.ie We are Ireland online

Policy Advisory Committee

11 November 2021

Meeting - PAC#29

We are
Ireland online

Policy Advisory Committee - Agenda

1. Membership Matters
2. Minutes from the PAC#28 meeting
3. Matters arising
4. Handling of online abuse which uses the .ie namespace
5. NIS 2 – Role for the PAC ?
6. Any Other Business
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 #28 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/

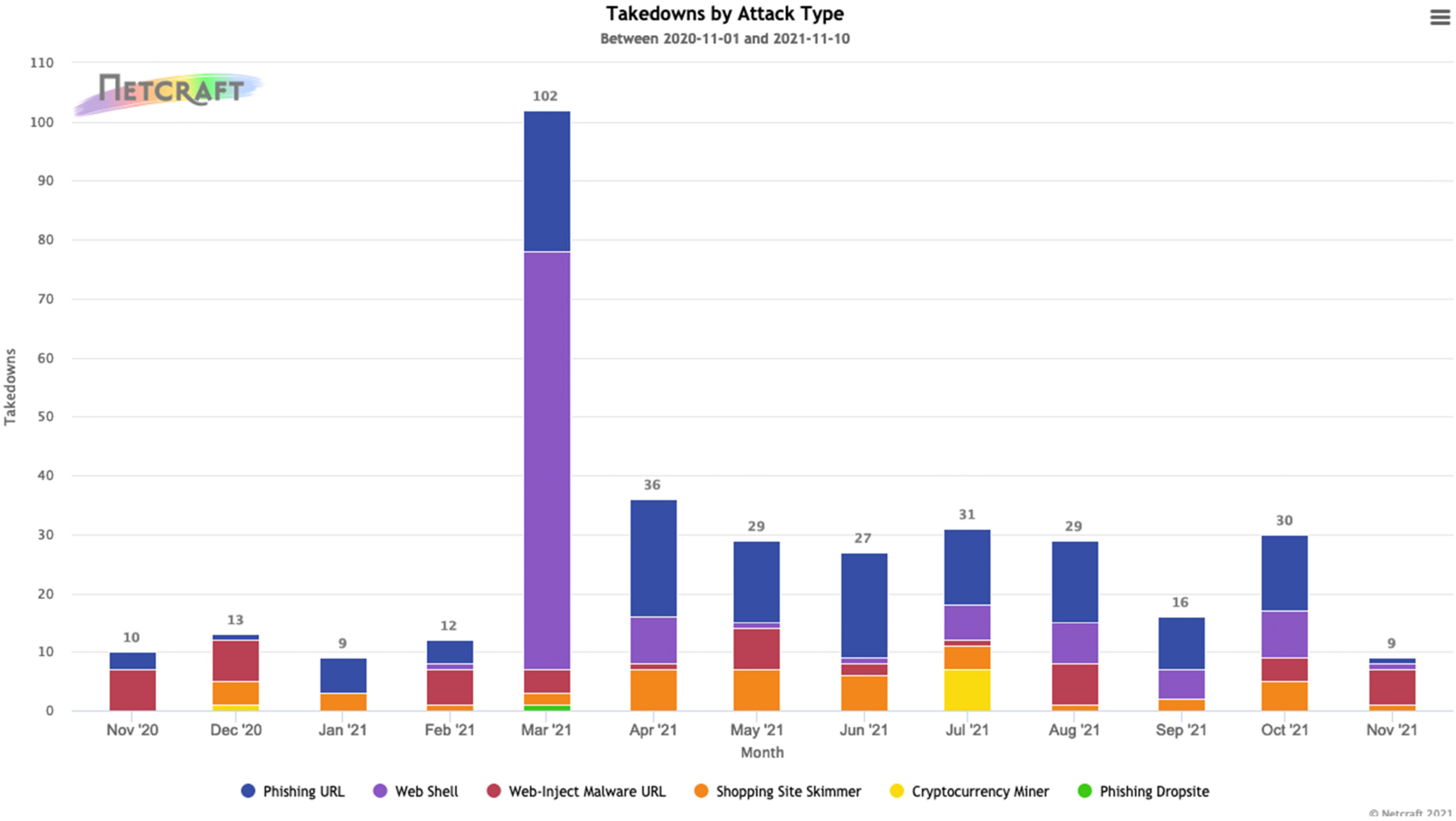
3. Matters arising

- NIS 2
- illegality online - engagement with GNCCB
- VAT-related Policy Change Request
- Digital Services Act
- Technical abuse - Netcraft service

