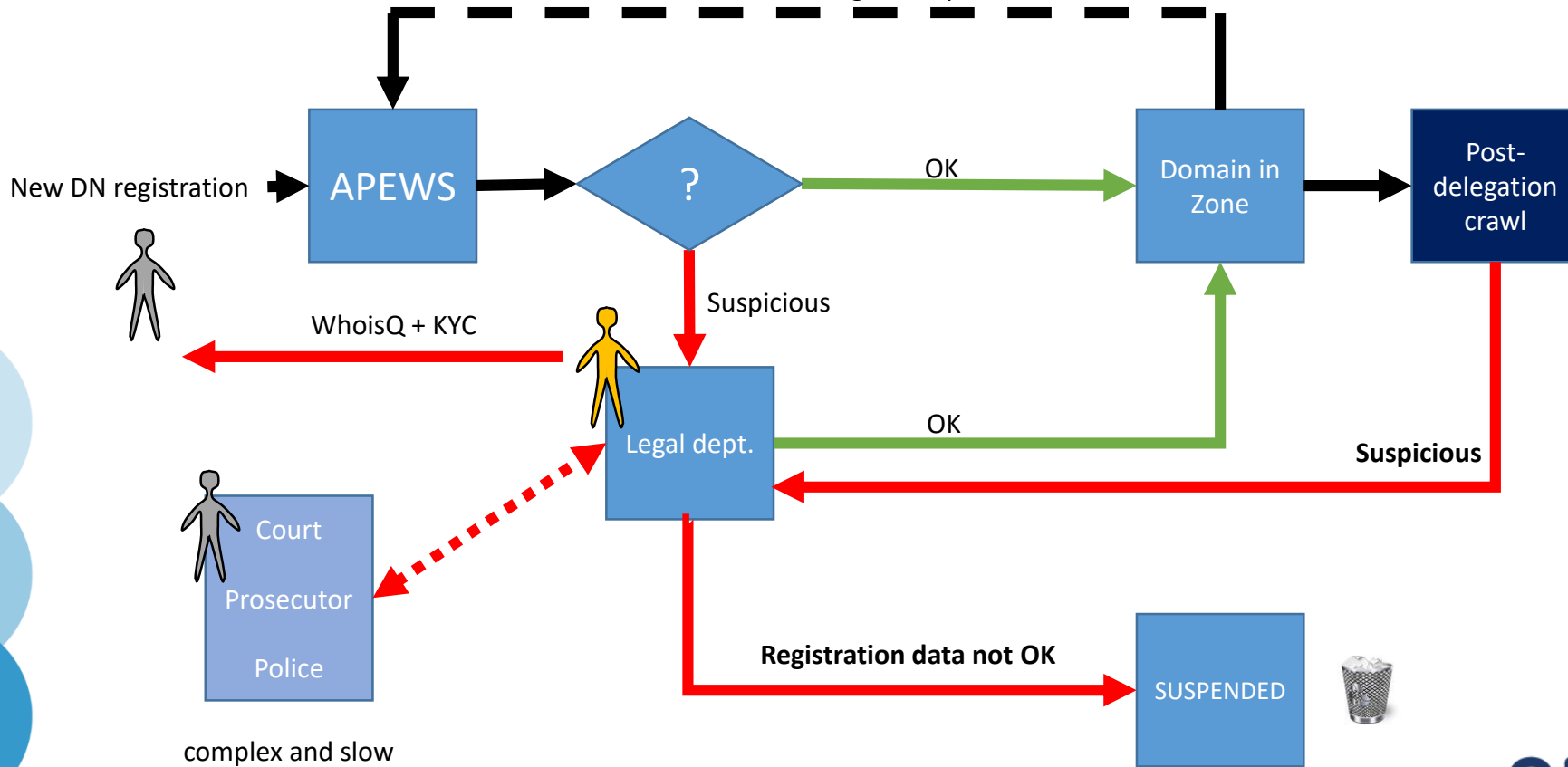
Crawl all DNs

Analyze HTML content

- web shop? → selling well-known brands?
- bank clone?
- etc (we easily create and add new modules)

