.ie We are
Ireland online

Policy Advisory Committee

24 February 2022

Meeting - PAC#30

Policy Advisory Committee
Agenda PAC #30

1. Membership Matters
2. Minutes from the PAC#29 meeting
3. Matters arising
4. Handling of online abuse which uses the .ie namespace
    - *4.1 GNCCB*
    - *4.2 Anti Abuse policy ?*
5. NIS 2 – Role for the PAC ?
6. Any Other Business
    - *Registrar issue*
    - *CER Directive*
7. Next Meeting

1. Membership Matters

- Please keep **microphones muted** throughout the call
- Please **“raise a hand”** to ask a question or **add comments** in the chat box
- Request to allow the meeting be **recorded** to assist with minute drafting
  - Recording will deleted once the Minutes are approved by PAC

2. Minutes of the PAC #29 Meeting

- Meeting minutes are circulated to the membership within one week of each meeting
- Comments/feedback accepted over a two week period
- If clarifications/edits are requested, and consensus exists, these are reflected in the Minutes
- Meeting minutes, and supporting slides, are published on weare.ie after the comment period has ended
- Published online at https://www.weare.ie/policy-development-process/

We are
Ireland online

3. Matters arising

- Illegality online - engagement with GNCCB *(see Agenda item 4)*
- NIS 2 *(see Agenda item 5)*
- Technical abuse - Netcraft service

