XV Ukrainian Internet Governance Forum IGF-UA

Kyiv, 19-21 November 2025
Annual Report

CONTENT

INTRODUCTION

The first Ukrainian Internet Governance Forum (IGF-UA) took place in September 2010 in Kyiv. Since then, the annual IGF-UA has become a continuation of a global series of Forums aimed at discussion of the most important issues of information society development, consolidation of the efforts of state authorities, business, Internet society, professional and academic elites aimed at accelerating the implementation of IT capabilities, creating conditions for comprehensive development of Internet technologies for the public benefit. IGF-UA has always been gathering participants from around the world representing international organizations, state authorities, non-governmental and commercial organizations in the field of ICT and the mass media.

Due to the military aggression of the Russian Federation against Ukraine, the Forum Organizing Committee chose a hybrid format for holding the IGF-UA. The main part of the participants used the video conference mode. The offline form of participation was provided for the administrative group, some moderators and speakers and was organized in a protected point of invincibility in Kyiv, created on the site of the Adamant company. In addition, online broadcasting and automatic translation of speeches (Ukrainian/English) with subtitles were provided.

The 16th IGF-UA was attended by participants from Ukraine and a number of other countries of the world, representing government institutions, I* organizations, the private sector, civil society, academic and technical communities, and the media.

IGF-UA continues to be an important component of the national discussion about the future of the Internet in Ukraine, Europe and the world.

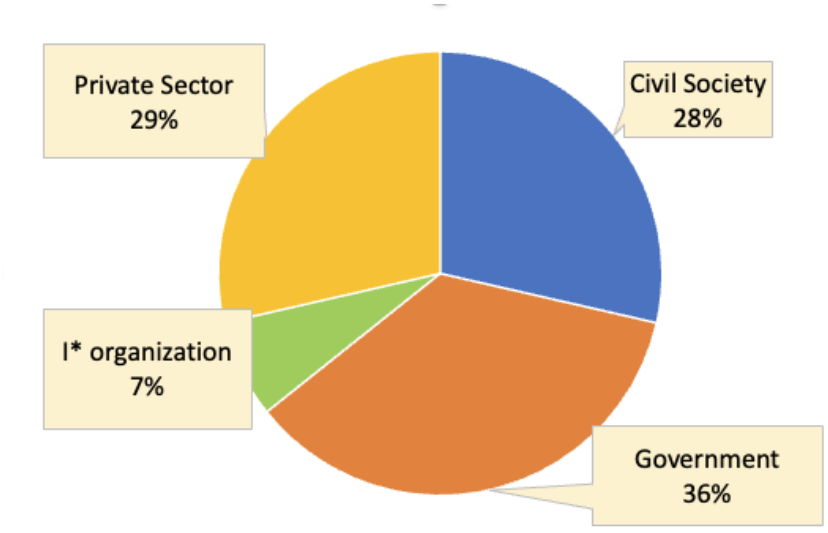
ORGANIZATIONAL PROCESS

The activities of the IGF-UA Organizing Committee are based on the "Guidelines for Holding the Ukrainian Internet Governance Forum IGF-UA (Memorandum of Understanding)". This document was developed to implement the decisions made during the 4th IGF-UA, *https://2013.igf-ua.org/principles.*

The Orcommittee is composed of 14 people who represent various groups in a balanced manner: civil society, government institutions, the private sector and I*-organizations.

Members of the IGF-UA Organizing Committee

	Name	Organization	Stakeholder group
1	Tetyana Dolinska	Ukrainian Southern Network Information Center	Private Sector
2	Valeriya Dubytska	Independent expert, representative of Youth IGF-UA organizing community	Civil society
3	Dmytro Kokhmaniuk	Independent Expert	Private sector
4	Volodymyr Kukovskyi	Organizing Committee Secretary	Civil society
5	Olena Kushnir	Ukrainian Internet Association	Private sector
6	Ivan Pietukhov	Commission for Science and IT, Ukrainian League of Industrialists and Entrepreneurs	Civil society
7	Oksana Prykhodko	European Media Platform, International NGO	Civil society
8	Oleksiy Semenyaka	RIPE NCC	I*-organizations
9	Svitlana Tkachenko	Hostmaster Ltd.	Private sector
10	Mykhailo Pokydko	Department of Digital Transformation of the State Special Communications Administration	Government institutions
11	Andriy Okayevych	Security Service of Ukraine	Government institutions
12	Yuriy Matsyk	Governmental Advisory Committee (GAC) at ICANN Governmental organizations	Government institutions
13	Hanna Postoliuk	Cyber Diplomacy Department of the Ministry of Foreign Affairs	Government institutions
14	Serhiy Shtepa	Parliamentary Committee for Digital Transformation	Government institutions