Analyze registration data and metadata

Domain renewal, data change, NS update



complex and slow

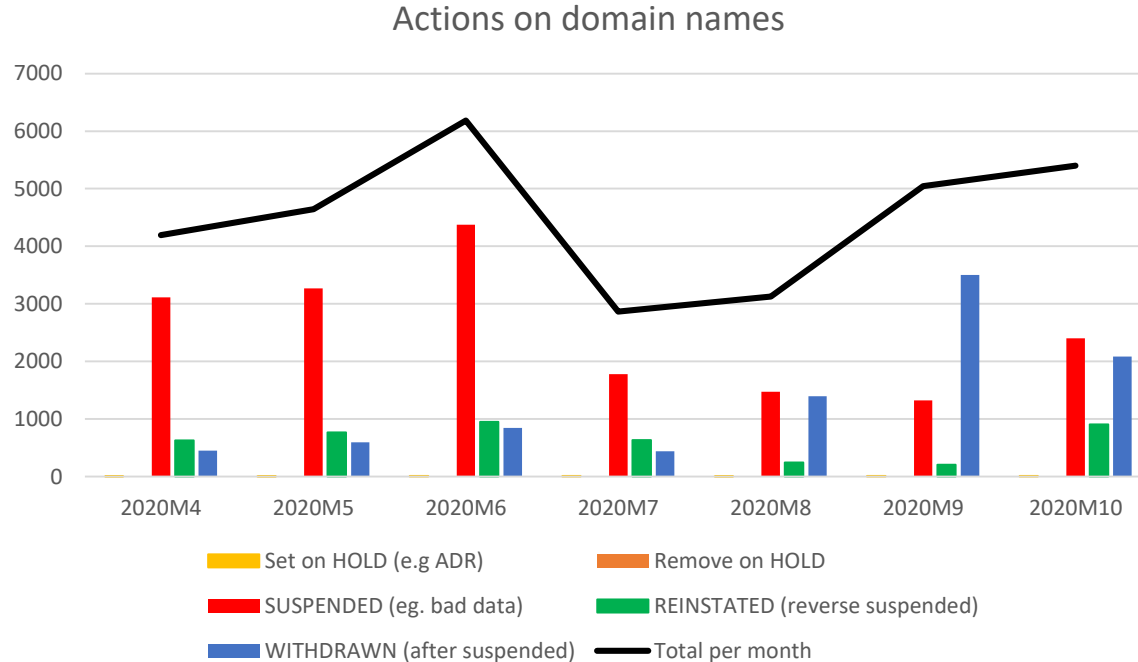
# 3. Check: Review of suspicious cases

Human revision by EURid's Legal department

- Whois Quality check: ask registrant to prove its whois data
  - Email exchange (calls)
  - Suspicions of receiving forged/*photoshoped* bills/ID documents
  - Now, **KYC** → much more difficult to lie
- We cannot suspend based on our opinion on web content
- So we share our suspicions with experts