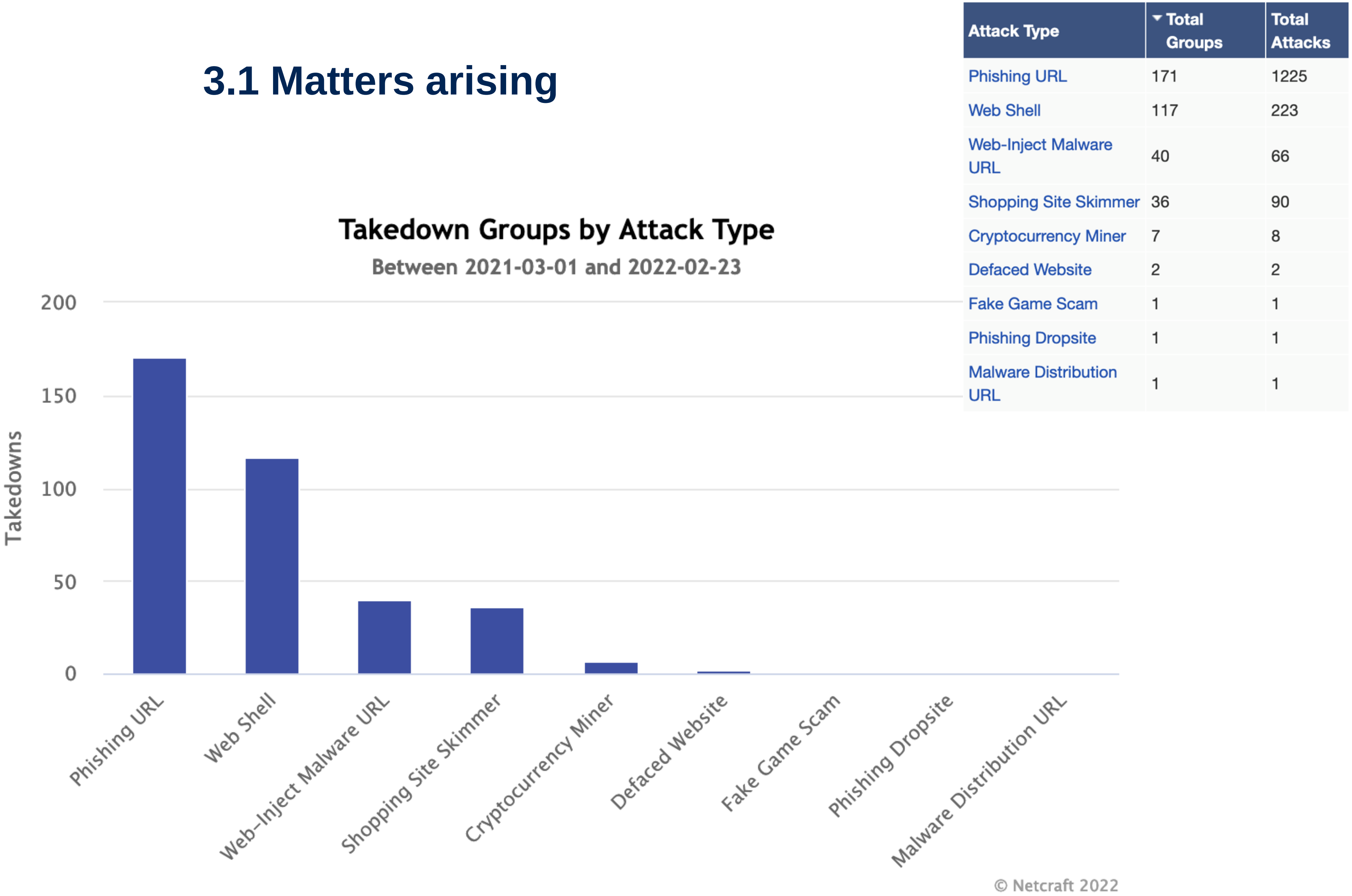
We are
Ireland online

3.1 Matters arising

Handling of online **Technical abuse:-** use of Phishing, Malware, botnets etc

Netcraft service:- 376 takedowns since commencement in Q1 2021

(1,617 attacks handled)



