MEETING REPORT

RIGF: RUSSIAN INTERNET GOVERNANCE FORUM

2021

TABLE OF CONTENTS

ABOUT RIGF

The 11th Russian Internet Governance Forum (IGF 2021) was held on April 7-9, 2021

Russian Internet Governance Forum is an event where all professional views can be brought to attention and discussed. The aim is to find a consensus between government agencies, telecommunications industry, businesses and society, leading to successful results in Russia and worldwide. With many ideas expressed during previous events turning into hands- on projects for Russian and international organizations, this year's Forum became a starting point for many collaborations for all RIGF attendees.

The 11th Russian Internet Governance Forum (RIGF 2021) took place in the Expocentre Central Exhibition Complex. It was held in a hybrid format: moderators, speakers, journalists and participants in the awards ceremony were invited offline.

This year, everyone who wanted to express their opinion on internet development took part in compiling a program for the forum. As a result, the Forum has acquired an extensive program consisting of seven sessions and a Youth Track.

Over three days speakers and other RIGF 2021 participants were discussing Information Security, Trust in the Internet, the Regulation of Social Networks, Data Sovereignty, the Use of Artificial Intelligence and many other important issues linked with Internet Development, the formation of the ecosystem of the Internet Governance and International Cooperation.

PARTNERS

ICANN's mission is to help ensure a stable, secure, and unified global Internet. To reach another person on the Internet, you have to type an address – a name or a number – into your computer or other device. That address must be unique, so computers know where to find each other. ICANN helps coordinate and support these unique identifiers across the world. ICANN was formed in 1998 as a not-for-profit public-benefit corporation and a community with participants from all over the world.

Kaspersky is a global cybersecurity company founded in 1997. Kaspersky's deep threat intelligence and security expertise is constantly transforming into innovative security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe.

The Technical Center of Internet is an accredited Russian IT-company, which main spheres of expertise are domain name industry, cybersecurity, data processing and software development. TCI serves as a technical back-end for the Russian national domain zone, it provides technical support for the registries and domain registration system of the ccTLDs .RU, .РФ, .SU and New gTLDs .ДЕТИ and .TATAR and ensures continuous operation of the domain addressing of the Russian Internet segment.

AGENDA

April 7

10:00 – 12:00
High-level plenary

Participants:

- **Maxut Shadayev**, Minister of Digital Development, Communications and Mass Media of the Russian Federation
- **Alexander Khinstein**, State Duma Committee on Informational Policy, Technologies and Communications, Chairman
- **Tatyana Matveeva**, Head of the Department for the Development of Information and Communication Technologies and Communication Infrastructure, Presidential Executive Office
- **Doreen Bogdan-Martin**, Director of the Telecommunication Development Bureau of the International Telecommunication Union
- Rashid Ismailov, VimpelCom PJSC
- **Anriette Esterhuysen**, IGF Multistakeholder Advisory Group Chair
- **Andrey Vorobyev**, Director of the Coordination Center for TLD .RU/.РФ

IP&IT Law Award Ceremony

12:10 – 13:40
Session 1. Internet Governance

Moderators: **Jovan Kurbalija**, DiploFoundation, **Andrey Vorobyev**, Coordination Center for TLD .RU/.РФ

Participants:

- **Mandy Carver,** ICANN
- **Rashid Ismailov**, VimpelCom PJSC
- **Wolfgang Kleinwächter**, University of Aarhus (Denmark)
- **Tatyana Matveeva**, Presidential Executive Office
- **Maxim Parshin**, Deputy Minister of Digital Development, Communications and Mass Media of the Russian Federation
- **Sergey Plugotarenko**, RAEC

13:50 – 15:20
Session 2. Emerging technologies. Artificial Intelligence and Ethics

Moderators: **Karen Kazaryan**, RAEC, **Anna Abramova**, MGIMO

Participants:

