We are
Ireland online

Policy Advisory Committee

26th May 2022

Meeting - PAC#31

.ie We are Ireland online

Policy Advisory Committee
Agenda PAC #31

1. Membership Matters
2. Minutes from the PAC#30 meeting
3. Matters arising
4. Handling of online abuse which uses the .ie namespace
    - *4.1 GNCCB*
    - *4.2 Anti Abuse policy proposal*
5. NIS 2 – Role for the PAC ?
6. Any Other Business
    - *EU Framework – IP protection - Alerting system proposed for domain names*
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

.ie We are Ireland online

2. Minutes of the PAC #30 Meeting

- Meeting minutes are circulated to the membership promptly after 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/

3. Matters arising

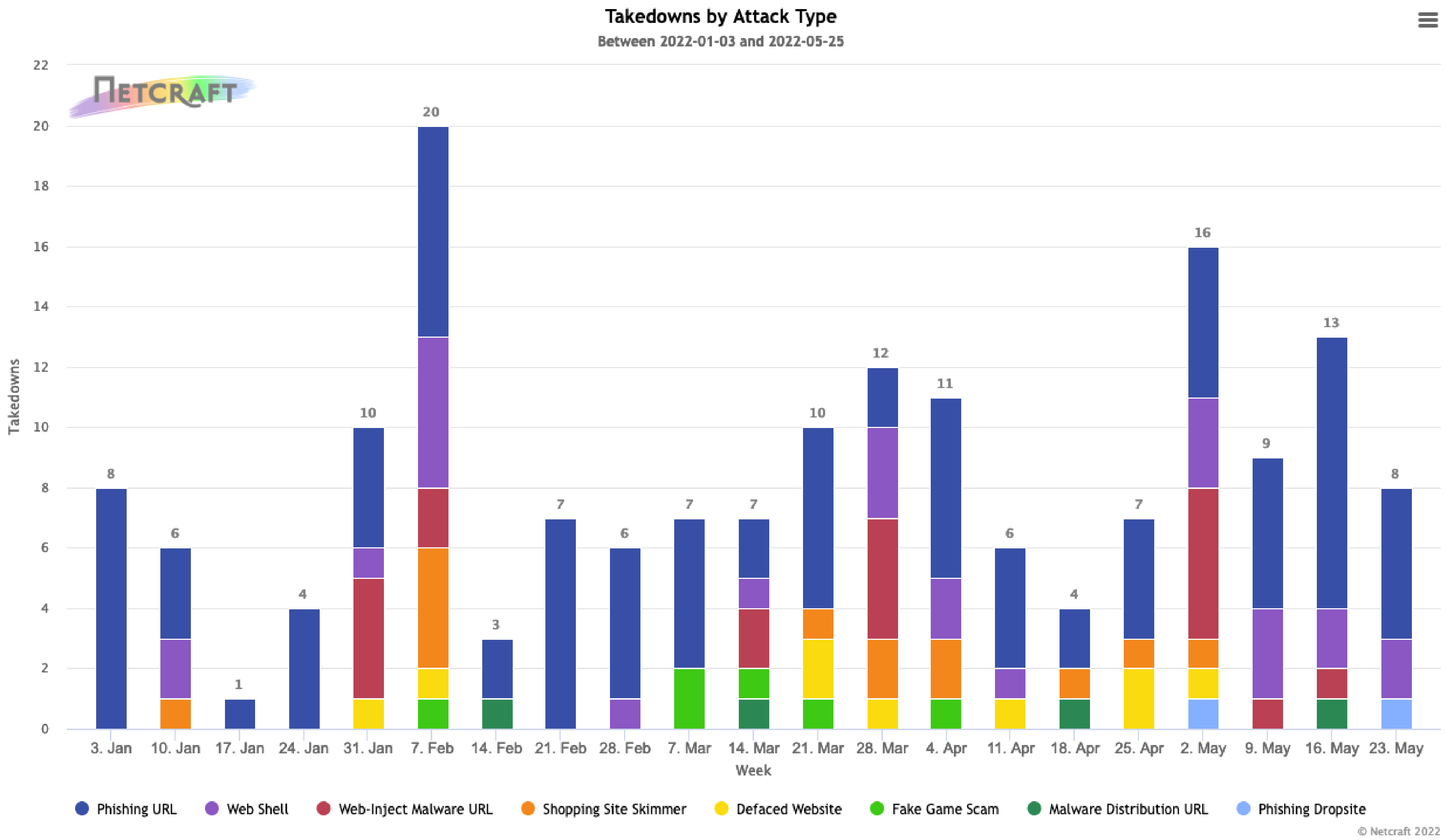
- Illegality online - engagement with GNCCB *(see Agenda item 4)*
- NIS 2 *(see Agenda item 5)*
- Technical abuse - Netcraft service

3.1 Matters arising

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

Netcraft service:- 175 takedowns YTD in 2022

(761 attacks handled)