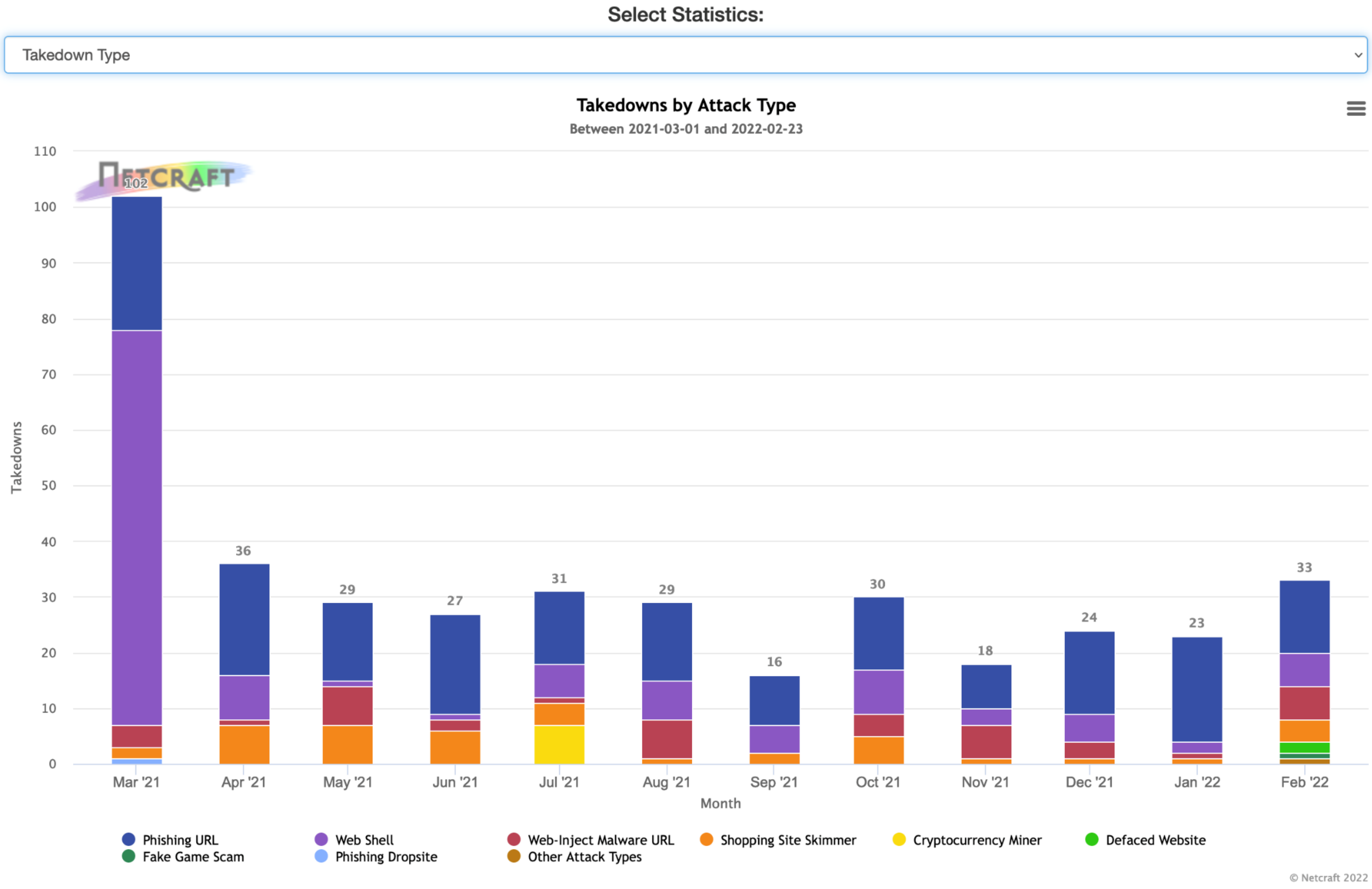
© Netcraft 2022

Attack Type	Total Groups	Total Attacks
Phishing URL	171	1225
Web Shell	117	223
Web-Inject Malware URL	40	66
Shopping Site Skimmer	36	90
Cryptocurrency Miner	7	8
Defaced Website	2	2
Fake Game Scam	1	1
Phishing Dropsite	1	1
Malware Distribution URL	1	1

3.1 Matters arising

Averaging c.25# p.m

(excl March ‘21)



Select Statistics:

Takedown Type

Takedowns by Attack Type

Between 2021-03-01 and 2022-02-23

© Netcraft 2022

4.1 Handling of illegality and criminal abuse in the .ie namespace

GNCCB - Suspension Request protocol document

- Common Ground & Goodwill is substantial

Paul Johnstone | Detective Sergeant | Garda National Cyber Crime Bureau

Harcourt Square, Harcourt Street, Dublin 2, D02 DH42, Ireland
www.garda.ie | ✉ **GNCCB@garda.ie** |***#GNCCB*** |
☎ +353 1 6663708 | +353 86 8281889 |
Consider the environment before printing this e-mail.

- Online dialogue to close the gaps between the Channel and AGS

- Draft protocol (circulated for PAC #29) is being referred upwards in AGS

4.1 Handling of illegality and criminal abuse in the .ie namespace

GNCCB - Suspension Request protocol document

- Remaining matters
  - Single point of contact (SPOC)
    - Multiple SPOCs – one per CAB, GNCCB, GNECB, GNDOCB. (Training on “what’s possible / what’s available”)
  - Sequence of engagement
    - default is Registrar, then Registry.
    - (exception where “RAR contact is not appropriate”); dead-end if Hoster is uncooperative / outside jurisdiction
  - Informing the registrant is the default
    - (exceptions, for operational reasons e.g. organised crime investigation)
  - Basis for refusal to suspend
    - eg missing or incomplete info on the Suspension Request doc
  - Basis for Registrar opt-out
    - entirely, or on a case-by-case basis
    - Adoption of the Protocol is not obligatory for .IE Registrars
  - Timing of a request:- re stage of AGS investigation
    - confirmed criminality Vs reasonable and justifiable suspicion that criminality is taking place
  - Validity period / term of suspension
    - Default suspension period is 90 days, then re-apply for extension

4.2 DNS Abuse – time for a formal .IE Policy ?

(more accurately ‘Abuse that uses the DNS’….)

Rationale for an Anti-Abuse policy:-

- Topic du jour
- Exponential increase in malware, phishing, scams in a digitally transformed post-Covid world
- EU* regulators attention
- Self-regulation provides confidence, builds trust through transparency
- Channel is mature & responsible & cares about Consumer Protection
- Formalises our position (we are in a good place; managed registry model; Netcraft service)
- ccTLDs will (eventually) follow gTLDs - obliged to have a policy

*The European Commission has just published its study on DNS abuse. The study assessed the scope, magnitude and impact of DNS abuse and provided input for possible policy measures. The study proposes a **set of recommendations** in the field of **prevention, detection and mitigation** of DNS abuse.