Participation of representatives of various stakeholders in the IGF-UA-2025 Organizing Committee

The IGF-UA Organizing Committee carried out its work not only during the period of direct preparation of the IGF events, but also throughout the entire period between the 15th and 16th IGF-UA. During this period, six meetings of the Organizing Committee were held – 08.07.2025, 24.07.2025, 05.09.2025, 02.10.2025, 11.11.2025, 17.11.2025 (meeting minutes in Ukrainian – http://igf-ua.org).

The Forum was organized by the Internet Association of Ukraine (InAU), the Science and IT Commission of the Ukrainian Union of Industrialists and Entrepreneurs (USPP), the European Media Platform NGO, and Hostmaster LLC with the support of the Verkhovna Rada of Ukraine Committee on Digital Transformation, the Ministry of Foreign Affairs of Ukraine, the Ministry of Digital Transformation of Ukraine, the National Commission for State Regulation of Electronic Communications, Radio Frequency Spectrum and Postal Services (NKEC), and sponsored by RIPE NCC (RIPE Network Coordination Centre) and ICANN (Internet Corporation for Assigned Names and Numbers).
The organizers of IGF-UA and the organizations that supported the Forum have a balanced representation of various stakeholder groups:

- Civil society: Commission for Science and IT of the Ukrainian League of Industrialists and Entrepreneurs; International NGO European Media Platform;
- Private sector: Ukrainian Internet Association, Hostmaster LLC;
- I*-organizations: RIPE NCC; ICANN;
- Government institutions: Parliamentary Committee for Digital Transformation, Ministry of Foreign Affairs of Ukraine, Ministry of Digital Transformation of Ukraine, National Regulatory authority of Ukraine in electronic communications.

AGENDA

The main goal of IGF-UA is to develop Internet governance in Ukraine through multilateral dialogue, as well as to promote the development of partnerships to coordinate stakeholders for the best and most balanced development of the Internet in the interests of the citizens of Ukraine. Based on this goal, the Organizing Committee has identified a list of key topics for discussion at IGF-UA. Based on these, 7 sections have been formed for discussion and debate.

Section 1. Cyber section on digital cyber resilience and artificial intelligence.

Section 2. De-occupation of the Internet and reducing Russia's influence in the digital space.

Section 3. The role of women in the field of electronic communications.

Section 4. Resilience of Internet access during war (blocking, Internet shutdowns).

Section 5. Approaches of the Council of Europe and the UN to combating cybercrime.

Section 6. Current issues of the domain space.

Section 7. The Future of Internet Governance and the IGF Mandate.

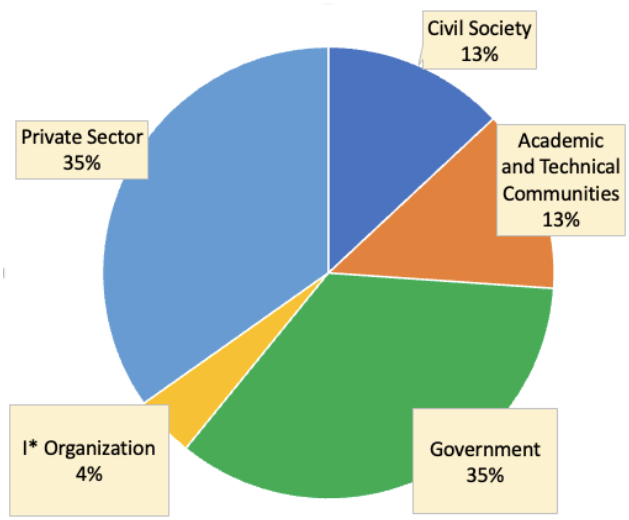
The Closing Plenary Session summarized the Forum.

