

Beyond Budapest: The UN Cybercrime Treaty and DNS Abuse

Oct. 20th, 2020

ICANN 69

At-Large Policy Session

CROSS-COMMUNITY INTERACTION

agenda

16:30 - 16:40 - Introduction and welcome
(Joanna Kulesza) - 14:30-14:40 UTC


16:40 - 16:55 - Current legislative processes
and their impact onto ICANN's DNS Abuse
policies - what to expect (Matthias
Hudobnik, ALAC EURALO) - 14:40-14:55 UTC

16:55 - 17:10 - Cybercrime and DNS Abuse
(Alexander Seger, Head of the Cybercrime
Division and Executive Secretary of the
Cybercrime Convention Committee, Council
of Europe) 14:55-15:10 UTC

17:10 - 17:30 - Q&A (Joanna Kulesza) - 15:10-
15:30 UTC

background

DNS Abuse and cybercrime – comparing notes



DNS Abuse Framework

DNS Abuse Framework

The Framework to Address Abuse launched earlier this year in October with eleven original signatories. We are proud to announce that there are now 48 signatory registrars and registries that are bound by these principles. We encourage any other registrar or registry that does not follow these principles yet to add their names so that we can all do our part to make the DNS and the Internet a more secure space

Please see the [latest version of the Framework here](#), and if you are interested in joining please contact one of the participating registrars or registries.

Framework to Address Abuse

- „DNS Abuse is composed of five broad categories of harmful activity insofar as they intersect with the DNS:
- **malware,**
- **botnets,**
- **phishing,**
- **pharming, and**
- **spam** (when it serves as a delivery mechanism for the other forms of DNS Abuse).”

Framework to Address Abuse

- „When Should a Registrar or Registry Act on Website Content Abuse?
- (...) we believe there are certain forms of Website Content Abuse that are so egregious that a registry or registrar should act when provided with **specific and credible notice**.

You are here: [Cybercrime](#)



Budapest Convention and related standards



Explanatory Reports
and Guidance Notes

www.coe.int/cybercrime

The **Convention on Cybercrime** of the Council of Europe (CETS No.185), known as the Budapest Convention, is the only binding international instrument on this issue. It serves as a guideline for any country developing comprehensive national legislation against Cybercrime and as a framework for international cooperation between State Parties to this treaty.

The Budapest Convention is supplemented by a **Protocol on Xenophobia and Racism** committed through computer systems.

▶ [The Budapest Convention \(CETS 185\)](#)



Ad hoc committee established by General Assembly resolution 74/247

Through its resolution [74/247](#), adopted on 27 December 2019, the General Assembly, *inter alia*, took note of Commission on Crime Prevention and Criminal Justice resolution [26/4](#) of 26 May 2017, in which the Commission expressed appreciation for the work done by the [Expert Group to Conduct a Comprehensive Study on Cybercrime](#) and requested the Expert Group to continue its work, with a view to examining options to strengthen existing responses and propose new national and international legal or other responses to cybercrime, and in this regard reaffirmed the role of the United Nations Office on Drugs and Crime (UNODC).

In the same resolution, the General Assembly decided to establish an **open-ended ad hoc intergovernmental committee of experts, representative of all regions, to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes**, taking into full consideration existing international instruments and efforts at the national, regional and international levels on combating the use of information and communications technologies for criminal purposes, in particular the work and outcomes of the open-ended intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime

The General Assembly also decided that the ad hoc committee shall convene **a three-day organizational session in August 2020, in New York, in order to agree on an outline and modalities for its further activities**, to be submitted to the General Assembly at its seventy-fifth session for its consideration and approval.



United Nations Update: Cyber-Related Discussions

ICANN Government & Intergovernmental Organization (IGO) Engagement

Veni Markovski
GE-005
15 July 2020

Scoping questions:

- Is there a link between DNS Abuse and cybercrime laws and international treaties?
- Is there a role for the **ICANN community** in the ongoing international discussions?
- How to effectively protect end users from online/DNS abuse? Is it time to move beyond law?