We are
Ireland online

4.2 DNS Abuse – time for a formal .IE Policy ?

The European Commission has just published its study on DNS abuse:

The study assessed the scope, magnitude and impact of DNS abuse and provided input for possible policy measures.

The study proposes a **set of recommendations** in the field of **prevention, detection and mitigation** of DNS abuse **addressed to DNS operators** (TLD registries, registrars, resellers and hosting providers, depending on their role in the DNS chain) but also to international, national and EU institutions and coordination bodies.

The study also recommends actions in the field of DNS metadata, WHOIS and contact information, abuse reporting, protection of the DNS operations, awareness, knowledge building and mitigation collaboration at EU level.

https://op.europa.eu/en/publication-detail/-/publication/7d16c267-7f1f-11ec-8c40-01aa75ed71a1/language-en/.

4.2 DNS Abuse – time for a formal .IE Policy ?

- ccTLDs – practices vary
- gTLDS - have a Domain Anti-Abuse Policy,
- legitimized by - section 3.5.2 of the Registry-Registrar Agreement ("RRA"),
- principles - abusive use(s) of domain names should not be tolerated.

<<gTLD>> defines abusive use as the wrong or excessive use of power, position or ability, and includes, without limitation, the following:

Illegal or fraudulent action **Spam** **Phishing** **Pharming**

Willful distribution of malware **Fast flux hosting**

Botnet command and control **Distribution of child pornography**

Illegal Access to other Computers or Networks:

We are
Ireland online

4.2 DNS Abuse – time for a formal .IE Policy ?

Pursuant to Section 3.6.5 of the RRA, <<gTLD>> reserves the right to deny, cancel or transfer any registration or transaction, or place any domain name(s) on registry lock, hold or similar status, that it deems necessary, in its discretion;

(1) to protect the **integrity and stability of the registry**;

(2) to comply with any **applicable laws, government rules** or requirements, requests of law enforcement, or any dispute resolution process;

(3) to **avoid any liability,** civil or criminal, on the part of <<gTLD>>, as well as its affiliates, subsidiaries, officers, directors, and employees;

(4) per the terms of the **registration agreement** or

(5) to **correct mistakes** made by <<gTLD>> or any Registrar in connection with a domain name registration.

5. NIS 2 – Role for the PAC ?

"All businesses are increasingly dependent on third party services - from major cloud providers, through the ecosystem of software as a service (SaaS) providers and managed service providers, to a new world of data and analytics service providers.

In the old days, our IT was on-premises, defended by firewalls and barriers, under our control and our management. This model is dead, and with it comes a raft of new digital infrastructure providers that we depend on for hosting, for platform and for service provision.

NIS is being revised to reflect this reality."