You can find the full version of the 16th IGF-UA programme – at https://2025.igf-ua.org/programs

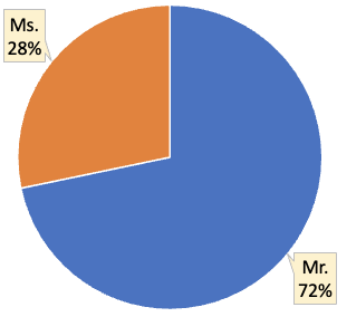
PARTICIPANTS

The Forum was attended by a significant number of participants from Ukraine and a number of other countries, representing government agencies, international organizations, the private sector, civil society, the academic and technical community, the media and youth. Since the forum was held in a video conference mode, everyone could watch its work in real time without registration. Registered Participants had the opportunity to participate directly in the forum. Participants without registration had the opportunity to provide feedback via chat and e-mail.

Full list of registered Participants of IGF-UA-2025 – *https://2025.igf-ua.org/participants*



Representation of various stakeholder groups among the IGF-UA-2025 registered participants



Gender composition of participants who registered for the IGF-UA-2025

FINANCING

Following the Guidelines of the Ukrainian Internet Governance Forum IGF-UA (Memorandum of Understanding), the necessary resources in terms of the preparation and conduct of the Forum were provided by the IGF-UA Organizers and Sponsors.

IGF-UA-2025 Budget

Sponsor	Balance from 2024	Proceeds in 2025	Respon-sible	Currency exchange date	Currency exchange rate	Amount of currency sold	Amount received in UAH	Expenses in 2025		Balance
								Expense items	Amount, UAH	
IGF-SA	535 USD		Member of the Organizing Committee O.Prikhodko	Sept 2025	41,67	535 USD	22 293,45 ₴	IGF-UA stickers with delivery	25 850,00 ₴	
RIPE NCC	380 UAH	1 000 EUR					380,00 ₴			
	500 EUR				47,11	115 EUR	5 417,65 ₴	Banking services	2 240,00 ₴	
				Nov 2025	48,58	1 385 EUR	67 283,30 ₴	Organization of the work of the point of invincibility	24 290,00 ₴	
								Transportation costs	5 650,00 ₴	
								First aid kits	28 620,00 ₴	
								Bracelets	900,00 ₴	
								Promo Youth IGF-UA	700,00 ₴	
								Banking services	4 801,10 ₴	
Total received after currency sale + available UAH:							**95 374,40 ₴**	**Costs 2025:**	**93 051,10 ₴**	**2 323,30 ₴**
Expected to receive from ICANN:							**500,00 EUR**			

Remaining balance will be used to hold IGF-UA events in Ukraine in 2026.

CONCLUSIONS

The panel moderators made their final statements at the final discussion panel. They emphasized the fruitfulness of the discussions, the importance of implementing international experience in Ukraine, and the role of the 16th IGF-UA discussions in further improving Internet governance.

Section 1. **CYBER SECTION IN THE AREAS OF DIGITAL CYBER RESILIENCE AND ARTIFICIAL INTELLIGENCE**

Moderator: Ivan Pietukhov (Commission for Science and IT, Ukrainian League of Industrialists and Entrepreneurs)

The section considered the current issues of ensuring the defense and private sectors with digital cyber resilience in conditions of war and changes in national legislation, namely, the transition from the CSII to the RMF and the implementation of NIS 2 without a preparatory period, practical cases were also considered and an exchange of experience in the implementation of RMF and the implementation of NIS 2 took place.

At the beginning of the section, **Dmytro Lande**, Professor, Doctor of Technical Sciences, Head of the Department of Information Security, Igor Sikorsky Kyiv Polytechnic Institute, spoke about the prospects for the application of the latest AI algorithms to improve cybersecurity and parliamentary control, emphasizing that the main element of any system remains a person, and all electronic systems and algorithms are auxiliary tools.

Stress testing issues were also considered, in particular, in his report **Vitaly Zubok** noted that this is no longer a purely academic topic, it is becoming an obligatory element of digital infrastructure, for example, in the financial sector and energy, stress tests have long become a practice. And after legislative changes and the implementation of NIS 2, cyber resilience, digital resilience and functional resilience in all areas of digital infrastructure have become necessary.

The full-scale invasion of the Russian Federation has strengthened the transition to the principles of Zero Trust, increased regulatory monitoring, including the deployment of new solutions. In particular, our allies and partners have helped Ukraine build a modern system of threat analytics and cyber defense, stated **Oleg Gaiduk**.

To strengthen the digital resilience of the OKI, **Valery Tsyupa** proposed interactive trainings and Tabletop exercises for management teams, practical cases of such training were considered.