- **Maxim Fedorov**, Skolkovo Institute of Science and Technology
- **Elsa Ganeeva**, Microsoft
- **Andrey Ignatyev**, Center for Global IT Cooperation, MGIMO University
- **Jan Kleijssen**, Council of Europe
- **Andrey Kuleshov**, MIPT
- **Andrey Neznamov**, Sberbank
- **Alexander Tyulkanov**, Skolkovo Foundation

AGENDA

April 8

10:00 – 11:30
Session 3. Regulation: Data Sovereignty

Moderator: Mikhail Yakushev, Higher School of Economics

Participants:

- **Bertrand de la Chapelle**, Internet & Jurisdiction Policy Network (France)
- **Nikolay Dmitrik**, Moscow State University
- **Aleksandra Orekhovich**, The Internet Initiatives Development Fund
- **Thomas Schneider**, OFCOM
- **Milos Vagner,** Roskomnadzor
- **Natalia Velikorodnyaya**, MTS

11:40 – 12:20
Virtuti Interneti award presentation and the awardee's keynote address

12:30 – 14:00
Session 4. Digital Platforms: the rules of the game

Moderator: Vadim Vinogradov, HSE

Participants:

- **Lucien Castex**, AFNIC
- **Bella Cherkesova**, Deputy Minister of Digital Development, Communications and Mass Media of the Russian Federation
- **Vladimir Gabrielyan**, Mail.Ru Group
- **Vadim Glushchenko**, Competence Center for Global IT Cooperation
- **Vladimir Tabak**, Dialogue

14:10 – 15:40
Session 5. Building a System of Trust in Supply Chains

Moderator: Nikolay Zubarev, Digital Economy

Participants:

- **Elena Bocherova**, Akronis-Infosecurity
- **Stanislav Fesenko,** Group-IB
- **Artyom Kungurtsev**, Moscow Department of Information Technology
- **Ghislain de Salins**, OECD
- **Oleg Sedov**, Rostelecom-Solar
- **Andrey Yarnykh**, Kaspersky Lab

AGENDA

April 9

10:00 – 11:30
Session 6. Attributing Cyberattacks on the Internet. Myths Busting

Moderator: Alexey Lukatsky, CISCO

Participants:

- Sergey Golovanov, Kaspersky Lab
- Alexander Kalinin, Group IB
- Liis Vihul, Cyber Law International (Estonia)
- Igor Zalevskiy, Rostelecom Solar

11:40 – 13:10
Session 7. User Agreements with Internet Platforms: Way to protect Russian Internet Users' Rights and the State's Interests

Moderator: Anna Dupan, Higher School of Economics

Participants:

- Elena Zayeva, FAS Russia
- Karen Kazaryan, RAEC
- Yury Kontemirov, Roskomnadzor
- Roman Krupenin, Yandex
- Dmitry Magonya, ART DE LEX
- Anna Starkova, «Rossiya Segodnya» media group

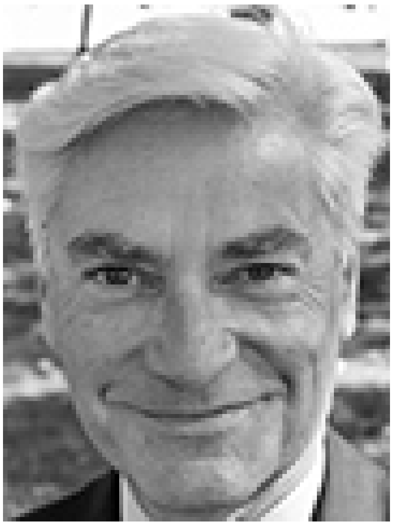
13:20 – 14:50
Session 8. Taking stock. Youth Session

- Ilona Stadnik, Coordination Center for TLD .RU/.РФ

Open mic

Closing of the Forum

KEYNOTE ADDRESS. VIRTUTI INTERNETI AWARD



The awards ceremony for Virtuti Interneti (for service to the internet industry), established by the Coordination Center for .RU/.РФ in 2010, was held on the second day of the Russian Internet Governance Forum (RIGF 2021). It is a unique prize awarded to representatives of the internet community, businesses, science and government who have made a significant contribution to Runet development and to the global network.