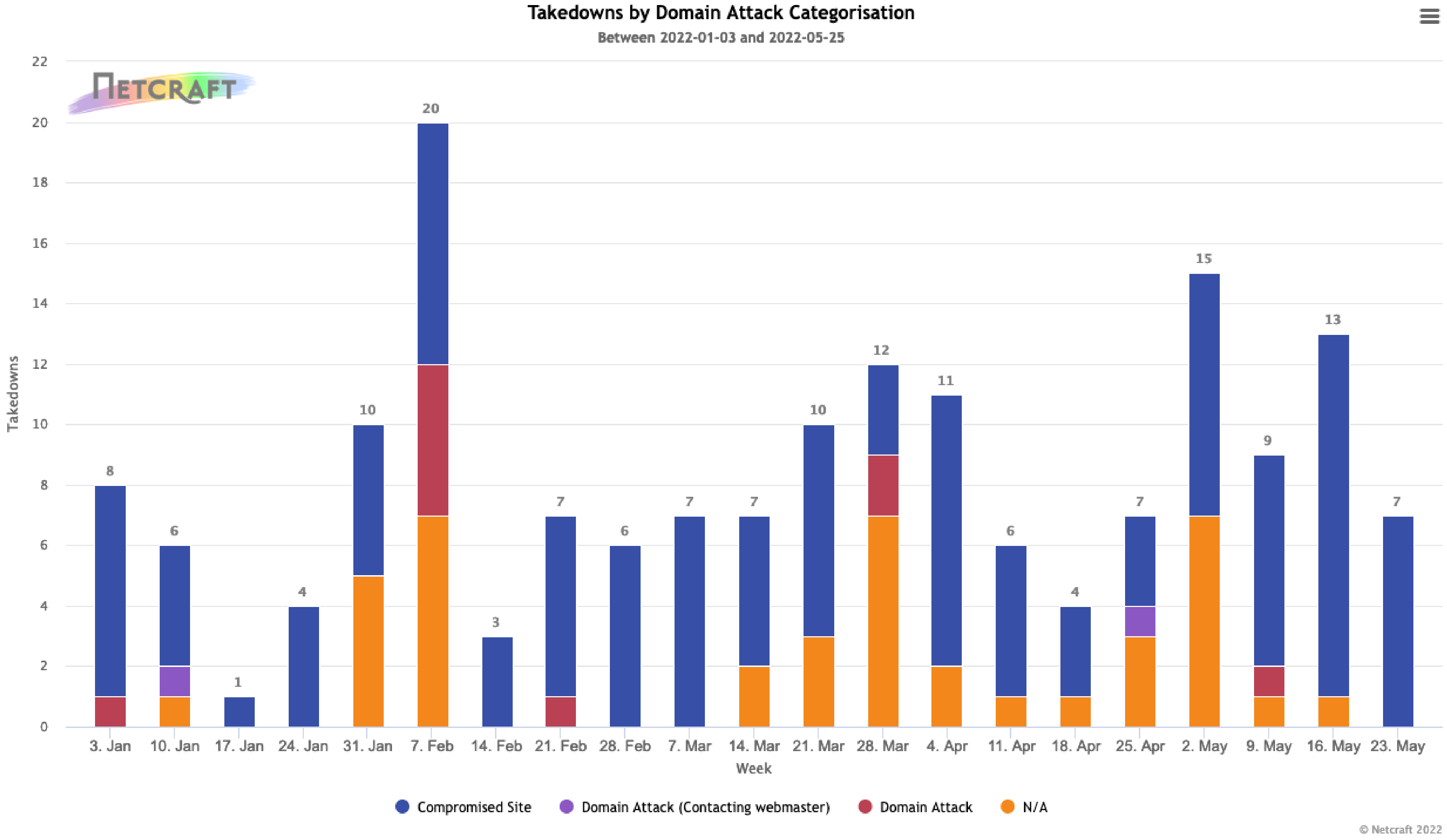
3.1 Matters arising

Compromised Site:
This category shows attacks where we believe that the fraudulent content has been uploaded by a third party to an otherwise benign site.

Domain Attack (Contacting webmaster):
Attacks are assigned to this category if the automated system believes the domain might be owned by the criminal, but there was not enough evidence to be certain. The webmaster is contacted for these takedowns.

Domain Attack:
This category shows attacks where we believe the entire domain is under the control of the criminal, and therefore we will not attempt to contact the webmaster.