Dani Michaux, EMA Cyber Leader, KPMG Ireland

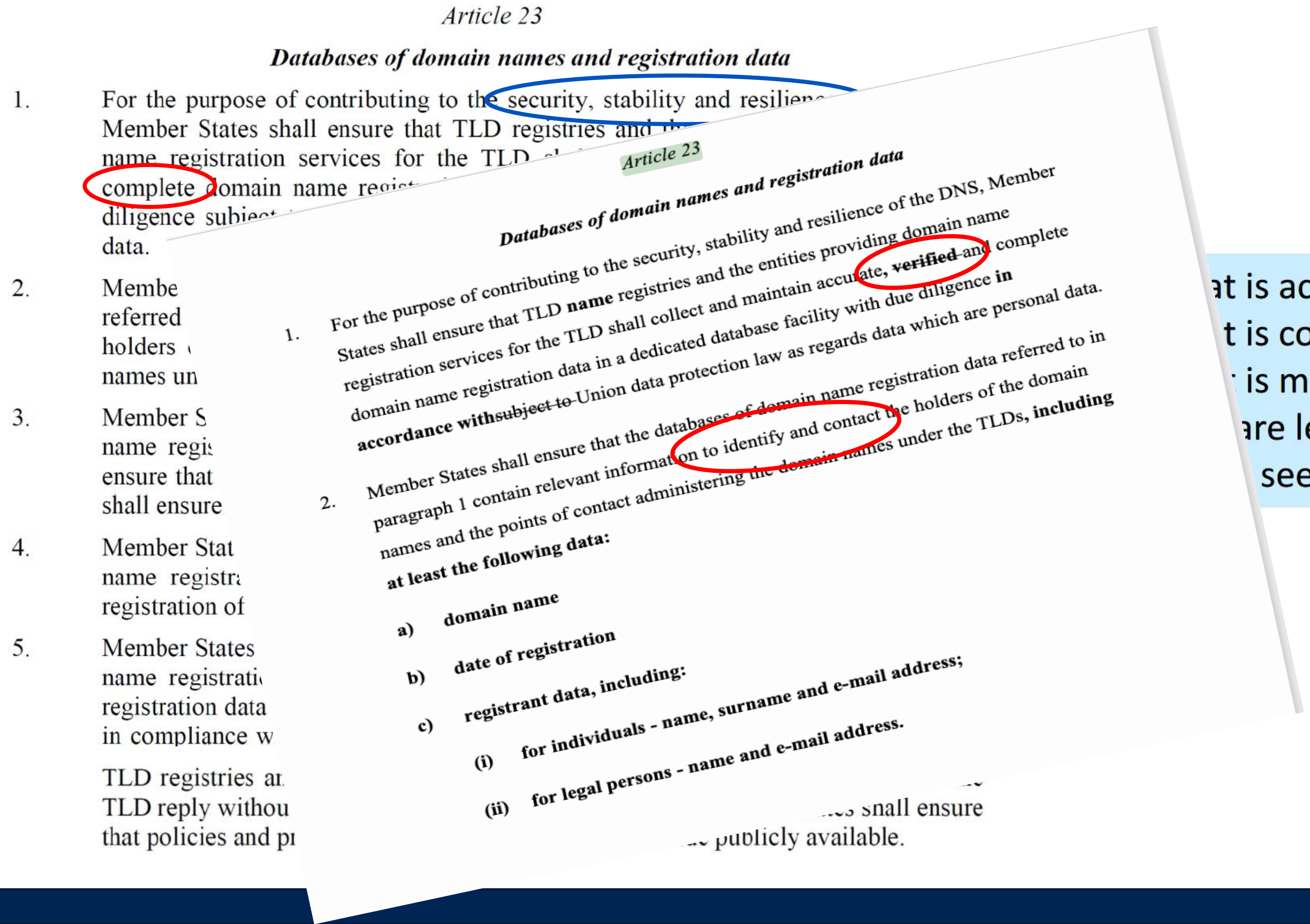
5. NIS 2 – Role for the PAC ?

Update on developments in 2022 so far:-

5. NIS 2 – Role for the PAC ?

***Article 23**:- implications for data accuracy & completeness*

Update on developments in 2022 so far:-



Article 23

Databases of domain names and registration data

1. For the purpose of contributing to the security, stability and resilien
Member States shall ensure that TLD registries and th
name registration services for the TLD sl
complete domain name regist
diligence subject
data.

2. Membe
referred
holders
names un

3. Member S
name regis
ensure that
shall ensure

4. Member Stat
name registra
registration of

5. Member States
name registrati
registration data
in compliance w

TLD registries ar
TLD reply withou
that policies and pr
s shall ensure
publicly available.

Article 23

Databases of domain names and registration data

1. For the purpose of contributing to the security, stability and resilience of the DNS, Member States shall ensure that TLD **name** registries and the entities providing domain name registration services for the TLD shall collect and maintain accurate, **~~verified~~** and complete domain name registration data in a dedicated database facility with due diligence **in accordance with**~~subject to~~ Union data protection law as regards data which are personal data.