Candidates are shortlisted by the RIGF Program Committee. The awards ceremony, followed by the winner's lecture, is an RIGF tradition.

Virtuti Interneti was presented for the 11th time this year. Many RIGF participants were among its past winners, including this year's speakers, Dr Wolfgang Kleinwaechter, Professor Emeritus for Internet Policy and Regulation at the Department for Media and Information Studies of the University of Aarhus, Sergey Plugotarenko, Director of the Russian Association of Electronic Communications (RAEC), and Dr Jovan Kurbalija, Founding Director of DiploFoundation, Head of the Geneva Internet Platform (GIP) and Author of An Introduction to Internet Governance.

Virtuti Interneti 2021 was presented to Bertrand de La Chapelle, Executive Director and Co-founder of the Internet & Jurisdiction Policy Network. He has been a promoter and implementer of multi-stakeholder governance for 18 years, building on his diversified experience as a diplomat, a civil society activist and a tech entrepreneur. Bertrand de La Chapelle served on the ICANN Board in 2010-2013. Other previous roles include France's Thematic Ambassador and Special Envoy for the Information Society (2006-2010) and an active participant in the World Summit on the Information Society (2002-2005) where he promoted dialogue between civil society, the private sector and governments.

During the lecture, Bertrand de La Chapelle looked back on the evolution of Internet Governance over the past 20 years and offered seven main lessons that this evolution had taught us. He proposed using the concept of technical RFCs to develop legal documents of a similar nature. He believes it is extremely important that all Internet Governance parties manage to overcome mutual mistrust: "In our complex societies that are inter-connected by transnational online services, when cooperation is actually required to organize our common spaces, we need a new governance architecture to deal with transnational issues. Do not fear to trust. Nothing significant can be built in terms of architecture if the starting point is mistrust".

HIGH-LEVEL PLENARY

Russian Internet Governance Forum traditionally starts on April 7, the anniversary of Russia's country code domain .RU. RIGF2021 is no exception

Director of the Coordination Center for TLD .RU/.РФ Andrey Vorobyev congratulated the domain on its 27th anniversary and added that since the previous forum, approaches to Internet Governance have undergone significant changes: "The COVID-19 pandemic forced us to stop for a moment, think carefully and reconsider many aspects of it. As far as Internet Governance is concerned, for the past couple of years, we have no longer heard any talk about a Global Internet Village. We can see that the balance between the interested parties has been upset, cybersecurity issues exacerbated. There are some positive aspects though. The Internet infrastructure in Russia and in other countries passed the stress test. For three days, we're concentrating on trying to come up with expert answers to new questions and challenges."

Maksut Shadayev, Russian Minister of Digital Development, Communications and Mass Media, opened the Forum by pointing out the following: "The Internet is the neural system of modern society and it requires to be dealt with, with care. Russia was at the roots of the Internet Governance Forum (IGF) and the first country in Eurasia with a national Internet Governance Forum. Today we are dealing with new challenges and threats which call for new responses. The dialogue on the RIGF platform is precious. I would like to wish all the people taking part in this forum every success and to assure them that the issues discussed here will be considered and may become a reality."

Tatyana Matveyeva, Head of the Department for the Development of Information and Communication Technologies and Communications Infrastructure at the Russian Presidential Executive Office, added that cooperation is a dialogue that produces agreements and arrangements; currently, as the Internet is seeing more challenges, it is very important to listen to each other and make the right decisions on Regional and International levels.

Maksut Shadayev and Tatyana Matveyeva hosted an award giving ceremony to present prizes and commendation letters for the contribution to building and developing the Russian Internet. During this symbolic event on the anniversary of .RU, six Coordination Center representatives received the awards. Coordination Center Director Andrey Vorobyev, Deputy Director Irina Danelia, Head of the Department of Registrar and User Relations Georgy Georgiyevsky and Head of Technical Support for the Department of Registrar and User Relations Lyubov Vidanova received commendation letters from the Russian President. First Deputy Director of the Coordination Center Vladimir Gorzhaltsan and Deputy Director Andrey Romanov received the medals of the Order for Services to the Fatherland (2nd degree).

