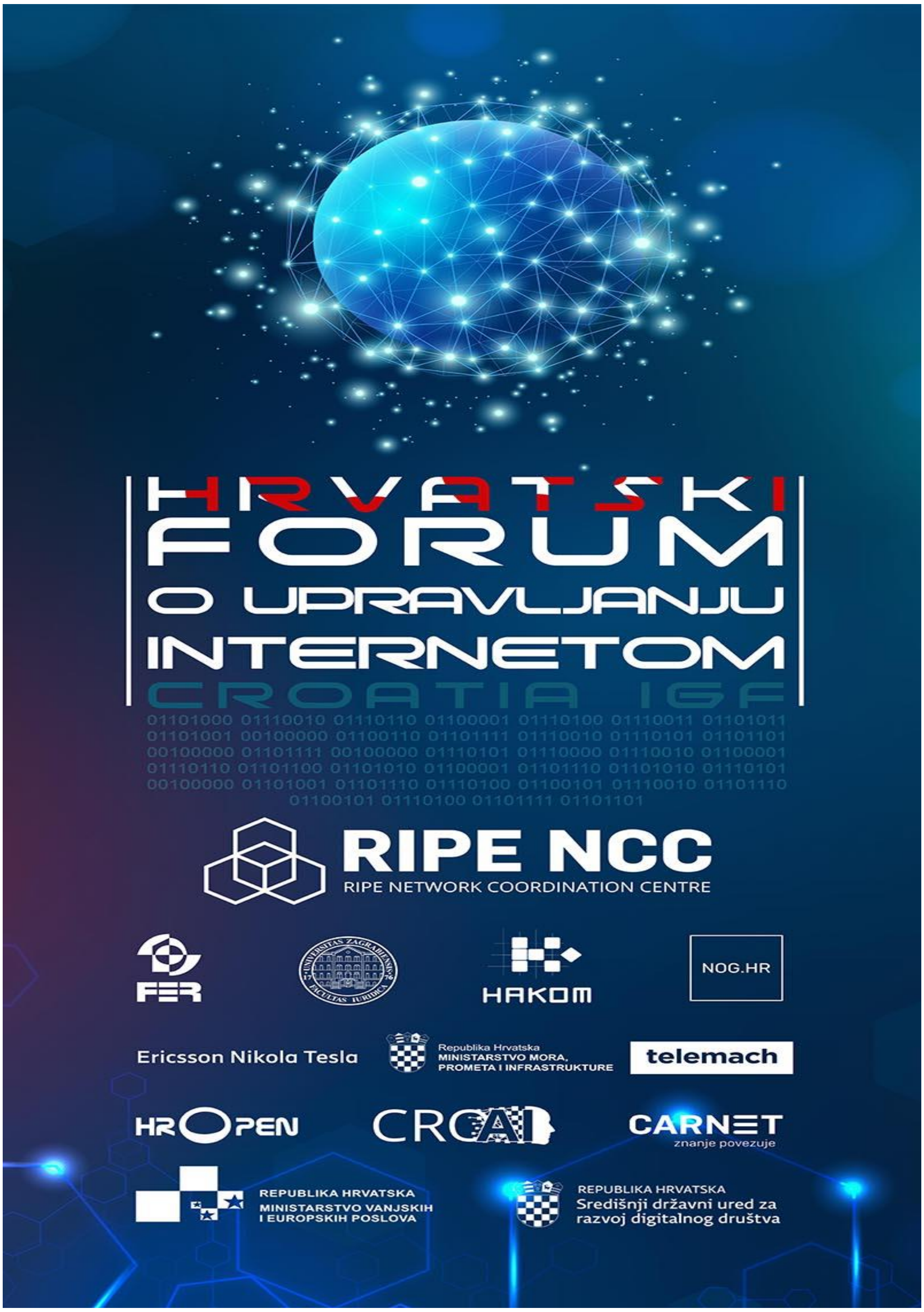
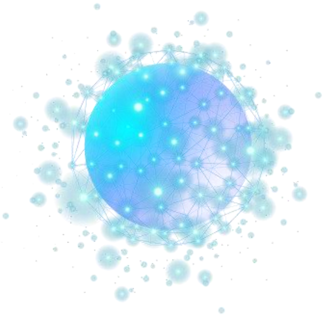
Croatian Internet Governance Forum CRO-IGF 2024 – Final Report





What is Internet Governance Forum?

The Internet Governance Forum (IGF) is a global initiative operating under the auspices of the UN, with the primary goal of fostering inclusive and equal participation of all stakeholders in discussions related to Internet governance. Established in 2006 during the "World Summit on the Information Society" (WSIS) in Tunisia, the IGF was envisioned as an open platform for addressing Internet governance issues.