3.1 Matters arising

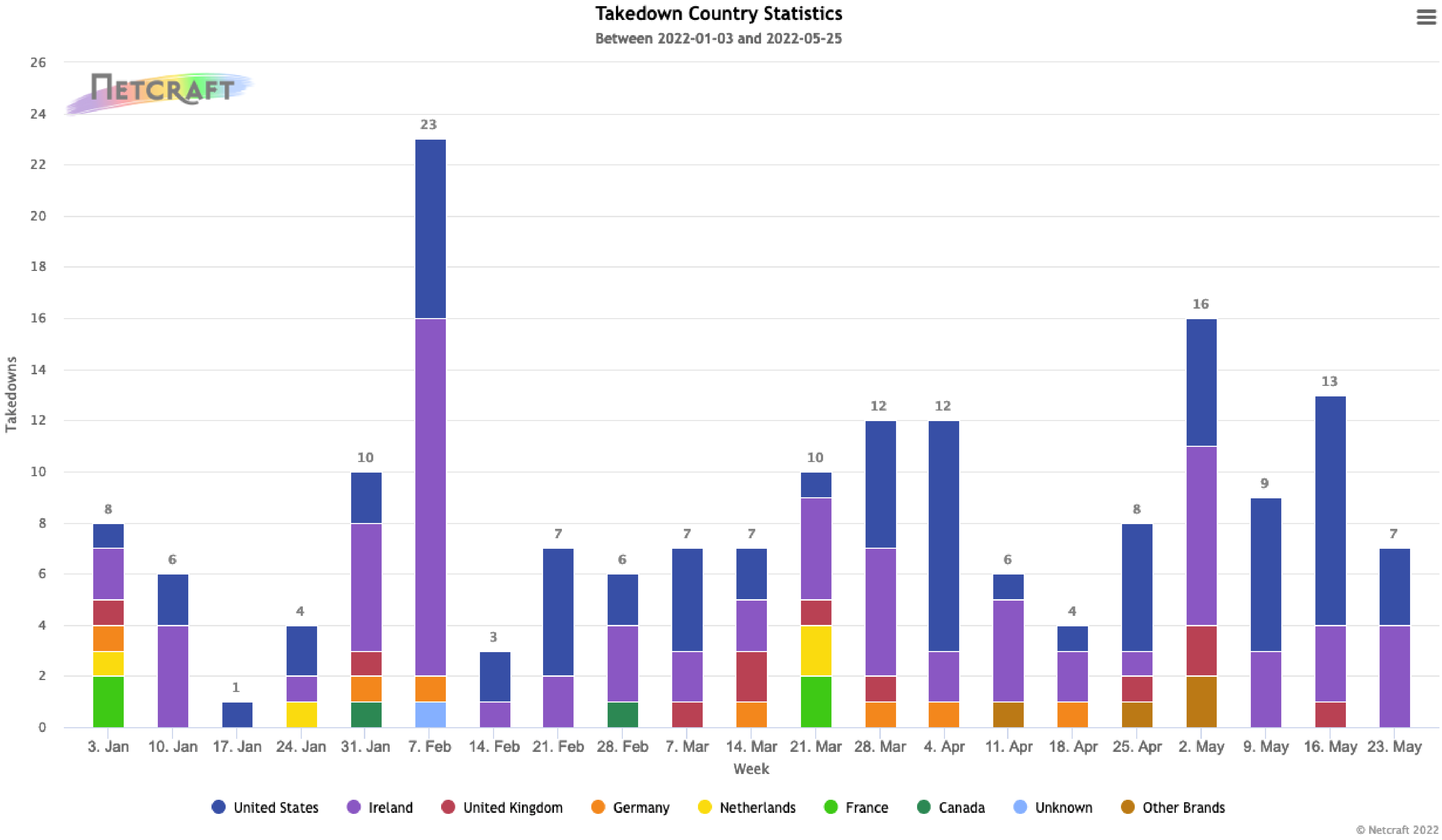


Takedowns by Domain Attack Categorisation

Between 2022-01-03 and 2022-05-25

© Netcraft 2022

3.1 Matters arising



.ie We are Ireland online

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

GNCCB - Suspension Request protocol document

- ➢ Agreement reached with the Garda National Cyber Crime Bureau (GNCCB)
- ➢ Key engagement at meeting on 10 March 2022 (esp. mutual understanding & due process)
- ➢ Agreement confirmed by email 17 May 2022 (circulated with Minutes)
- ➢ Common ground & Goodwill is substantial

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

GNCCB - Suspension Request protocol document

- Agreement reached on the following:-
  - 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

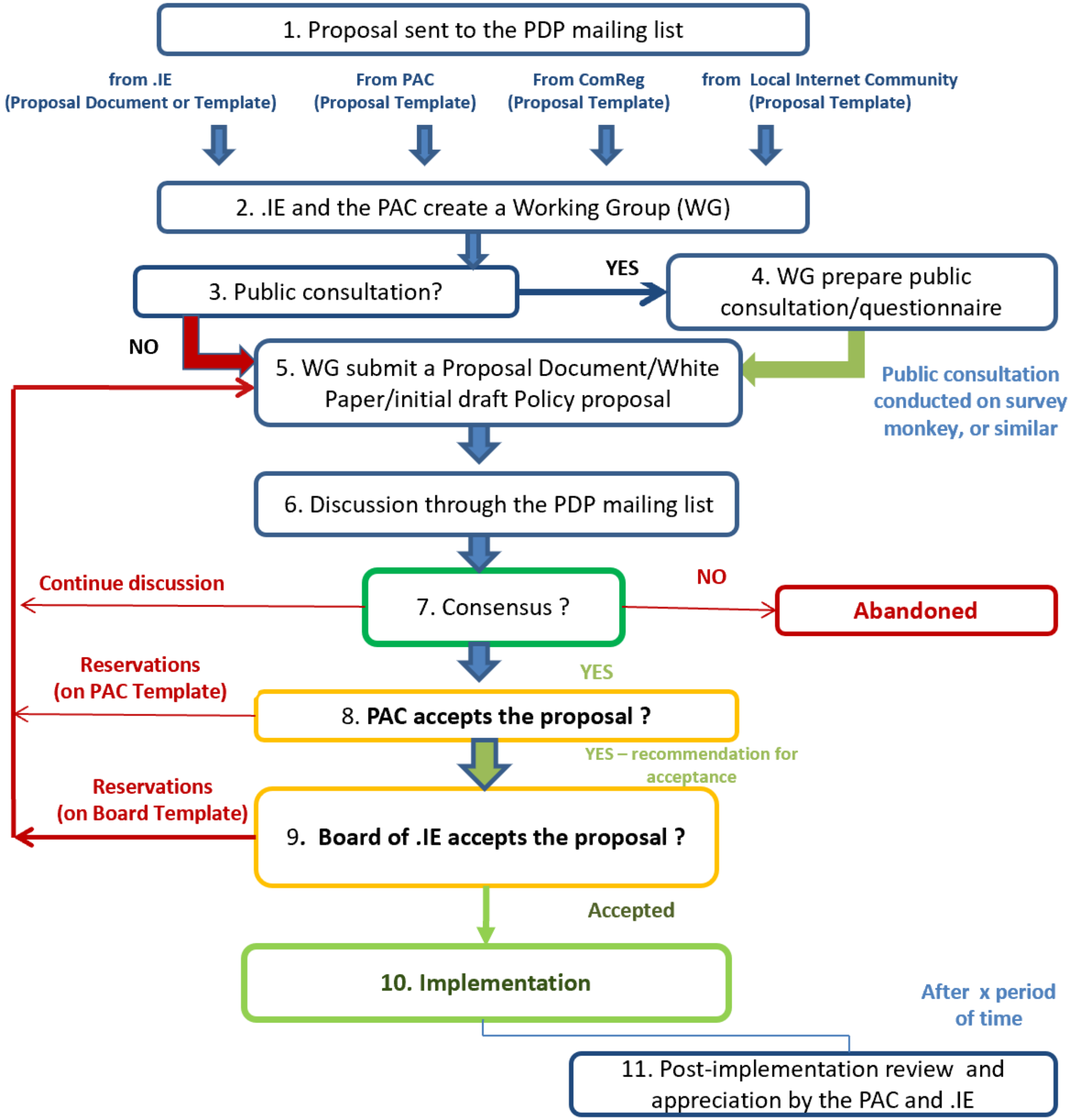
4.1 Handling of illegality and criminal abuse in the .ie namespace