There was a discussion of the problematic issues of the transition from KSZI to RMF (American standard of cybersecurity systems), the Director of the Department of State Control in the Field of Information Protection and Cybersecurity of the State Special Communications Administration **Igor Stelnyk** spoke about the new ecosystem of information protection and ways to solve the problems of imperfection of legislation, he noted that the State Special Communications Administration is trying to solve this at the level of regulatory legal acts, which should be prepared together with interested business entities and NGOs.

Oleg Shemetov (MOU), shared the experience of implementing international cybersecurity standards, in particular, he contrasted that the Ministry of Defense was the first of the state bodies to confirm the conformity of systems built on the basis of security profiles, developed and approved the Cybersecurity Strategy and is already training its own evaluators.

Independent cybersecurity expert **Konstantin Korsun**, in order to increase efficiency and professionalism, proposed to take away all cybersecurity functions from 11 government entities and give them to one separate cybersecurity body and build real communications between it and society, which is categorically lacking in state bodies. The existence of a separate cybersecurity body will promote the cybersecurity market, he noted, and it will also save the general budget.

Conclusion: transparency in relations and close interaction between government, business and society have a positive impact on Ukraine's digital cyber resilience and defense capability.

Section 2. **DEOCCUPPATION THE INTERNET AND REDUCING RUSSIA'S INFLUENCE IN DIGITAL SPACE**

Moderator: Olena Kushnir, Ukrainian Internet Association

Focus: regaining control over networks, digital resources, and infrastructure in the deoccupied territories.

Key theses of the speeches

1. Yuriy Matsyk
   - Ukraine is forming a comprehensive model of digital deoccupation.
   - International organizations (ICANN, ITU, GAC) play a critical role in the return of digital resources.
   - Coordination of the state, the regulator, and the technical community is needed.
2. Tetyana Dolinska
   - The Russian Federation is systematically changing routing, domains, and network infrastructure.
   - Documentation of such actions is the basis for international courts.
   - The most valuable evidence: route snapshots, domain changes, data from occupied networks.
3. Viktoriya Opanasyuk
   - Restoring the Internet in Kherson is a complex practical process with security risks.
   - The Russian Federation tried to redirect traffic through its operators.
   - Operational control over local infrastructure is a key factor in success.
4. Svitlana Tkachenko
   - The .UA domain remains stable despite the war.
   - .UA is part of digital identity and national security.
   - Domain administration requires additional protection mechanisms.

Main conclusions of the discussion

1. Theft of IP addresses and ASNs is a violation of digital sovereignty.
2. An international mechanism for the return of digital resources is necessary, but does not yet exist.
3. A digital occupation registry should be created that would record changes in routes, domains, and IP blocks.
4. RIPE, ICANN, and technical communities should play a more active role in countering the digital expansion of the Russian Federation.

Final message

Deoccupation of the Internet is a strategic component of the state's defense. It requires:

- technical solutions;
- legal mechanisms;
- active diplomacy;
- participation of international partners.

The section confirmed: the digital front is one of the key ones in the war for Ukraine's sovereignty..

Section 3. **THE ROLE OF WOMEN IN THE SPHERE OF ELECTRONIC COMMUNICATIONS**

Moderator: Olena Kushnir, Ukrainian Internet Association

Focus: Women's Leadership in Telecom, Cybersecurity, Digital Diplomacy, and Internet Governance.

Keynote Speeches

1. Natalia Tkachuk (NSDC, Top Cybersecurity Woman of the World 2025)
   - Women have become key participants in cyber defense during wartime.

- State initiatives support professional growth and involvement of women in the cyber sector.
- Women's leadership shapes the sustainability of state cyber processes.