This decision was prompted by the recognition of the necessity to involve a broader community in the governance and regulation of the Internet. As a result, a diverse range of topics emerged, spanning from IP addresses and Internet protocols to domain management. In this context, it is crucial for multiple stakeholders, including civil society, academia, industry, and the private sector, to actively engage in these discussions alongside state representatives. This collaborative approach allows for well-rounded perspectives and ensures that a wide array of interests and expertise are considered in shaping Internet governance policies.

The IGF does not have a decision-making mandate, nor does it adopt binding acts, but their results may affect other processes, which have binding effects. The IGF, by drawing its conclusions and drawing attention to topics that are relevant, can influence decision makers and thus participate in forming an official national position or public policy in the field of internet governance.

The IGF is fully open to the participation of anyone interested in the issues of Internet stability, its security, usage and development. IGF is an annual event. Topics that will be discussed on the IGF can be suggested by anyone interested.

In addition to the global IGF initiative, there are regional (e.g. EuroDIG - European Dialogue on Internet Governance, SEEDIG - South East European Dialogue on Internet Governance), national (e.g. CRO-IGF), or age (Youth IGF) initiatives.

IGF initiatives, especially national and regional ones, are important as they promote communication among all stakeholders, foster the development of a culture of dialogue among different stakeholders on internet-related issues, which helps in anticipating different perspective and interests. Important principles on which the IGF is based are:

- openness and transparency (allowing all interested parties to participate in the IGF, public insight into all parts of the IGF's work)
- inclusivity (enable active involvement of all concerned)
- bottom-up approach (involving the public in the creation of the IGF program)
- is not intended for sale of goods and services
- multi-stakeholder model (model of involvement of all stakeholders: academia, business sector and industry, civil society organizations and state and public administration)

Why CRO-IGF?

The National IGF has been running for several years now as a platform for open and inclusive multi-stakeholder discussions on Internet governance issues in Croatia. The first CRO-IGF was held in Zagreb on 6 May 2015 at the Faculty of Electrical Engineering and Computing, University of Zagreb. One of the topics discussed was about the benefits that CRO-IGF as a platform could bring to Croatia. Reports from the very first as well as subsequent CRO-IGFs have been uploaded to the global IGF website: https://www.intgovforum.org/en/content/eastern-european-regional-group.

The goals of CRO-IGF are:

- to point out to various stakeholders the opportunities for involvement in Internet governance processes relevant to their business and activities, and to encourage dialogue and, if necessary, help in capacity building for better understanding of Internet-related topics;
- to empower all stakeholders in Croatia to actively participate in national, and then directly or indirectly, regional and international Internet governance processes;
- to identify Internet governance topics that are important for Croatia.

CRO-IGF 2024 Preparatory Process

This year, the Organizing Committee decided to involve public in the selection of topics. The public had the opportunity to choose 2 of the proposed 4 topics. So, they chose: Cyber Security and Artificial Intelligence.

The Organizing Committee prepared program consisting of two panel discussions:

1. Cyber security - the NIS2 Directive
2. Artificial Intelligence

CRO-IGF 2024 Organizational Committee

Academic Community: Tihomir Katulić, Faculty of Law, University of Zagreb Marin Vuković, Faculty of Electrical Engineering and Computing, University of Zagreb	Private sector/Industry: Adrian Ježina, Telemach Hrvatska Hrvoje Hadžić, Ericsson Nikola Tesla Martina Silov, CroAI Branimir Rajtar, NOG.hr
Public Sector: Krešo Antonović, Ministry of the Sea, Transport and Infrastructure Tihomir Lulić, Ministry of Foreign and European Affairs Marin Ante Pivčević, SDU-RDD[1] Nataša Glavor, Ivana Jelačić, CARNET Mislav Hebel, HAKOM, GAC Representative Zdravko Jukić, HAKOM, GAC Representative (Advisor)	Internet Users/Civil Society: Kristijan Zimmer, Croatian Open Systems Users' Group, HrOpen

More detailed information on organizations with representatives on the CRO-IGF Organizing Committee:

Ministry of Foreign and European Affairs	https://mvep.gov.hr/en
Ministry of the Sea, Transport and Infrastructure	https://mmpi.gov.hr/en
Central State Office for the Digital Society Development (SDU-RDD)[2]	https://rdd.gov.hr/o-sredisnjem-drzavnom-uredu/9?lang=en
Croatian Academic and Research Network - CARNET	https://www.carnet.hr/en/
Faculty of Law, University of Zagreb	https://www.pravo.unizg.hr
Faculty of Electrical Engineering and Computing, University of Zagreb	https://www.fer.unizg.hr
Ericsson Nikola Tesla	https://www.ericsson.hr/en/homepage
Croatian Open Systems Users' Group, HrOpen	http://www.open.hr/
CroAI, the Croatian Artificial Intelligence Association	https://www.croai.org/
Network operators group Croatia (NOG.hr)	https://nog.hr/en/about/about/
Croatian Regulatory Authority for Network Industries (HAKOM)	https://www.hakom.hr/en/home/8