GNCCB - Suspension Request protocol document

- Next Steps ?
  - Communication with wider registrar channel
  - List of contact phone numbers for RAR / .IE / Garda to be created and shared
  - Publicity for the Co-operation Agreement
  - Awareness building with GNCCB professionals
  - Single points of contact (SPOC)
  - Embedding ‘The Process’

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

- Formal Policy Development Process (PDP)
- 10 steps
- Consensus-building phases
- Consultations as required.
- Transparent – on .IE website*



1. Proposal sent to the PDP mailing list

from .IE (Proposal Document or Template)

From PAC (Proposal Template)

From ComReg (Proposal Template)

from Local Internet Community (Proposal Template)

2. .IE and the PAC create a Working Group (WG)

3. Public consultation?

YES

4. WG prepare public consultation/questionnaire

NO

5. WG submit a Proposal Document/White Paper/initial draft Policy proposal

Public consultation conducted on survey monkey, or similar

6. Discussion through the PDP mailing list

Continue discussion

7. Consensus ?

NO

Abandoned

YES

Reservations (on PAC Template)

8. PAC accepts the proposal ?

YES – recommendation for acceptance

Reservations (on Board Template)

9. Board of .IE accepts the proposal ?

Accepted

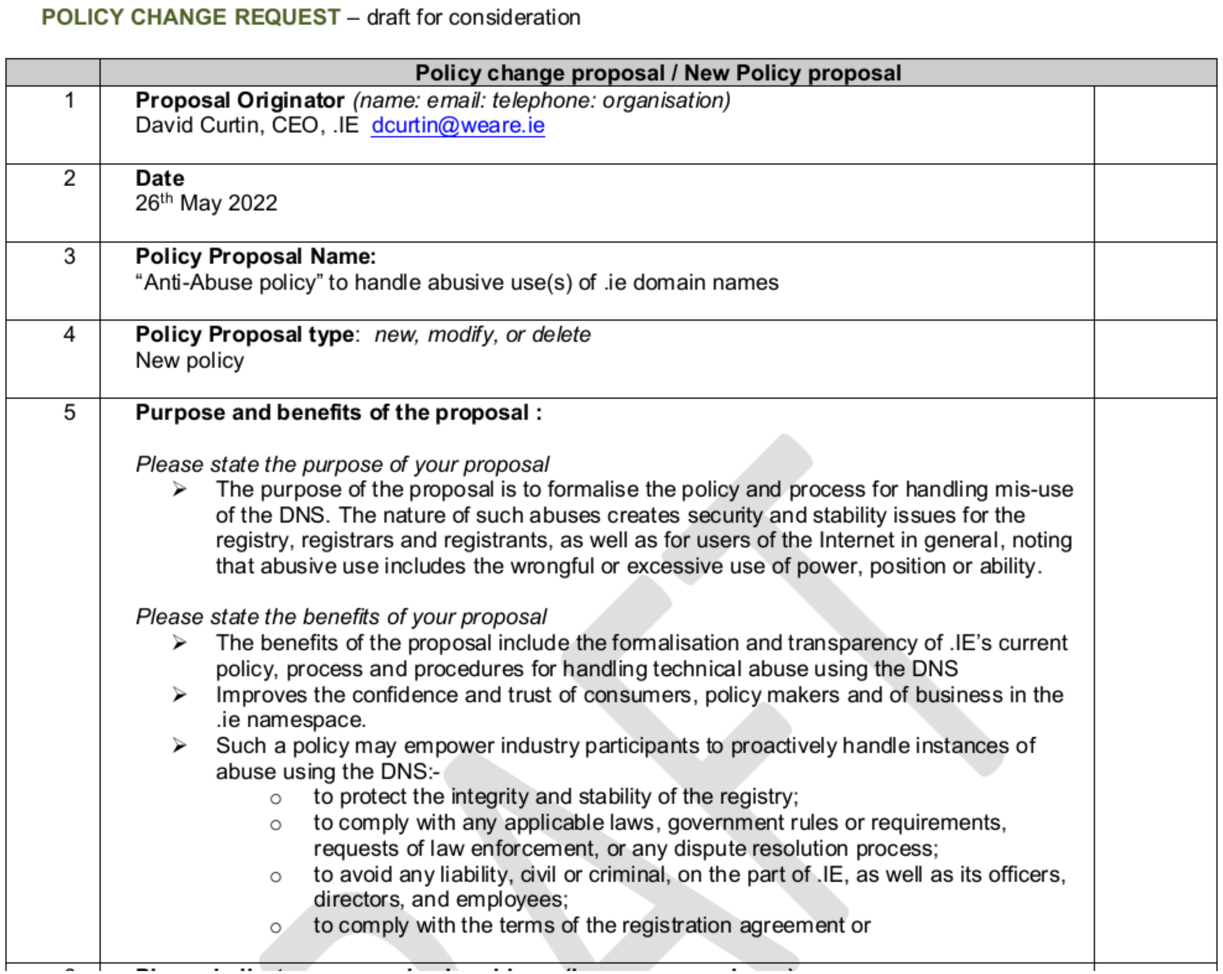
10. Implementation

After x period of time

11. Post-implementation review and appreciation by the PAC and .IE

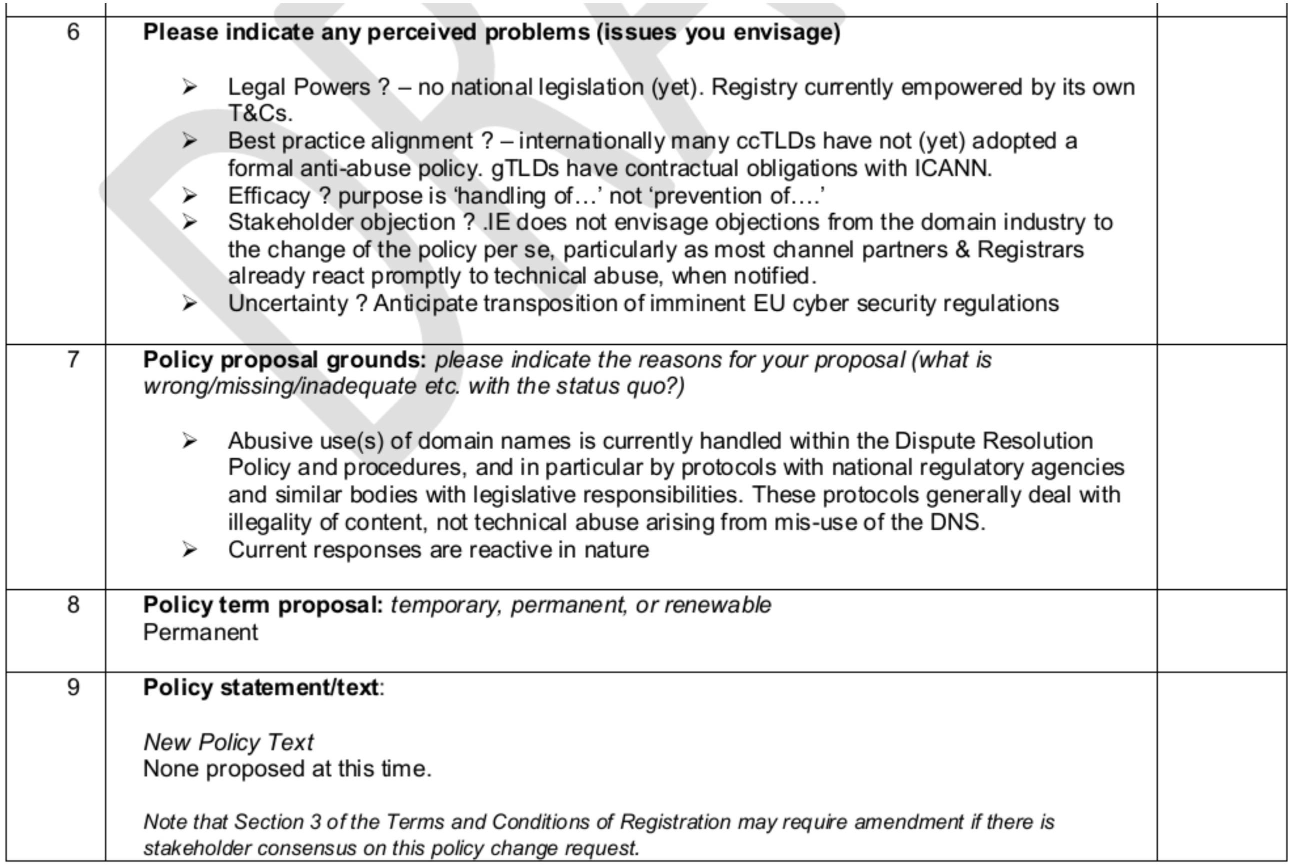
* https://www.weare.ie/policy-development-process/