2. Member States shall ensure that the databases ~~of domain~~ name registration data referred to in paragraph 1 contain relevant information to identify and contact the holders of the domain names and the points of contact administering ~~the domain names~~ under the TLDs**, including at least the following data:**

   a) **domain name**

   b) **date of registration**

   c) **registrant data, including:**

      (i) **for individuals - name, surname and e-mail address;**

      (ii) **for legal persons - name and e-mail address.**

at is accurate?
t is complete?
is maintain?
are legitimate
seekers?

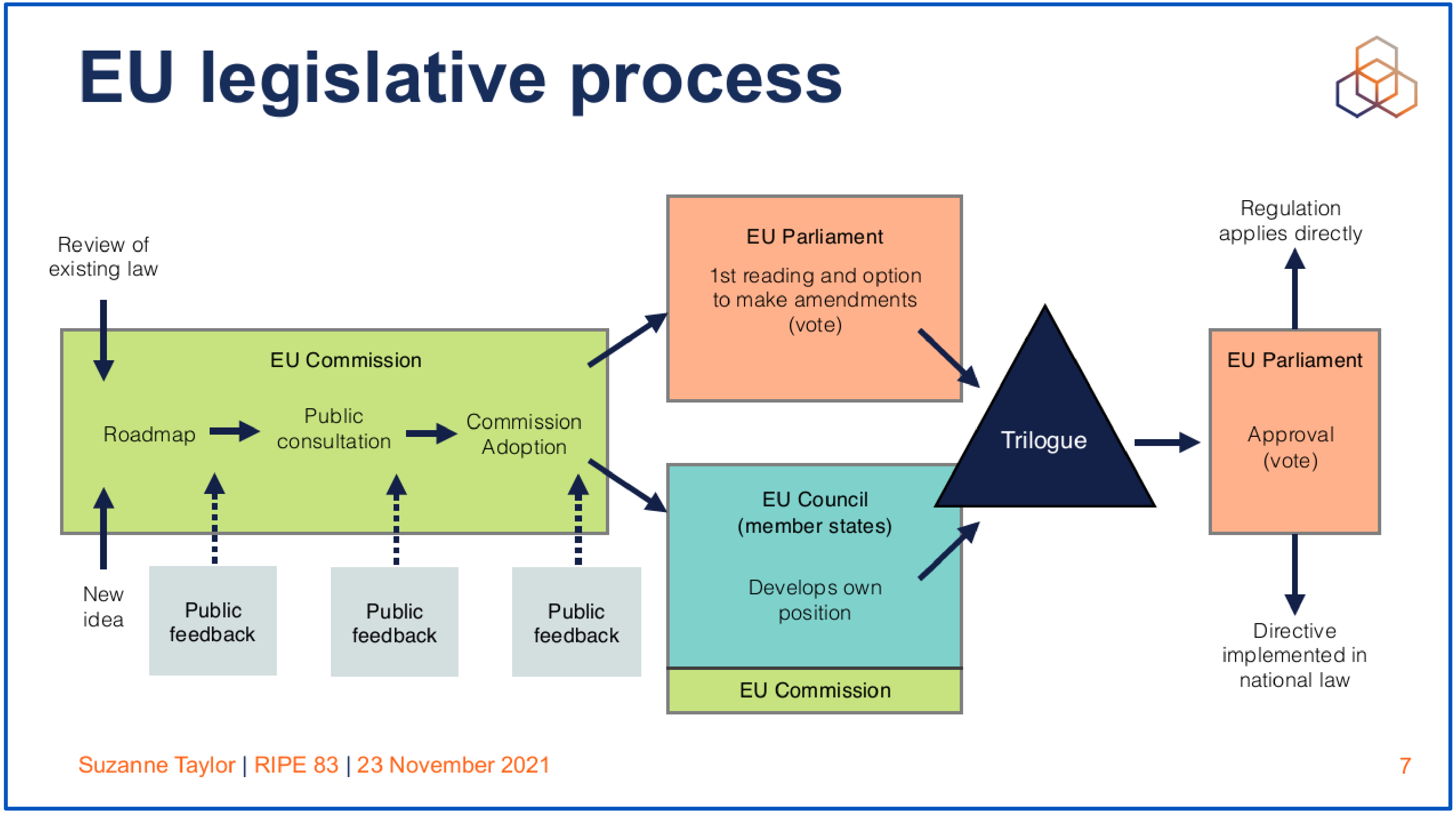
We are
Ireland online

5. NIS 2 – Role for the PAC ?

Update on developments in 2022 so far:-

- The French Presidency aims - re Timing / Trilogues / and linking DSA & CER Directives.
- Some positive proposed edits from the **Council** draft…..
  - Article 23 - excludes "Verification"
  - Less conflict with GDPR in Whois proposals