CRO-IGF web site is available at http://www.carnet.hr/carnet_events/cro_igf
LinkedIn profile: https://www.linkedin.com/company/croatian-internet-governance-forum/

CRO-IGF community contact could be reached using email address cro-igf@carnet.hr

[1] as of 17.05.2024. part of Ministry of justice, public administration and digital transformation

[2] as of 17.05.2024. part of Ministry of justice, public administration and digital transformation

CRO-IGF 2024 Event

The seventh Croatian IGF was held in Opatija on 22 May 2024 at Grand Hotel Adriatic as an independent event at the MIPRO 2024 Conference. This event had the following agenda:

15:30 – 16:00 Welcome drink and networking
16:00 – 16:05 Short introduction – Ivana Jelačić, CRO-IGF 2024 Coordinator
16:05 – 16:15 Welcoming speech – mr. sc. Mislav Hebel, Deputy President of the HAKOM's Council
16:15 – 17:30 Theme 1: Cyber security - The NIS2 Directive
17:30 – 17:45 Coffee break
17:45 – 19:00 Theme 2: Artificial Intelligence
19:00 – 19:10 Conclusion and messages

Ivana Jelačić, the Coordinator of this year's CRO-IGF gave a short introduction on what CRO IGF is, why it is important and how it fits into wider perspective of the Internet Governance. She also presented the agenda for this year's Forum.

Ivana Jelačić, CRO-IGF 2024 Coordinator giving introductory statement.

mr. sc. Mislav Hebel, Deputy President of the Council of the Croatian Regulatory Authority for Network Industries (HAKOM), greeted the attendees and wished everyone a successful event.

Mislav Hebel, Deputy President of the HAKOM's Council holds the opening statement.

Cyber security - The NIS2 Directive

The NIS2 Directive brings significant changes in the field of cyber security for companies in the EU. Croatia transposed this directive into national Cybersecurity Act, which entered into force on 15 February 2024.

Panel Participants:
Panelists:

- Martina Dragičević (A1 Hrvatska, Croatian employers' association)
- Nataša Glavor (CARNET/ National CERT)
- Jagoda Peleponjko (Croatian Regulatory Authority for Network Industries - HAKOM)
- Nikola Markovinović (Gama Global)
- Goran Brdar (Atos Convergence Creators)

Moderator: Associate Professor Tihomir Katulić, Ph.D., Faculty of Law, University of Zagreb

At the panel related to cyber security and NIS2 directive, the following questions were raised:

- whether additional investments in infrastructure and personnel will be required in organizations subject to the Cybersecurity Act,
- how we as a country will deal with the need to develop specialized skills and capacities in the field of cyber security,
- what are the opportunities that the NIS2 directive can bring to the cyber security sector and how we can improve national cooperation involving all parts of society, especially the private sector and competent authorities.

Panel: Cybersecurity - The NIS2 Directive

Messages from the panel discussion:

- It is a privilege to live in a time when the cyber security framework is being regulated and to be able to contribute as members of society.
- The NIS 2 Directive is a good opportunity to raise awareness of the importance of cyber security in everyday life.
- The new Cybersecurity Act, which transposed the NIS2 Directive, will improve the protection of data and information systems.