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



POLICY CHANGE REQUEST – draft for consideration

	Policy change proposal / New Policy proposal	
1	**Proposal Originator** *(name: email: telephone: organisation)* David Curtin, CEO, .IE dcurtin@weare.ie	
2	**Date** 26th May 2022	
3	**Policy Proposal Name:** "Anti-Abuse policy" to handle abusive use(s) of .ie domain names	
4	**Policy Proposal type**: *new, modify, or delete* New policy	
5	**Purpose and benefits of the proposal :** *Please state the purpose of your proposal* ➢ The purpose of the proposal is to formalise the policy and process for handling mis-use of the DNS. The nature of such abuses creates security and stability issues for the registry, registrars and registrants, as well as for users of the Internet in general, noting that abusive use includes the wrongful or excessive use of power, position or ability. *Please state the benefits of your proposal* ➢ The benefits of the proposal include the formalisation and transparency of .IE's current policy, process and procedures for handling technical abuse using the DNS ➢ Improves the confidence and trust of consumers, policy makers and of business in the .ie namespace. ➢ Such a policy may empower industry participants to proactively handle instances of abuse using the DNS:- ○ to protect the integrity and stability of the registry; ○ to comply with any applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process; ○ to avoid any liability, civil or criminal, on the part of .IE, as well as its officers, directors, and employees; ○ to comply with the terms of the registration agreement or	



6	**Please indicate any perceived problems (issues you envisage)** ➢ Legal Powers ? – no national legislation (yet). Registry currently empowered by its own T&Cs. ➢ Best practice alignment ? – internationally many ccTLDs have not (yet) adopted a formal anti-abuse policy. gTLDs have contractual obligations with ICANN. ➢ Efficacy ? purpose is 'handling of…' not 'prevention of….' ➢ Stakeholder objection ? .IE does not envisage objections from the domain industry to the change of the policy per se, particularly as most channel partners & Registrars already react promptly to technical abuse, when notified. ➢ Uncertainty ? Anticipate transposition of imminent EU cyber security regulations	
7	**Policy proposal grounds:** *please indicate the reasons for your proposal (what is wrong/missing/inadequate etc. with the status quo?)* ➢ Abusive use(s) of domain names is currently handled within the Dispute Resolution Policy and procedures, and in particular by protocols with national regulatory agencies and similar bodies with legislative responsibilities. These protocols generally deal with illegality of content, not technical abuse arising from mis-use of the DNS. ➢ Current responses are reactive in nature	
8	**Policy term proposal:** *temporary, permanent, or renewable* Permanent	
9	**Policy statement/text**: *New Policy Text* None proposed at this time. *Note that Section 3 of the Terms and Conditions of Registration may require amendment if there is stakeholder consensus on this policy change request.*	

We are
Ireland online

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.

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

European Commission

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 ?

Common Practice / Best Practice

- 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

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

Registry-Registrar Agreement ("RRA"),

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 ?

Update on developments since PAC#30 :-

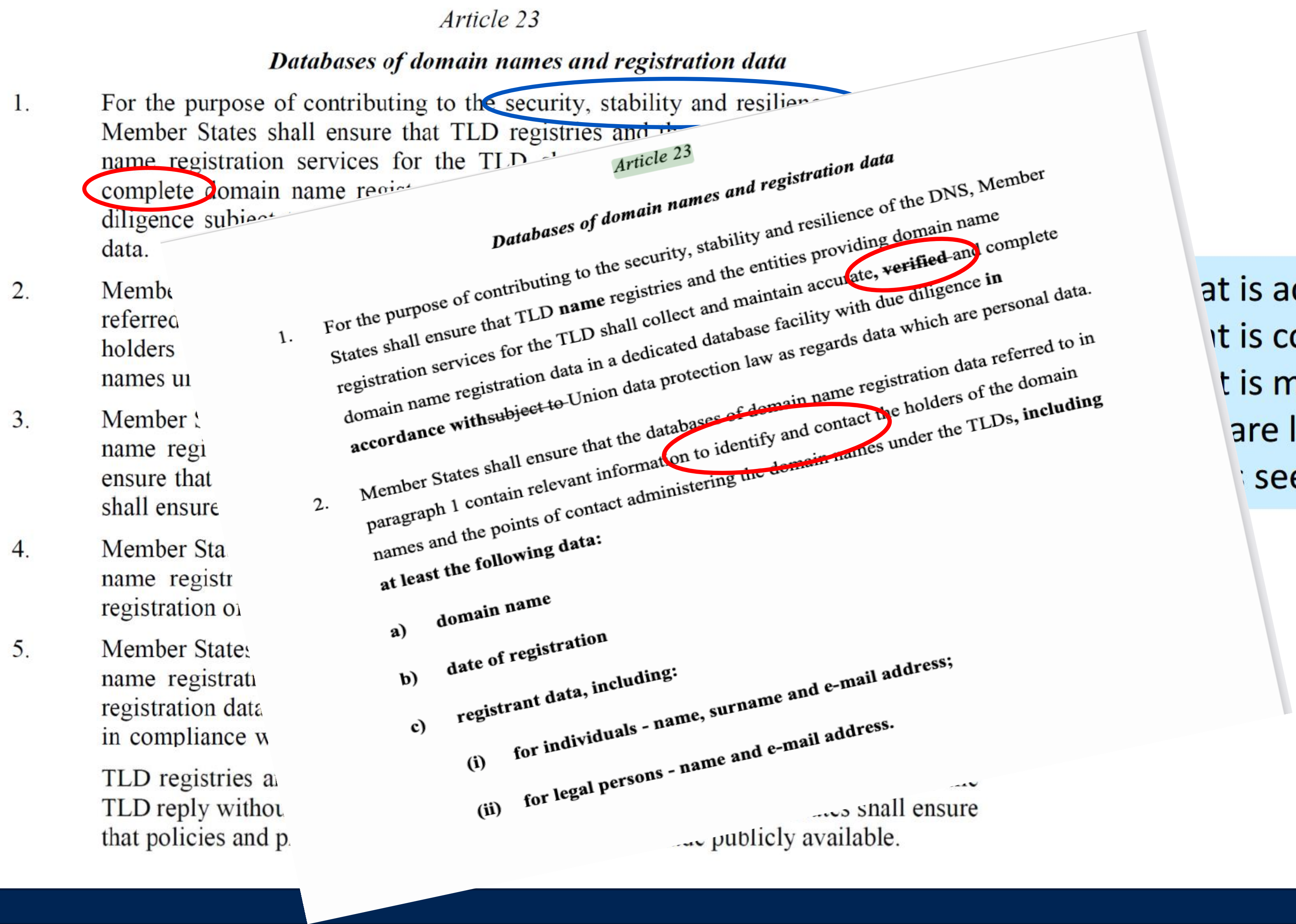
- The French Presidency aims - re Timing / Trilogues / and linking DSA & CER Directives.
- 12 May – Final stage of Trilogue negotiations
- Results ?