  - Data Access – to legitimate access seekers
  - Member States would have 24 months to transpose (not 18 months, per Commission's proposal)
- Scope ?
  - not apply to entities - in areas like defence or national security, public security, law enforcement and the judiciary.
  - Parliaments and central banks - exempt, though the public administration arms of **central** govt's would not.
  - Member states to decide whether NIS2 applies to the public administration of their **regional** and **local** govt too.
  - The Council also reduced the directive's reporting obligations in order to avoid causing "over-reporting
  - Council wants to avoid creating an excessive burden on the entities covered
  - micro-SMEs (threshold # of domains)
- Potential to tie eID to the *implementation* of Article 23
- Verisign PIR & Donuts are worried about the financial impact of Article 23 (=> uncertainty for gTLDs too)

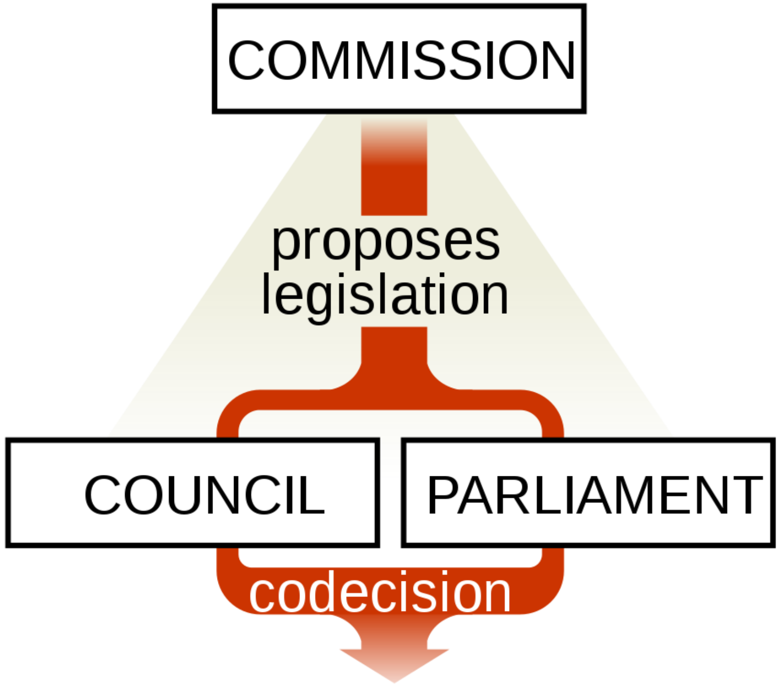
5. NIS 2 – Role for the PAC ?