HIGH-LEVEL PLENARY

Alexander Khinshtein, Chairman of the State Duma Committee on Information Policy, Information Technology and Communications, continued the opening ceremony. He noted that the Russian technological system and Internet infrastructure were ready for the challenges of the COVID-19 pandemic. “Thanks to their readiness, the Russian Internet has made a qualitative leap in its development over the past year,” he said. “Russia has always been famous for its ‘golden brains’ and we have numerous examples of successful IT projects. We need to prioritize Russian assets in all segments of our digital life.” Alexander Khinshtein also called for developing a collective social agreement between the state, businesses and users, that would make the digital sphere more user-friendly and safe, helping the Internet become a positive learning environment.

Anriette Esterhuysen, Chair of the IGF Multistakeholder Advisory Group, also greeted the participants and noted the role of RIGF in developing the global Internet Governance. She encouraged all the participants to attend IGF 2021, due to be held in Poland in November. She elaborated on the current problems, which are in the focus of IGF, such as economic matters, social inclusivity, human rights, connectivity and providing access to the internet to every person in the world, cybersecurity, digital inequality, climate change, inclusivity and many other things.

Doreen Bogdan-Martin, Director of the ITU Telecommunication Development Bureau and a candidate to become the next Secretary-General of the International Telecommunications Union, in particular focused on inclusivity of the Internet while presenting her remarks. She pointed out that half of the population of the world, or 3.7 billion people, still have no access to the Internet. She also spoke about the UN’s program aimed at addressing this issue and providing the entire World Population with access to the Internet by the year 2030. She also talked about the International efforts to engage young people in resolving these matters and specifically noted the role of national Internet Governance Forums, including Russia’s IGF.
VimpelCom President Rashid Ismailov, who is also Russia’s candidate for International Telecommunication Union Secretary-General this year, noted that every country has its own legislation but we all share the same internet and “balkanization” of the internet is not on anybody’s agenda. “We need to preserve the Internet as it is today and develop it accordingly.”

Youth Digital Ombudsman Dmitry Gulyayev and his colleague Alexey Starikov presented the results of the 1st Russian Youth Forum on Internet Governance, Youth RIGF 2021. One of the outcomes of the forum, a Youth Message, reads, in part: “We see the Internet as a secure and friendly environment where every person can decide who to be, how to learn a new profession, how to receive and transfer new knowledge. We see the Internet as a space with freedom of speech, a place of universal equality and priority for general human values, where technological achievements contribute to preserving our diversity. We support minimizing the damaging impact of modern technology on the environment and human health.

SESSION 1. INTERNET GOVERNANCE

In July 2018, the UN Secretary-General announced the creation of the High-level Panel on Digital Cooperation to develop proposals on improving cooperation in the digital area between governments, the private sector, civil society, International organizations, research organizations, the engineering community and other interested parties. The panel finished their discussions and in June 2019 presented the concluding report, The Age of Digital Interdependence.

The report comprises five sets of recommendations on how the international community could adopt joint measures to streamline digital technology and lower the risks:

- Build an inclusive digital economy and society;
- Develop human and institutional capacity;
- Protect human rights and human agency;
- Promote digital trust, security and stability;
- Foster global digital cooperation.

In 2025, Russia will host the last IGF that will take place under the current mandate; the Forum reform plan will be ready by that time.

Talking points:

- Why do we need global digital cooperation?
- Does the digital world share common values?
- Are there effective platforms where all countries can be heard?
- How can inclusive global Internet Governance be created within the G193 (UN) instead of other “Gs” such as the G7, G20 or G2 (China–US)?
- How can the risk of Internet fragmentation affect global economic development?
- How can the risk of Internet fragmentation affect Global Supply Chains, social connections, scientific cooperation, and so on?
- What are the prospects for the implementation of the Roadmap for Digital Cooperation?