2. Tatyana Popova (Telecommunications Chamber of Ukraine)
   - The public sector plays a systemic role in telecom reforms.
   - Public expert institutions are an important platform for involving young women.
   - Civic activity creates space for influencing the policy of electronic communications development.
3. Vanda Scartezini (Brazil, DNS Women)
   - DNS Women is a global network of support for women in technical fields.
   - The creation of international women's communities strengthens the role of women in the technical management of the Internet.
   - Ukraine has great potential to involve its specialists in the global processes of ICANN, IETF and IGF.
4. Olena Lutsenko (RETN)
   - Women manage international telecom projects even during war.
   - Leadership in crisis situations requires flexibility and strategic thinking.
   - The combination of global experience and Ukrainian realities creates unique management models.
5. Liljana Pecova-Ilieska (North Macedonia, IMPETUS)
   - The Western Balkans demonstrate effective practices in involving women in cybersecurity.
   - Key steps: institutional support, educational programs, joint regional initiatives.
   - There is potential for the launch of Ukrainian-Balkan programs from 2025.
6. Anastasia Bryhynets (DUICT)
   - The formation of a new generation of female cyber defenders begins with education, mentoring, and practice.
   - Young professionals are already participating in real cyber projects.
   - Female students are increasingly interested in technical specialties, even during wartime.
7. Svitlana Tkachenko (Hostmaster)
   - Women play an important role in domain management and digital diplomacy.
   - The .UA domain is not only infrastructure, but also an element of Ukraine's international presence.
   - Women's leadership helps promote Ukrainian standards in global Internet organizations.

Panel discussion conclusions

1. The greatest strength of female leadership in war is resilience, empathy, and strategy.
2. A female leadership style in telecom and cybersecurity exists and is manifested in the ability to balance risks, make decisions under pressure, and create long-term solutions.
3. To attract young women to technical fields, we need:
   - scholarship programs;
   - mentoring networks;
   - participation in international technical communities (ICANN, RIPE, IGF);
   - role models who show real success stories.

Final message

The section demonstrated that women are an indispensable part of Ukraine's digital resilience. They maintain the cyber front, manage the telecom infrastructure, promote Ukraine in international processes, and shape the future of electronic communications.

Section 4. **INTERNET ACCESS RESILIENCE DURING WAR (BLOCKING, INTERNET SHUTDOWNS)**

Moderators: Yuriy Matsyk, GAC ICANN, **Oleksiy Semenyaka**, RIPE NCC

The discussion revealed a fresh perspective on the issue of network accessibility. The session opened with a review of the need to revise the global taxonomy of Internet shutdowns (report by O. Semenyaka). The existing definitions no longer correspond to the realities of the modern world: we need a classification that takes into account not only technical failures or political censorship, but also the consequences of natural disasters and, critically important for us, hostile actions by other states (including in cyberspace) and the conduct of warfare.

This theoretical basis was supported by unique facts. Y. Matsyk (Ministry of Digital Transformation) provided data demonstrating the scale of challenges at the national level, while operators from the Kherson region shared invaluable practical experience. Their stories about organizing uninterrupted work, new regulations, and engineering solutions in conditions of occupation and shelling are examples of exceptional adaptability and professional heroism.

We came to a common conclusion: the collected array of information is unique Ukrainian know-how. These are not just situational solutions for survival, but a valuable intellectual asset. This experience must be systematized and preserved, as it can become the foundation for building resilient networks around the world in the face of future crises.

Today, communication is not about entertainment or business; it is a basic human need, on par with safety and food. The ability to obtain information, contact relatives, or call for help saves lives. Therefore, it is our duty to develop these achievements, transforming our traumatic experience into global expertise in resilience.

Section 5. **COMPARISON OF THE COUNCIL OF EUROPE AND THE UN APPROACHES TO COMBATING CYBERCRIME**

Moderator: Oksana Prykhodko, iNGO European Media Platform.

Speakers: Giorgi Jokhadze, Project manager of the Council of Europe Cybercrime Programme Office, Oleksiy Tkachenko, Representative of the National Security and Defense Council of Ukraine at the EU Cybersecurity Agency ENISA

Ukraine ratified Budapest (the Council of Europe) Convention on Cybercrime in 2005, and has long and very fruitful cooperation with the CoE. This cooperation is very important in time of war, and is in line with Euro-integration process of Ukraine. The Budapest Convention creates clear mechanisms for trusted international cooperation in fight against cybercrime with respect to human rights, transparency and rule of law.

Ukraine did not participate in the process of developing of the UN Convention against cybercrime, adopted by the UN in 2024 (with strong support from Russia, Iran, North Korea and other non-democratic countries).

UN Convention creates cybercrime-evidence framework parallel to the Budapest Convention and, while complementing it in many aspects positively, brings risks of lesser safeguards in the fight against cybercrime and fragmentation, potentially having effect on freedom of threatens having effect on freedom of speech and other human rights.

