



United Nations

Department of
Economic and
Social Affairs



Inter-Parliamentary Union
For democracy. For everyone.



የኢ.ፌ.ዲ.ሪ
የሕዝብ ተወካዮች
ምክር ቤት
HOUSE OF
PEOPLES REPRESENTATIVES
OF THE FDRE

Internet Governance Forum 2022 | Parliamentary track

Addressing cyberthreats: National, regional and international approaches

Concept note

CONTEXT

From 28 November to 2 December 2022, the Government of Ethiopia will host the United Nations 17th Internet Governance Forum (IGF 2022) under the overarching theme *Resilient Internet for a Shared Sustainable and Common Future*. Participants from around the world are expected to take part in this event in Addis Ababa and online.

In recent years, the IGF has sought to strengthen the parliamentary dimension of the forum by facilitating the participation of parliamentarians in discussions on some of the most pressing issues related to the use, evolution and governance of the Internet and related digital technologies. Participants in the [2019](#), [2020](#), and [2021](#) parliamentary events recommended, among others, that national parliaments cooperate and exchange good practices on dealing with digital policy issues, and strengthen their engagement in international processes.

In 2022, the IGF parliamentary track started with a digital policy symposium held in the context of the Africa IGF, on the theme [The role of parliamentarians in shaping our common digital future: An African perspective](#). Building on this, the track will continue at the 17th IGF in Addis Ababa with a series of parliamentary activities to be held on 30 November and 1 December on the theme *Addressing cyberthreats: National, regional and international approaches*. In the spirit of the [United Nations \(UN\) General Assembly resolution 74/304](#), these activities will be **jointly organized by the United Nations Department of Economic and Social Affairs (UN DESA), the Inter-Parliamentary Union (IPU) and the House of Peoples' Representatives of Ethiopia**.

KEY TOPICS

As the Internet and digital technologies increasingly shape our economies and societies, they also create vulnerabilities for individuals, public and private entities, critical infrastructures, and much more. The cyber threat landscape is a complex one, including issues as diverse as denial of service attacks, malware and ransomware, cyberattacks on supply chains and providers of essential services, and the weaponization of digital technologies.

How ready are countries to deal with these and other cyberthreats? What policy, regulatory and legislative measures are or need to be put in place to increase the level of cybersecurity and address cybercrime? Are national authorities empowered to implement such frameworks? And how to leverage multistakeholder, multisector and multi-level cooperation to create a more secure cyberspace? These and similar questions will be discussed at the IGF 2022 parliamentary track, offering parliamentarians an opportunity to exchange good practices, discuss challenges and solutions, and engage with other stakeholders in a dialogue aimed to help inform efficient and effective policy making and implementation.

OBJECTIVES

- Update members of parliaments (MPs) on the continuously changing landscape of cyberthreats and their implications for individuals, the society and the economy.
- Foster dialogue and exchanges of experiences among MPs on national approaches to protecting cybersecurity and addressing cybercrime.
- Discuss the role of MPs and legislation in shaping a safer and more secure digital space.
- Explore challenges – and potential solutions – related to the implementation and enforcement of legislative frameworks related to cybersecurity and cybercrime.
- Expose MPs to UN-level processes focused on cybersecurity and cybercrime: the [Open-ended Working Group on security of and in the use of information and communications technologies](#) (OEWG) and the [Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes](#) (Ad Hoc Committee).
- Engage in a dialogue with other actors (business sector, technical community, civil society) on multistakeholder approaches to addressing cyberthreats.

OUTPUT

Parliamentarians from around the world are invited to discuss the proposed issues with experts, share their views, explore the questions at hand, and exchange opinions and experience on (existing or potential) legislative solutions. The main messages that emerge from these exchanges (with potential guidelines, suggestions and recommendations for parliaments) will be captured as the formal output of the IGF 2022 parliamentary track.

PLAN OF ACTIVITIES

The programme below is indicative at this stage and will be shaped further in the lead-up to IGF 2022.

Calendar of activities	
Date and time	Focus
Online introductory session	
10 November, 13:00 UTC	<p>[optional] What is the IGF and what to expect from the meeting and the parliamentary track?</p> <ul style="list-style-type: none"> MPs will be invited to an online discussion to set the scene for IGF 2022 and the parliamentary track.
Parliamentary events at IGF 2022 30 November and 1 December (Addis Ababa & online)	
30 November, 13:50 – 14:50 UTC+3	<p>[Parliamentary session 1] Policy, regulatory and legislative frameworks for cybersecurity and cybercrime: national and regional approaches</p> <ul style="list-style-type: none"> How can policies, regulations and legislation help strengthen cybersecurity and address cybercrime? What should such frameworks look like? What examples of good (and maybe not so good) practices are out there? How can parliaments help strengthen national cyber capabilities?
30 November 15:05 – 16:35 UTC+3	<p>[Parliamentary session 2] Implementation of cybersecurity and cybercrime frameworks: challenges and solutions</p> <ul style="list-style-type: none"> What happens after the adoption of cybersecurity and cybercrime policy/regulatory/legislative frameworks? Are relevant national authorities adequately equipped (e.g. financial resources, human and institutional capacities) to implement such frameworks? If not, how to ensure this is the case? What does it take to ensure efficient and effective regional, international, and multistakeholder cooperation in implementing such frameworks?
1 December, 09:30 – 11:00 UTC+3	<p>[Parliamentary session 3] Unpacking UN processes</p> <ul style="list-style-type: none"> GGE: What were the main outcomes of the group and what is happening with them? OEWG: What has the group achieved so far? What challenges does it face? And what is expected from the group? Ad Hoc Committee: What are the main issues under

	<p>consideration? Are these areas of agreement and disagreement?</p> <ul style="list-style-type: none"> • How can parliamentarians help raise awareness about these processes and strengthen the engagement of national actors?
<p>1 December, 13:45 – 15:00</p>	<p>[Roundtable] The role of parliaments in addressing cyberthreats</p> <ul style="list-style-type: none"> • What roles can/should parliaments play in fostering strengthened multistakeholder cooperation at national, regional and international levels? • What are the roles and responsibilities of various actors (governments, parliaments, private sector, technical community, civil society) in addressing cyberthreats and contributing to the creation of a safer and more secure digital space? • What key international multistakeholder initiatives are in place and how can their work be strengthened?
<p><i>MPs are cordially invited to actively participate in all other IGF 2022 sessions taking place during the week and contribute their views and experiences to the discussions. The overall programme will be made available on the IGF website.</i></p>	