- Some positive proposed edits from the **Council** draft…..
  - Article 23 - dilutes "Verification"
  - Less conflict with GDPR in Whois proposals
  - Data Access – to legitimate access seekers
  - Member States would have 21 months to transpose
  - Scope
  - MS shall "require" Vs shall "ensure"

We are
Ireland online

5. NIS 2 – Role for the PAC ?

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



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
complete domain name regis
diligence subject
data.

2. Membe
referred
holders
names ur

3. Member S
name regi
ensure that
shall ensure

4. Member Sta
name registr
registration o

5. Member States
name registrati
registration data
in compliance w

TLD registries a
TLD reply withou
that policies and p
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**

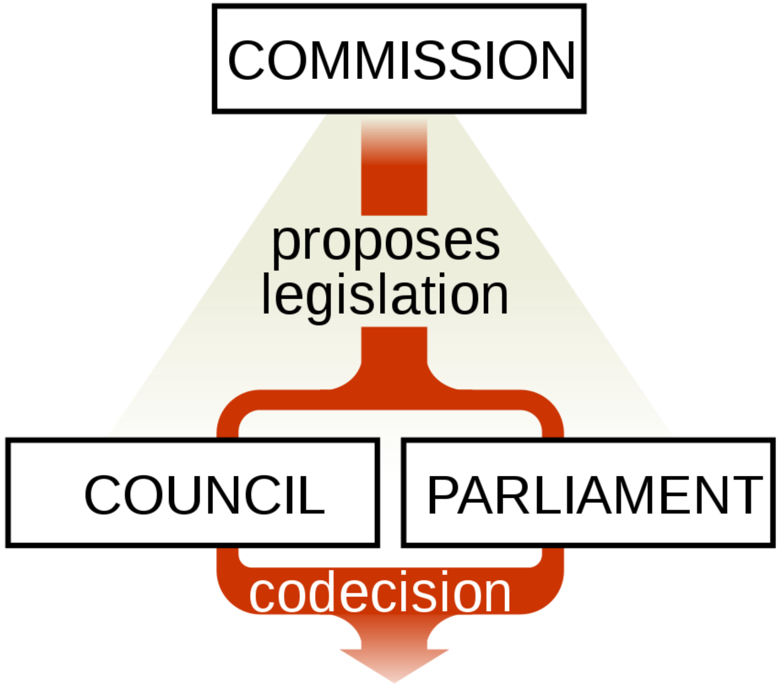
c) **registrant data, including:**

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

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

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

5. NIS 2 – Role for the PAC ?



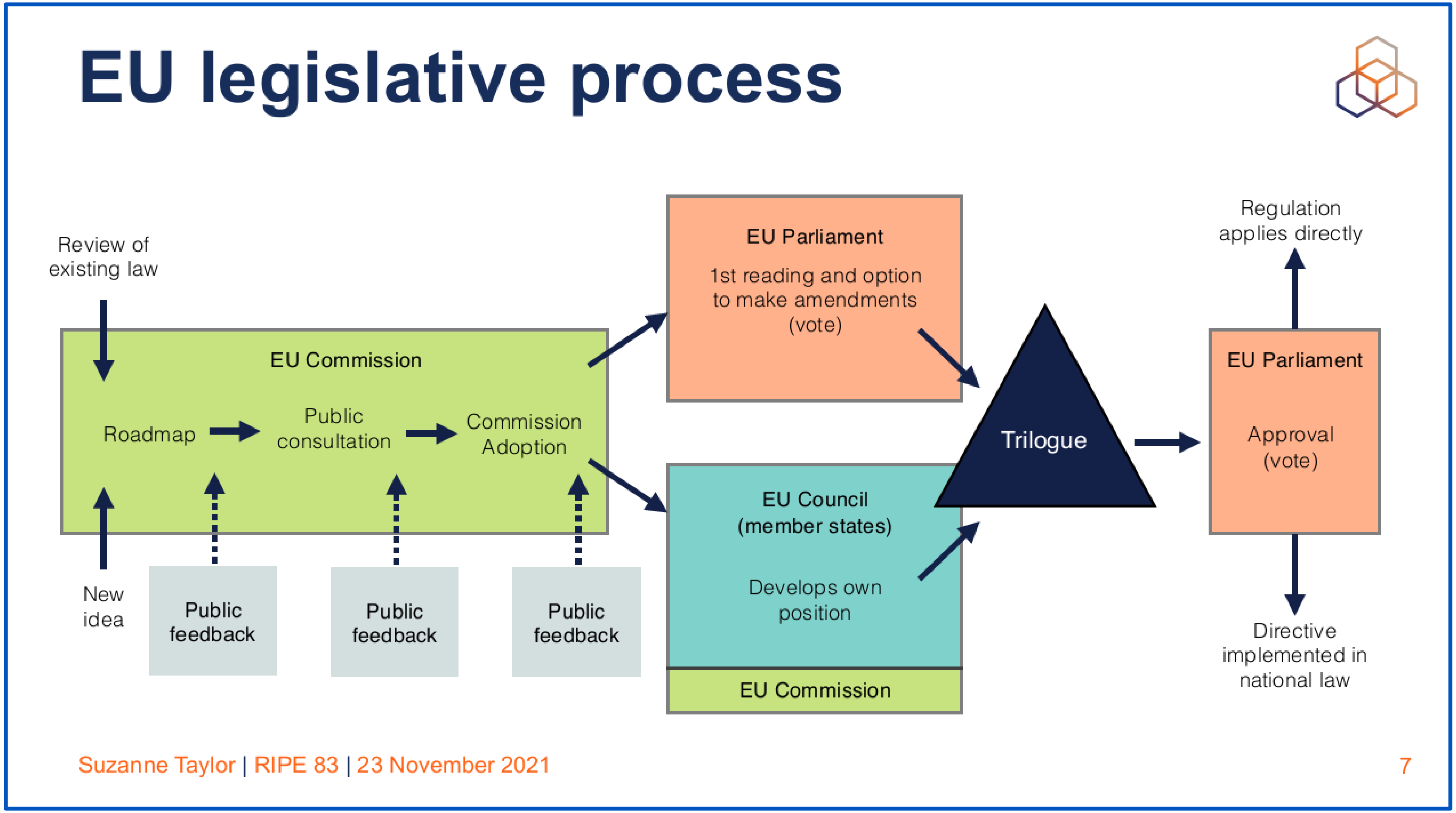