EU legislative process

Suzanne Taylor | RIPE 83 | 23 November 2021

5. NIS 2 – Role for the PAC ?



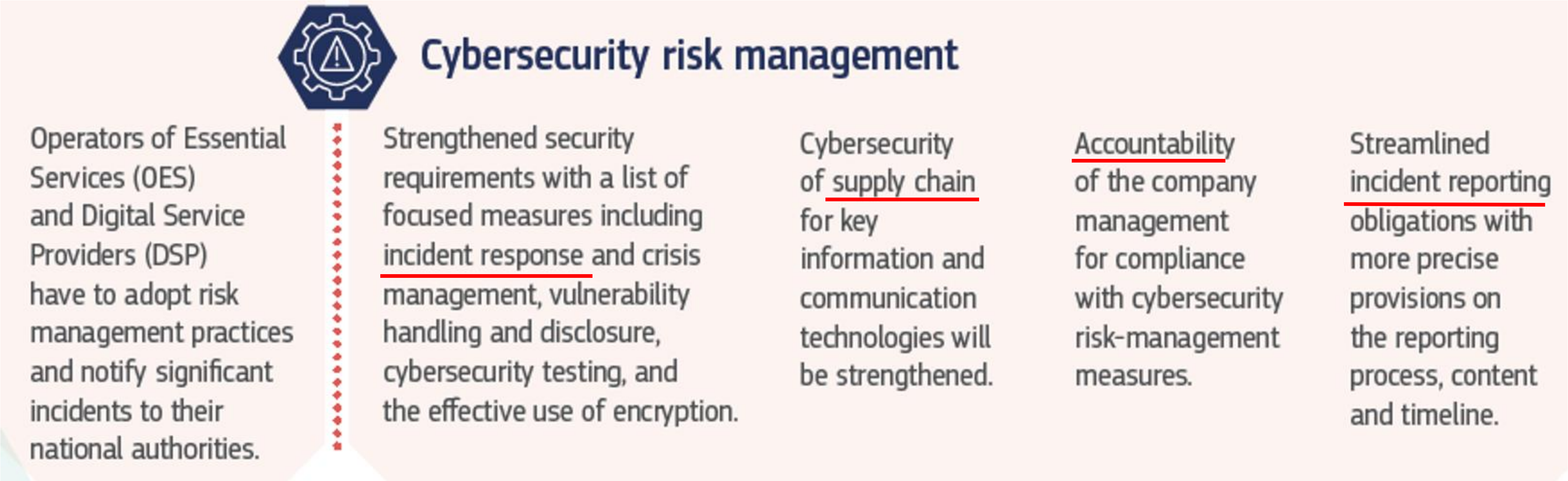
- European Commission (who proposed NIS2 directive)
- European Parliament* (created amendments incl. ITRE draft)
- EU Council of Ministers (Council of the European Union) — *which has possibly the most favourable draft for PAC members*

** The European Parliament's Committees:-*

- *Industry, Research and Energy (**ITRE**).*
- *Internal Market and Consumer Protection (**IMCO**).*
- *Civil Liberties, Justice and Home Affairs (**LIBE**).*

5. NIS 2 – Role for the PAC ?

How can we make progress on ‘The Good’



Cybersecurity risk management

Operators of Essential Services (OES) and Digital Service Providers (DSP) have to adopt risk management practices and notify significant incidents to their national authorities.

Strengthened security requirements with a list of focused measures including incident response and crisis management, vulnerability handling and disclosure, cybersecurity testing, and the effective use of encryption.

Cybersecurity of supply chain for key information and communication technologies will be strengthened.

Accountability of the company management for compliance with cybersecurity risk-management measures.

Streamlined incident reporting obligations with more precise provisions on the reporting process, content and timeline.

5. NIS 2 – Role for the PAC ?

How can we make progress on ‘The Good’

- Legislation is 2 years away, but **cyber threats** are here today
- **Awareness** building – “Just inform” via Newsletter, Blogs, Webinars, YouTube clips
  - *Audience* - RAR channel, SMEs in the Supply Chains, TDs & policy makers,
  - *Content* - sections from Registrars (cyber security), Lawyers (~GDPR conflicts), IRISS (preparations), NCSC (NIST 101 tips).
  - *Collaboration* between:- Registrars, Lawyers, IRISS/Cyber Ireland; NCSC; LEA’s….
  - *Messaging* :- Start now on cyber defences, think about ISO alignment 1st;
- Share **Impact Assessment** document – cyber benefits, regulatory cost burden, need for eID,
- **Lobby** letter - to those transposing into national legislation – do’s & dont’s; ask for early clarifications
- **Engagement** - Channel needs a clear legal framework (esp. re conflicts with GDPR provisions)
- Cyberthreats – how to improve **current** resilience and incident response capacities of critical infrastructures

6. AOB

- Registration & Naming Policy issue – raised by registrar
- Directive on the resilience of critical entities (CER Directive)

8. Next Meeting

Proposed date:

5th May 2022

.ie We are Ireland online

Policy Advisory Committee

24th February 2022

Meeting - PAC#29