Section 6. **ACTUAL ISSUES OF DNS**

Moderator: Oksana Prykhodko, iNGO European Media Platform

Speakers: Svitlana Tkachenko, Hostmaster, Ivan Petuhov, ULIE, Oleksandr Olshanskuy, Internet Invest LLC, Oleg Chernobay, Chernobay&Partners, Oleksiy Semenyaka, RIPE NCC, Tetyana Dolinska, SUNIC, Yuriy Matsyk, Ministry of Digital Transformation of Ukraine, GAC ICANN.

The participants of the discussion noted the exceptional stability of the administration of the .ua domain (both at the technical and administrative level and at the level of international cooperation). At the same time, there are already certain problematic issues related to top-level domains in Ukraine, and the next round of new gTLDs brings more challenges than opportunities.

These (already existing) problems are related, in particular, to the Cabinet of Ministers' Resolution No. 851/2015 "Some Issues of the Use of Domain Names by State Bodies in the Ukrainian Segment of the Internet", which requires "officials to use exclusively electronic mailboxes hosted on servers located in the GOV.UA or .UKR domain zone for official correspondence."

Correspondence through email accounts located on Cyrillic domains still remains a problematic issue, and most representatives of government agencies do not even suspect the existence of Cyrillic domains with the names of their agencies.

In addition, the wording “in the Ukrainian segment of the Internet” contradicts the principles of “One World – One Internet” and transparently hints at the Russian-Chinese principles of Internet governance.

To solve this problem, it was proposed to contact the Cabinet of Ministers with a request to cancel this resolution.

It was also proposed to contact the Cabinet of Ministers with a request to instruct the Ministry of Foreign Affairs to deal with the inclusion of .su in ISO standards. This domain - .su was removed from the ISO 3166-1 list (a list created exclusively for country codes) in 1992, after the collapse of the Soviet Union. Nevertheless, this domain continues to exist now (in the ISO 3166 list, as “exclusively reserved”). Nevertheless, this domain continues to exist (in the ISO 3166 list, as “exclusively reserved”), and russia tries to do its best to return this domain to the ISO 3166-1 list (by analogy with .eu and .uk).

Of particular concern is the absolute lack of transparency in the administration of .укр (the inability to send information requests or cybersecurity inquiries to the official addresses listed on the IANA website). These and other issues have prompted Ukrainian stakeholders to initiate informal communication with ICANN regarding the status of this domain..

Section 7. IGF MANDATE AND FUTURE OF INTERNET GOVERNANCE

Moderators: Oksana Prykhodko, iNGO European Media Platform, **Tetyana Dolinska**, SUNIC

Speakers: Anja Gengo, IGF Secretariat, Dimitris Zacharius, ICANN, Oleksiy Semenyaka, RIPE NCC, Amrita Choudhuri, IGF Supporting Association, Olivier MJ Crepin-Leblond, EuroDIG, Ivan Petuhov, YLIE.

Despite all the skepticism (at least from Ukrainian stakeholders) regarding the UN's ability to make adequate decisions, the participants in the discussion were mostly positive: the IGF's mandate (according to the results of the vote during the UN General Assembly on December 17) will be extended, although perhaps in a slightly different format. And not forever, but perhaps for another 10 years.

But even in the absence of such a mandate, all participants emphasized the importance of the existence of such an open multi-stakeholder platform that allows for discussions (or at least to initiate such discussions) at the national, regional, and global levels.

The issue of supporting Youth IGF-ua and IGF-UA was discussed separately. This year, the sponsors of the Ukrainian IGFs (because IGF-UA has a joint budget with Youth IGF-UA) were RIPE NCC and ICANN. Also, thanks to the many years of support of the Ukrainian forums from IGF SA, there is still something left for this year.

At the same time, some Ukrainian stakeholders were more pessimistic, but the joking "Let's live until next fall" is more of a challenge than a doubt. After all, it is then, at the traditional time of Youth IGF-UA and IGF-UA, that we will be able to unite again, discuss new ideas, and show that our community is a force that drives progressive change forward!

YOUTH IGF-UA

The VIII Youth IGF-UA was opened by Valeria Dubitska (European Media Platform). Welcome remarks from the co-organizers and sponsors of Youth IGF-UA (Ivana Petukhova, USPP, Oleksiy Semenyaka, RIPE NCC, Olena Kushnir, InAU, Oksana Prykhodko, European Media Platform) concluded with an "Introduction to Internet Governance" by Gabriela Shchytek (ICANN).