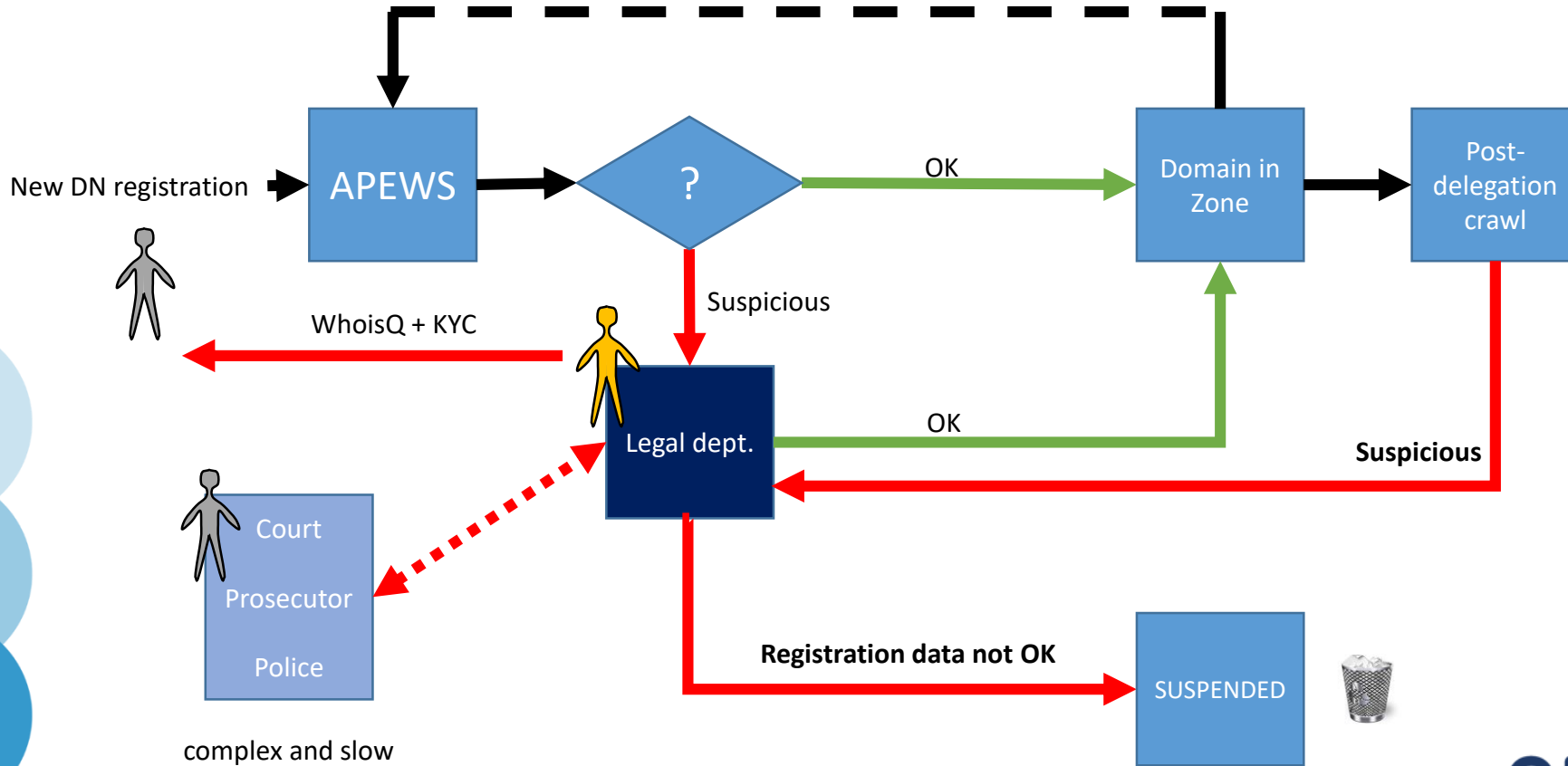


# 3. Review of suspicious cases



Date: 2021.06.14 Distribution: Public

Domain renewal, data change, NS update



complex and slow

# 4. Share intelligence

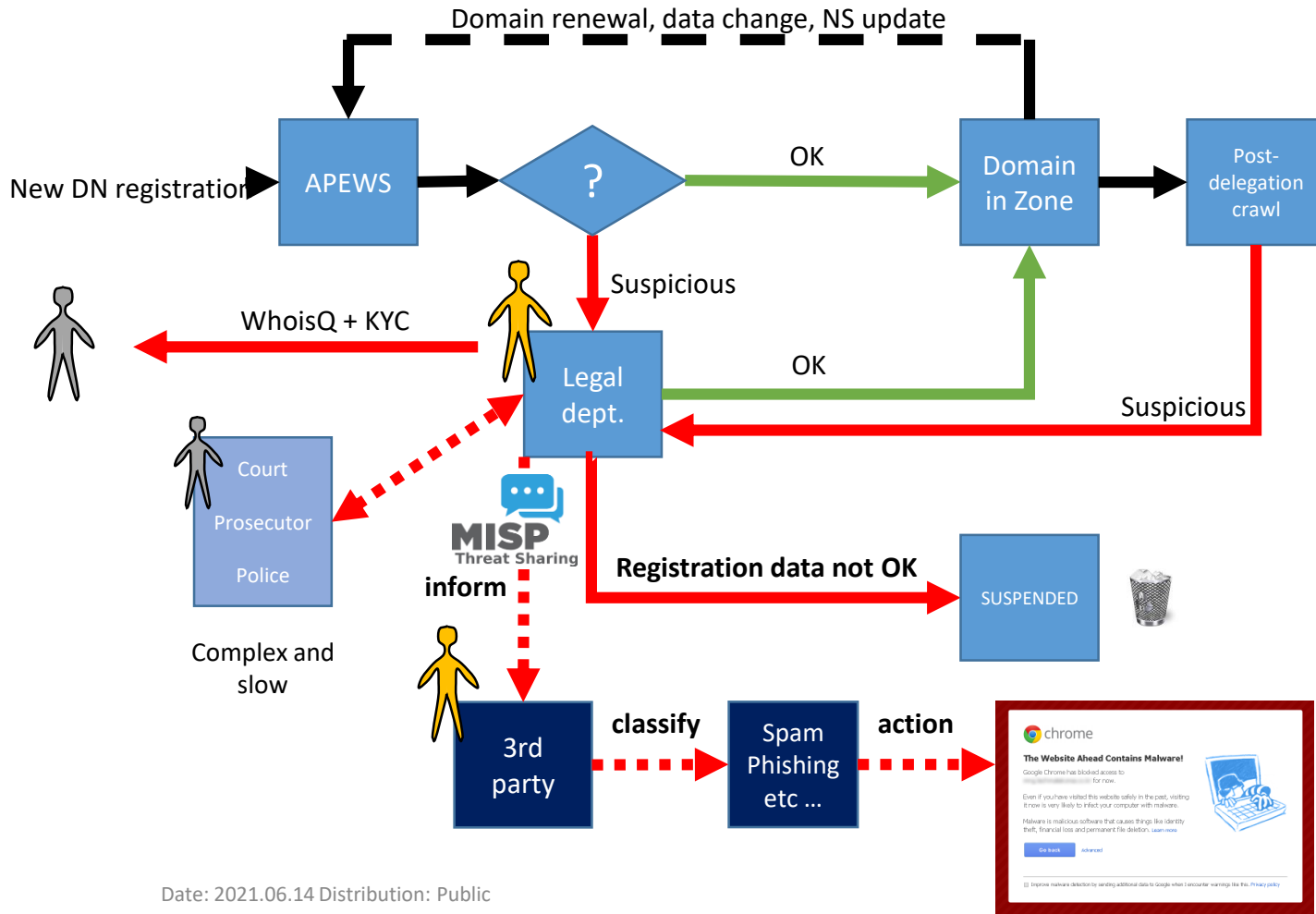
Sharing allegedly suspicious DNS with 3<sup>rd</sup> party experts  
(depending on alleged “type of abuse”)

- EUROPOL
- CERT.be + CCB (Centre for Cybersecurity Belgium)
- FOD Economy (Belgian customs)
- ASOP (Alliance for Safe Online Pharmacy)
- APWG.eu (Anti Phishing Working Group)
- eCommerce Foundation
- Global Cyber Alliance
- ...



# 4. Share intelligence

We (daily) share our findings in parallel to our own checks (WhoisQ + KYC)



## Aantal namaakwebsites daalt: proactieve aanpak werkt!

Online namaakverkoop en piraterij op het internet blijven hoge toppen scheren. Toch worden er minder namaakwebsites opgericht, blijkt uit het aantal afgesloten websites in België. Dit is het resultaat van de internationale campagne In Our Sites en de proactieve samenwerking met EURid, DNS Belgium en de douane. België scoort hiermee goeie punten en is op dat vlak wereldwijd één van de koplopers.