- European Commission (who proposed NIS2 directive)
- European Parliament* (created amendments incl. ITRE draft)
- EU Council of Ministers (Council of the European Union) — *which has possibly the most favourable draft for PAC members*

** The European Parliament's Committees:-*

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

We are
Ireland online

5. NIS 2 – Role for the PAC ?



EU legislative process

Review of existing law

New idea

EU Commission

Roadmap → Public consultation → Commission Adoption

Public feedback

Public feedback

Public feedback

EU Parliament

1st reading and option to make amendments (vote)

EU Council (member states)

Develops own position

EU Commission

Trilogue

EU Parliament

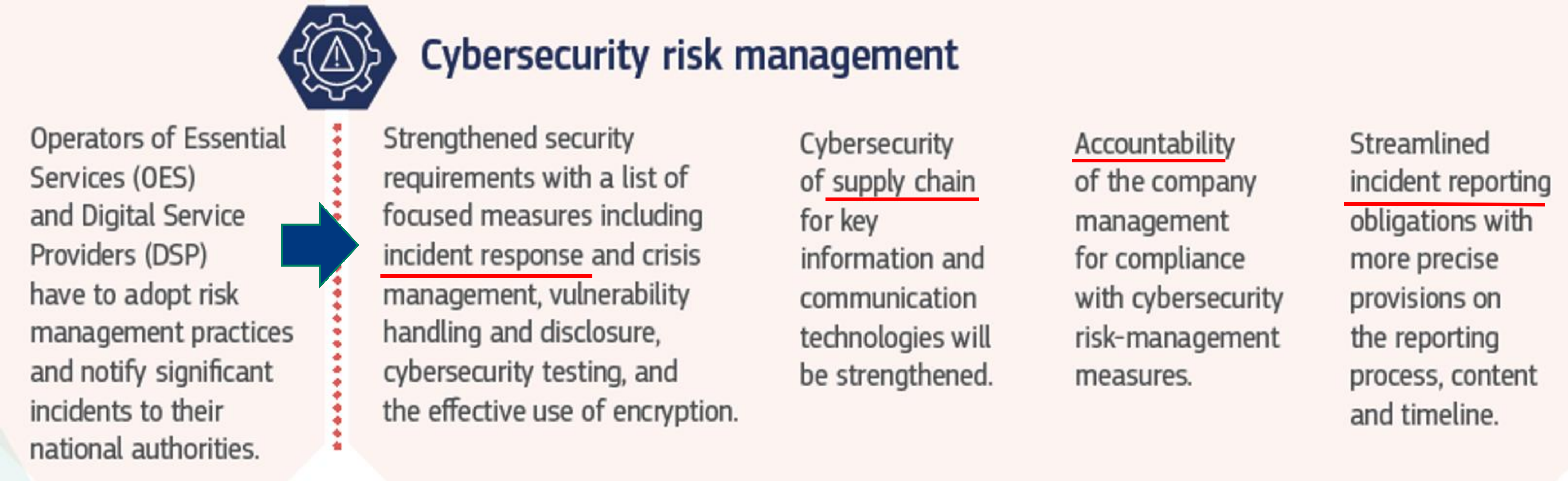
Approval (vote)

Regulation applies directly

Directive implemented in national law

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.

.ie We are Ireland online

5. NIS 2 – Role for the PAC ?

How can we make progress on ‘The Good’

- Legislation is c.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

7. Next Meeting

Proposed date:

Thurs 28th July 2022