The first section - "Disinformation and Information Warfare" - was prepared and moderated by Dmytro Kushnir. It was dedicated to the current challenges of disinformation, information warfare and the role of artificial intelligence (AI) in modern information threats for Ukraine and Europe.

The section brought together international experts, investigative journalists and representatives of Ukrainian state institutions to exchange experience, practical cases and analytical approaches to countering disinformation and FIMI (Foreign Information Manipulation and Interference). The speakers of the section (Anayit Khoperiya from the Ukrainian Center for Countering Disinformation, Benjamin Delhomme from NATO StratCom COE and Max Bernhard from CORRECTIV.Faktencheck) discussed current trends in disinformation and information warfare, the experience of the Center in countering disinformation and state information threats, the role of AI in modern information operations and challenges for democratic societies, considered a practical case of investigating fake news magazines and mechanisms for creating disinformation. The section aroused considerable interest among the participants of the Youth IGF-UA and received positive feedback for the practical focus and high level of expertise of the speakers. The combination of Ukrainian experience, international analytics of NATO StratCom COE and journalistic investigations of CORRECTIV was especially valuable for the audience. The discussion confirmed the need for further deepening cooperation between Ukrainian and European experts, as well as the importance of focusing on threats associated with the development of AI in the field of disinformation.

The section dedicated to cybersecurity issues was moderated by Eliza Rogotska (Axon Partners). Andriy Mankish dedicated his speech to "Possibilities of using AI in cyberwarfare" and analyzed the use of artificial intelligence in offensive and defensive cyber operations, as well as an overview of the most common cases of using AI in cyberwarfare and the impact of AI on the pace and scale of cyberattacks, Mykola Titov made a report on the topic: "Time under control: the strategic role of NTP servers in critical infrastructure and cybersecurity" (the role of accurate time in the work of energy, telecommunications, government services; explanation of the principles of NTP operation and Q&A on the threats of time manipulation and their potential consequences), and Denys Poslavsky (CERT-UA) introduced the participants of the event to the basics of cyber hygiene and responding to cyber incidents and provided practical recommendations for citizens and organizations on the first steps in the event of a cyberattack and analyzed the human factor in cybersecurity. During the discussions, it was emphasized that effective cyber resilience of Ukraine is formed not only through the implementation of technological solutions, but also through the development of human potential, the establishment of interaction between the public sector, business and civil society, as well as the active involvement of youth. Special attention was paid to the need to strengthen educational programs, increase the level of digital awareness and systematically present Ukrainian experience in international processes and discussions in the field of Internet Governance and cybersecurity.

Eliza Rogotska and Solomiya Yaremenko (Human Rights Platform) presented the BCOP RIPE Task Force study: "Documented Experience in Maintaining the Resilience of Ukrainian Networks during War (Based on NOGUA and RIPE NCC). The BCOP (Best Current Operational Practices) Task Force was formed at RIPE 67 in October 2013 to initiate and coordinate the process of documenting important common operator practices in the field of Internet networks. Since the beginning of the full-scale invasion, RIPE has been carefully studying the unique experience of Ukrainian operators and, based on NOGUA, already has good developments that form the basis of documented recommendations for network resilience for the entire global community. The section "International Opportunities for Ukrainian Youth" was moderated by Solomiya Yaremenko. Nadia Tjahja (YouthDIG), Laura Lorenzo (RIPE NCC Fellowship), Anja Gengo (IGF Secretariat, Youth IGF) and Olena Kushnir (EuroSSIG) presented international youth programs in the field of

Internet Governance, educational and fellowship opportunities for students and youth and discussed the problematic issues of involving Ukrainian youth in the international community of participants in educational programs and training opportunities. Ukrainian students do not always participate in international training opportunities, so this section became a kind of "guide to opportunities" for Ukrainian youth. This approach was useful and practical, as participants not only learned about specific opportunities, but also were able to understand how to successfully apply for training programs. The VIII Youth IGF-UA ended with an invitation to begin work on the preparation and holding of the next, IX, Youth IGF-UA.

You can see the videos of IGF-UA-2025 at: https://2025.igf-ua.org/stream

CONTACTS

IGF-UA Organizing Committee

www.igf-ua.org, info@igf-ua.org

tel/fax: +38 044 278-2925

15/3 Olesia Honchara street, office 22, Kyiv, 04053