- A great opportunity to prepare for business protection, the possibility of working in the field of cyber security outside the borders of the home country.
- It is important that entrepreneurs are involved in the process of adopting acts - public bodies want to listen to the proposals and practices of entrepreneurs. Private sector's view on the policies is also needed.
- There are no significant changes for large telecom operators.
- The big challenges are expected for small entrepreneurs. It is necessary to find mechanisms to help entrepreneurs in determining the set of measures they must implement. That set should be rational and proportional to the scope of business.
- The supply chain - many new business entities will learn to cover the application, some directly, some indirectly.
- It is crucial to have the understanding and support of management, as well as financial and human resources.
- The new regulations put the responsibility of management in the foreground. The damage occurs to the subject, so management is motivated to invest in cyber resilience.
- Cost of implementation - figure out how to help entrepreneurs skip the gap as soon as possible. Provide grants through funding from European and national programs.
- The National Coordination Center for industry, technology and research in the field of cyber security was established (https://www.nks.hr/en/), which will allocate national funds from European funds intended for cyber security.
- It is important that all sectors are maximally educated and informed about cyber security.
- Three things are important: education, governance and technical measures.
- Employee education - employees must be informed about cyber security. It is necessary to design a good program and to include different communication channels (posters, emails, messages).
- People are essential in cyber security; it is human who is the basic link in cyber security.
- Education should be interesting.
- Employees are obliged to comply with the measures. We are all responsible in the workplace.
- Education is important, but so is punishment. We cannot educate forever; we must have the sanction to publicly set the boundaries of education.
- Must work on creating a pool of information security experts. The need for experts will increase their number.
- Conduct a cyber security competition at the high school and academic level, then monitor the contestants, and guide and raise motivation for continuing education for jobs related to cyber security.
- Include entrepreneurs who are interested in participating in training in the field of cyber security.
- Consider including services that will replace people. The lack of specialists can be solved by purchasing certain services.
- IGF is still one of good examples on how to involve and include all interested parties in discussions of common interest.

Artificial Intelligence

Artificial Intelligence - The Artificial Intelligence Act, the first comprehensive legal framework for AI in the world, which provides clear requirements and obligations regarding its application.

Panel Participants

Panelists:

- Juraj Bilić, Deputy CEO for the Artificial Intelligence Sector in CARNET/ Project manager for CARNET's project "Support for the application of digital technologies in education - BrAIn"
- Marija Bošković Batarelo, founder and director of Parser compliance d.o.o.
- Ivan Ćaleta, Center for a safer Internet
- Associate Professor, Hrvoje Lisičar, Ph.D., Faculty of Law, University of Zagreb
- Professor Romana Matanovac Vučković, Ph. D., Faculty of Law, University of Zagreb

Moderator: Ana Smoljo, CARNET's Communications Office and member of the CroAI Board of Directors

Topics discussed in the panel:

- Act on artificial intelligence and its adaptation to future needs
- the high-risk systems
- the influence of AI on intellectual property and copyright
- protect privacy and data.
- new challenges in the field of cyber security.

Panel: Artificial Intelligence

Messages from the panel discussion:

- The AI Act is technologically neutral. Applies only to the EU area.
- It represents a framework, for which it remains to be seen how useful it will be in practice.
- There are many exceptions from the Act.
- It is directly applied, but we need a lot of implementing acts.
- The EU is not doing itself any good in the economic sense, because we will allow others to develop economically faster. It is necessary to put wisely everything into practice. Education systems will automatically be at high risk.
- The right to privacy of EU citizens is mandated.
- Forbidden form of emotional recognition and thinking.

- Technology is galloping. It is crucial to involve the scientific community, scientists have a lot of knowledge and need to show how much they know so that industry knows about it and uses it.
- AI is targeting systems that are high risk, but video games are not regulated and the users are mostly children.
- We need to teach children how to think critically and how to consume content that is offered in a productive way.
- The key is education from the earliest age. Parents and experts who educate children should also be educated. People's motivation is important. It is essential to educate adults on how to teach children about AI.
- Protection of copyright and intellectual property rights – AI only "reads" original content and then no longer uses it. Current copyright framework is not satisfactory. Interest of the content producers needs to be considered.
- The future – among other things it is also necessary to ensure national sovereignty by having enough processing power e.g. graphics cards (GPU) to keep all the data of the state within the country. As AI algorithms are performed on graphics cards (GPU), the one that manufactures graphics cards at the same time potentially controls how much AI will be adopted or used in specific countries.
- Small and large language models on laptops and mobile phones will be able to function offline and everyone will have their own assistant.
- Technology is neither positive nor negative. What matters is what people are like and what they want to use it for!

Audience

The Forum was attended by round 40 participants. The presence of participants from different stakeholders was evenly distributed among Government and the public sector, private sector, academia and civil society representatives.

Conclusions

The main conclusions of the Forum are the messages generated in its open and inclusive format. The participants recognized that this format is excellent for exchanging ideas and positions that may influence relevant policy processes at the national and international levels. It is necessary to continue to further develop a dialogue on issues related to the Internet and in particular Internet governance among all the interested stakeholders.

Special Thanks

CRO-IGF's annual event was made possible by the positive attitude and efforts of all the members of the CRO-IGF Organizing Committee. Special thanks to the MIPRO Conference that hosted this year's forum. Support and sponsorship from the RIPE NCC Organization was very valuable and very important in organizing CRO-IGF 2024 event. Thanks everyone!

More Information and Contact

It is possible to contact the Croatian multi-stakeholder community for Internet governance issues by email: cro-igf@carnet.hr

Zagreb, 3 July 2024