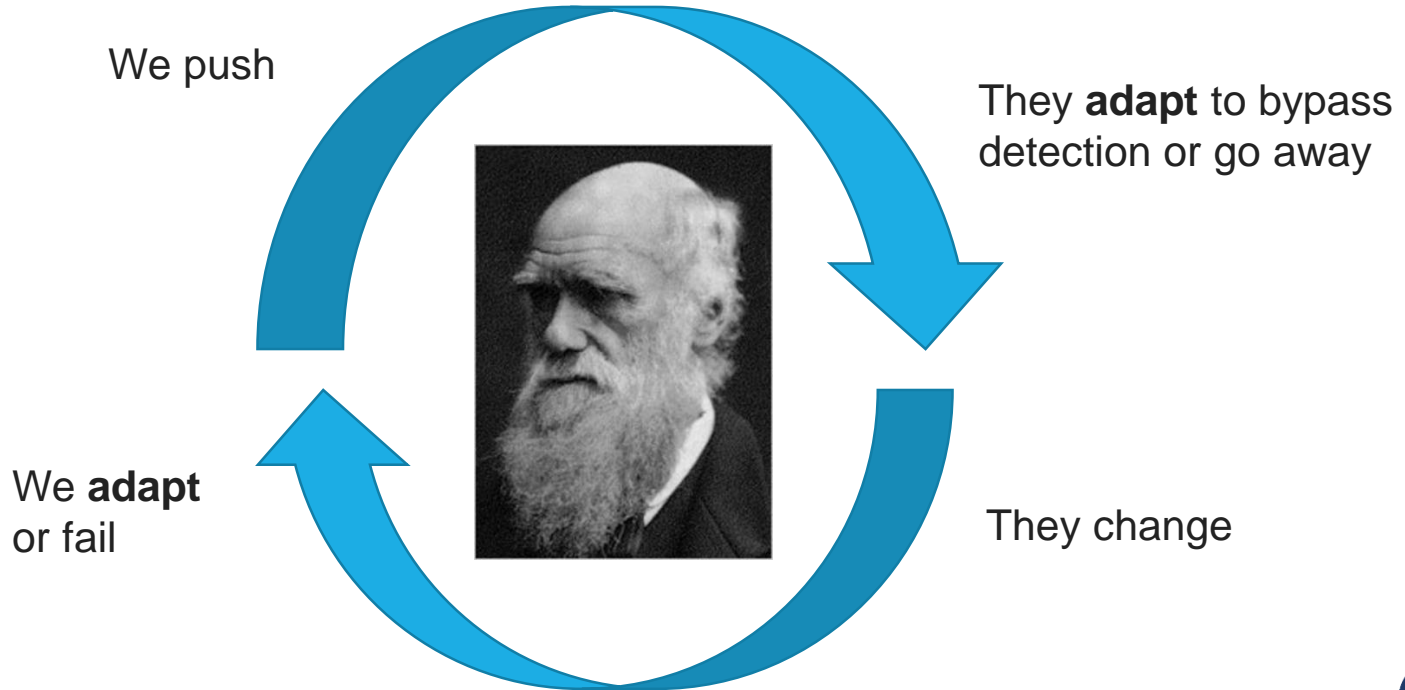
Vorig jaar sloten de Economische Inspectie en de douane 990 namaakwebsites af. Dit jaar is dat aantal lichtjes gestegen tot 1.016. Op het eerste gezicht lijkt er niet veel veranderd, maar niets is minder waar. Sinds de coronacrisis steeg het aantal online aankopen immers gevoelig. Toch steeg het aantal afgesloten namaakwebsites op .be en .eu niet evenredig. Dat is te danken aan de samenwerking van de FOD Economie met EURid, DNS Belgium en de douane in het kader van de internationale Europol-actie In Our Sites. Die zet in op een proactieve aanpak. EURid en DNS Belgium sluiten verdachte websites die eindigen op .be of .eu meteen bij de bron af. Hoewel de online verkoop in 2020 een boost kende, steeg het aantal geblokkeerde namaakwebsites met .be en .eu niet. Deze manier van werken maakt van België zelfs één van de koplopers op wereldwijd vlak.

## Number of fake websites decreases: proactive approach works!

Online counterfeiting and Internet piracy continue to soar. Yet fewer fake websites are being set up, according to the number of closed websites in Belgium. This is the result of the international In Our Sites campaign and the proactive collaboration with **EURid**, DNS Belgium and customs. Belgium scores good points with this and is one of the leaders worldwide in this area.

<https://news.economie.fgov.be/193665-aantal-namaakwebsites-daalt-proactieve-aanpak-werkt>

# But... This is a Darwinian marathon



# And...

- We do see **changes in behaviours**



- Eg. pushing abusers to send “valid” but useless data
  - Some issues clearly disappeared
  - Invented and plausible registration data
  - There are repositories of fake-valid ID data in github
  - Anonymizer services (no need in EU due to GDPR, but...)
  - **KYC** to the rescue!



# Thanks! Questions?

Jordi.iparraguirre@eurid.eu

..eu ..eю ..EU

Powered by **EURid**