3. Matters arising

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

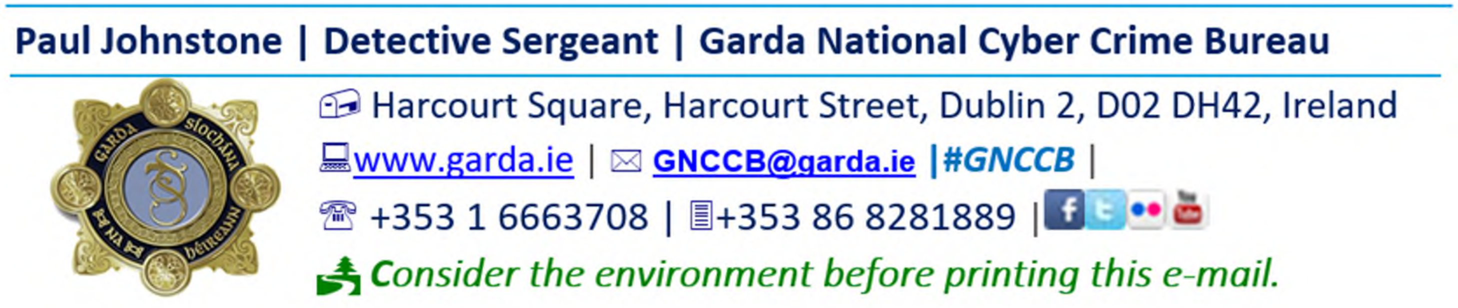
Netcraft service:- 309 attacks handled since commencement in Q1



4. 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

We are
Ireland online

4. 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”)
- 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
- Protocol – TBC:- potential extension to MoU or Cooperation Agreement

5. NIS 2 – Role for the PAC ?

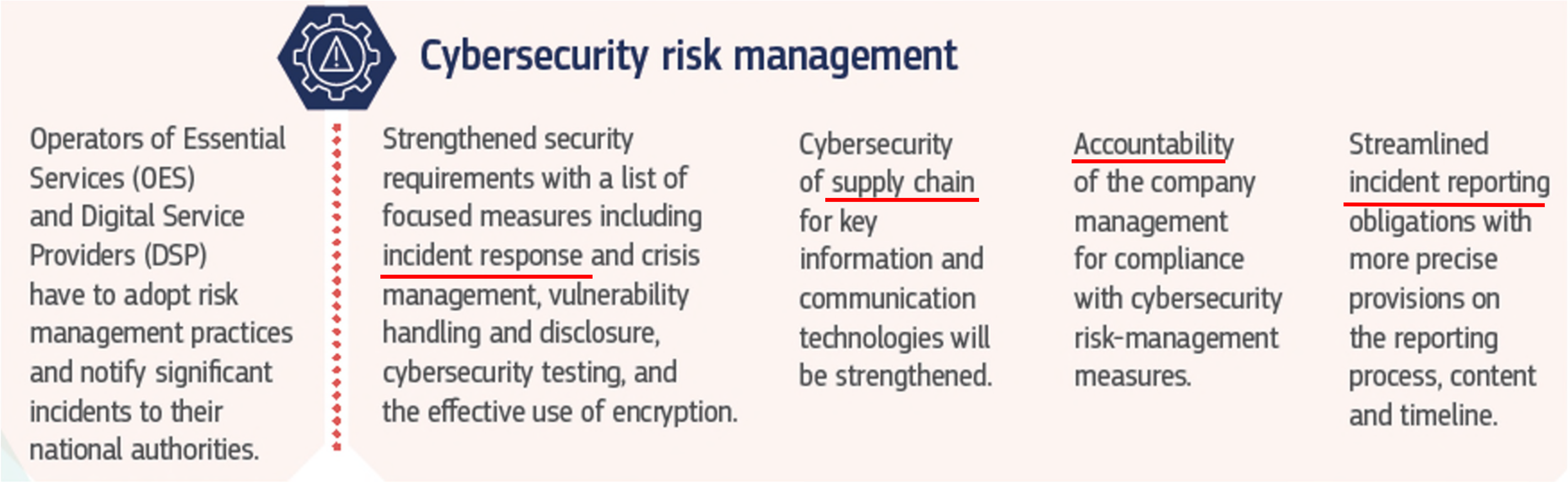
“All businesses are increasingly dependent on third party services - from major cloud providers, through the ecosystem of software as a service (SaaS) providers and managed service providers, to a new world of data and analytics service providers.

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 ?



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.

