IGF Dynamic Coalition on Data and Trust

8 December 2021, 11:45-12:45 UTC

DCDT was launched in 2020. We perceived a gap in the DC landscape for sharing best practices on data and trust. A meeting of the (DCDT) took place at the IGF meeting in Katowice, Poland. Due to the ongoing Covid-19 pandemic, the meeting was held virtually. A live stream and transcript of the session can be found at https://www.intgovforum.org/en/content/igf-2021-%E2%80%93-day-2-%E2%80%93-dynamic-coalition-on-data-and-trust

The agenda for this session was guided by input from members of the DCDT on a planning call held in September 2021, and built on themes outlined in the DCDT action plan for 2021 as well as an intersessional panel held at the EuroDIG in Trieste.

The session was entitled *Enhancing community cooperation to ensure effective data management and accuracy.* The session was focused on data management, data accuracy, and the upcoming NIS2 EU directive from different perspectives. An interactive session involving more than 50 participants explored the roles and responsibilities of actors within the DNS environment and related industries for data quality and enhancing trust, in light of the EU proposals to update the NIS2 Directive. The session began with short interventions from five speakers.

Benjamin Bögel of the European Commission provided a general overview of the legislative aims and objectives of NIS2. The original NIS directive was first implemented in 2016, and is now being updated. It is nearing the end of the legislative process. The proposed changes will expand the scope of the directive to cover cloud providers, market places, DNS TLDs and IXPs, and in future it will also include social networks, CDNs, internet service providers and trust service providers. The proposed measures are high level, such as incident reporting within 24 hours of knowledge of an incident, business continuity, supply chain security and others.

Article 23 of the NIS2 directive directly affects the domain name industry, both registries and registrars. It proposes a new legal framework, with the objectives of supporting the fight against DNS abuse, and increasing the overall level of cybersecurity. This will be done by ensuring accuracy of registration data, ensuring registries and registrars will have a firm legal ground to provide access from legitimate access seekers. All requests to access should receive a timely reply (either positive or negative). Article 23 reserves the right to provide guidelines on accuracy, drawing on industry good practices.

Polina Malaja of CENTR focused on the likely impact of Article 23 of the NIS2 on the domain name industry and in particular the requirement for registries and registrars to keep 'accurate and complete' databases of WHOIS data and the provision of lawful access to data. Since the original NIS directive came into force, European ccTLDs have been consistently identified as operators of essential services. This has encouraged ccTLD operators to make additional investments in security and the resilience of their networks. While recognising that the purpose of Article 23 is to prevent and combat DNS abuse, as drafted it is likely to have a limited impact on cybersecurity – such as helping to combat DDoS attacks or DNS hijacking -- while imposing considerable technical and financial burdens on the DNS industry. The speaker expressed the view that there is a risk of shifting the focus in ways that may not have the desired impact on security, and will deflect from ensuring safe and trusted online space. That is a collaborative effort of many actors, based on clear procedure and rule of law.

Dirk Jumpertz of EURid noted that while Article 23 has drawn the attention of the DNS community, the other provisions of the NIS directive also impact ccTLD operators. A key concern is inconsistencies of approach between member states in the transposition of the directive. For example, the scope of the very first directive is different in Belgium, the Netherlands and Luxembourg owing to differences in transposition. It is unclear how registrars or gTLD registries fit into the proposed framework, or whether they meet the definition of essential entities. On Article 23, there is a risk that member states may add further requirements against the accuracy obligation. Lastly, DNS is not about registration data. It is about the DNS - a system that allows us to use the internet as it is. Making sure the DNS is stable and resilient is the most important thing. The DNS must flow - that's what's important.

Keith Drazek of Verisign provided a perspective from a registry operator located outside the European Union. He raised concerns about the impact of the NIS2 language on the multistakeholder community at ICANN, and the territorial impact for those outside the EU. Another important element is the distinction between the roles, responsibilities and capabilities of registries and registrars. Verisign, the .com and .net registry, has not collected or held registrant data for more than 20 years—it is not required to run the registry. Instead, the registrant data are held at the registrar level. Will the NIS2 have the impact of requiring entities to collect data that they do not need, and transfer that data across borders?

Arda Gerkens of the online child protection hotline EOIK provided the perspective of end-users and those defending the rights of children against online exploitation and sexual abuse. The objective of this stakeholder group is to have the swift deletion of such materials. In general, their approach is to identify the hosting party because the

website owner usually does not respond. The majority of image hosting websites are small enterprises with limited resources, there is unlikely to be an accurate abuse address so it is challenging to make contact. While respecting that new regulatory framework imposes compliance burdens, especially on small enterprises, it is important to have accurate data for who owns websites – and this is also good for consumers.

Discussion and Q&A

Giovanni Seppia, External Relations Manager at EURid, moderated an interactive discussion together with Emily Taylor of Oxford Information Labs who was the online moderator.

Scope: One attendee asked whether the intention is to include all TLD operators within the scope of the NIS2 directive, regardless of size? A number of companies have .brand TLDs which are essentially more of an internal matter, and are not providing a service to the public at large, and therefore, are not essential infrastructure. Commission officials confirmed that if a .brand TLD is not provided as a registration service, it is out of scope of the NIS2 directive. The directive only applies to services that are available publicly. Registrars are not generally within scope, but all entities on DNS resolution chain (including resolvers) are within scope.

Transposition. Commission speakers acknowledged that NIS1 has not worked perfectly, and that there had been a great divergence on transposition by member states. The Commission is trying to address this by issuing detailed guidance for transposition, drawing on best practices.

Jurisdiction. The NIS2 will have extra territorial effect. A lot of European companies registered domain names under gTLDs. The general rule is that entities are supervised concurrently in each member state where they operated. For DNS providers, which are highly digitised, there is an exception – they will be supervised by the member state where the entity has its main establishment or, if located outside the EU, where it has its representative.

There was a question about interplay between the proposed Article 23 obligations, and GDPR requirements for data minimisation. There was a suggestion that the key requirement should be the ability to contact the registrant. Requirements over and above an email address run the risk of imposing barriers to entry or creating unintended consequences such as conflict with other laws internationally. Another speaker agreed that ‘contactability’ is the key concept.

Concerns were raised in relation to the definition of **legitimate access seekers**. If it is limited only to law enforcement, that would exclude private sector organisations investigating harms, many of whom work closely with law enforcement.