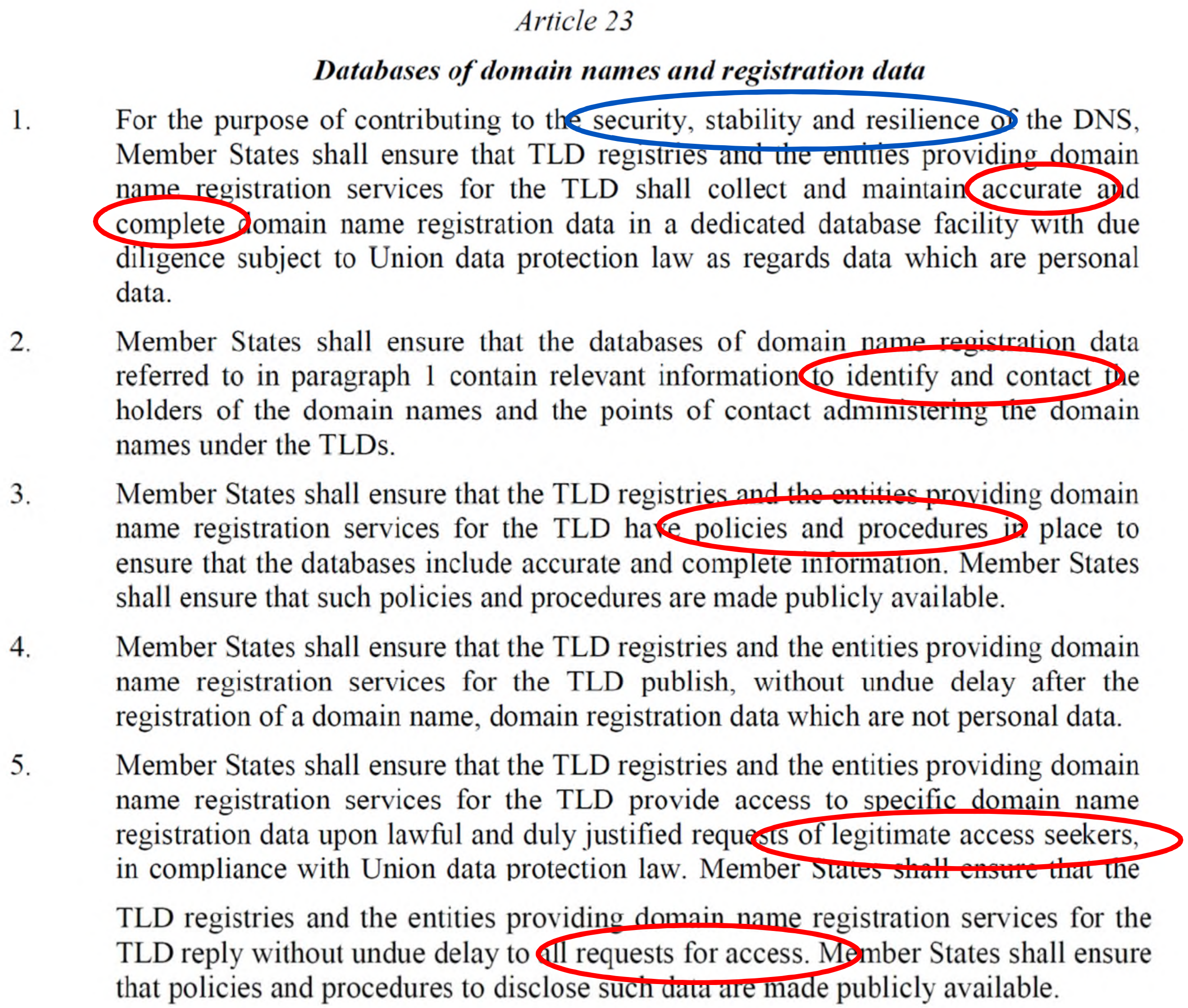
Cybersecurity of supply chain for key information and communication technologies will be strengthened.

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 ?

***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 resilience of the DNS, Member States shall ensure that TLD registries and the entities providing domain name registration services for the TLD shall collect and maintain accurate and complete domain name registration data in a dedicated database facility with due diligence 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.

3. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD have policies and procedures in place to ensure that the databases include accurate and complete information. Member States shall ensure that such policies and procedures are made publicly available.

4. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD publish, without undue delay after the registration of a domain name, domain registration data which are not personal data.

5. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD provide access to specific domain name registration data upon lawful and duly justified requests of legitimate access seekers, in compliance with Union data protection law. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD reply without undue delay to all requests for access. Member States shall ensure that policies and procedures to disclose such data are made publicly available.

- What is accurate?
- What is complete?
- What is maintain?
- Who are legitimate access seekers?

5. NIS 2 – Role for the PAC ?

- Issues include:-
  - Data Verification – compliance costs, KYBC, practicality, ID of forgeries, no eID's in Ireland
  - Data Access – to legitimate access seekers
  - Whois accuracy – is not 'security, stability and resilience of the DNS'
  - Scope – micro-SMEs (threshold # of domains)
  - Electronic identification – no cross border harmonization currently
  - Conflicting obligations váv GDPR
  - Red Tape - weakens competitiveness of the European domain market
  - Supply chain responsibilities

5. NIS 2 – Role for the PAC ?

- Role for the PAC ?
  - Awareness building
  - Burden of regulatory costs
  - Transposition into national legislation – early clarifications
  - Channel needs a clear legal framework (esp. re GDPR provisions)
  - Cyberthreats - improve the resilience and incident response capacities of critical infrastructures

8. Next Meeting

Proposed date:

17th February 2022

We are
Ireland online

Policy Advisory Committee

11 November 2021

Meeting - PAC$^{\#}$29