SESSION 1. INTERNET GOVERNANCE

The session on internet governance, moderated by Andrey Vorobyev, Ilona Stadnik (Coordination Center for TLD .RU/.РФ) and Jovan Kurbalija (DiploFoundation), focused on the report, The Age of Digital Interdependence, released in 2018 by the High-level Panel on Digital Cooperation, established at the instruction of UN Secretary-General to develop proposals on improving cooperation in the digital area between governments, the private sector, civil society, international organizations, research organizations, the engineering community and other interested parties.

The participants discussed why global digital cooperation is necessary, what values the digital world shares as well as what efficient platforms are available where all countries can be heard. Other items on the agenda included the risk of internet fragmentation and the implementation of the Roadmap of Digital Cooperation.

Maxim Parshin, Deputy Minister of Digital Development, Communications and Mass Media of the Russian Federation, noted that internet governance requires a global consensus resulting in a global pact identifying coordinated approaches and policies. “It is important to designate a body within the UN that will be responsible for developing and implementing legal regulations and standards on internet governance. The International Telecommunications Union (ITU) seems to be the most suitable platform for this purpose,” he added.

President of VimpelCom Rashid Ismailov, who is also running for ITU Secretary-General this year, pointed out the current trend for dividing countries into two blocs – those who support total freedom of the internet and believe in the so-called Silicon Valley model and those who are concerned about national sovereignty. The parties have been on the path towards convergence though, especially on the ITU platforms since the union is focusing on developing countries and eliminating digital inequality.

“The key areas for international cooperation include growing economic inequality in view of digitalization. The digital gap is widening: with monopolies growing, local companies suffer from competition and fail to properly process personal data, including due to the lack of a qualified workforce that drains developed countries. One way to overcome the digital gap is to optimize tax and other legal regulations. Digital giants should pay higher taxes in the countries where they operate. Still, it is vital not to overdo it,” Rashid Ismailov said.

SESSION 1. INTERNET GOVERNANCE

Mandy Carver, Senior Vice President for Government and Intergovernmental Organization (IGO) Engagement at ICANN, spoke about the principles of technical governance that were first presented on December 20 at the 15th IGF: “Technical internet governance focuses on the way the internet works. It is purely the technical aspects related to the components, that contribute to secure, stable and resilient Internet. A crucial aspect of technical internet governance is the need to ensure, from a technical perspective, that the internet is accessible to everyone. The decision that we use the integrated domain name space, the common IP-addressing system and common protocol specifications, was the biggest factor enabling the growth of the internet over the last 40 years.”

Jovan Kurbalija, founding director of DiploFoundation and head of the Geneva Internet Platform (GIP), did not agree that the technical community represented by ICANN cannot be concerned with political issues because on the internet there is no clear division between technical and non- technical aspects. It is indeed important, he believes, to maintain security and uninterrupted operations of the core infrastructure. Still, there are many important matters at the intersection of technical aspects and geopolitics.

The session participants also discussed engagement of all stakeholders into the internet governance narrative, including representatives of small countries. They noted that dividing countries into supporters of total freedom and supporters of national sovereignty is an outdated approach as their views are becoming largely similar. Summarizing the session, Jovan Kurbalija proposed to refrain from counting models and looking for differences but instead make an effort to find common ground.

RIGF SECTION

SESSION 2. EMERGING TECHNOLOGIES. ARTIFICIAL INTELLIGENCE AND ETHICS

Under the Concept on Regulation of Relations in Artificial Intelligence and Robotics until 2024, increasing the independence of such systems, reducing human control over the process of use and the not quite transparent process of decision making have created public demand for regulatory restrictions on the use of artificial intelligence and robotic systems.

Thus, one of the conditions for introducing artificial intelligence in such areas as medicine, industry and transport is the need for a responsible approach to the development of AI. This approach will allow for outlining mechanisms to delegate process management to AI and minimize existing risks.

Ethics and artificial intelligence have become a key topic for discussion at various levels: national, international and sectoral. It is becoming increasingly obvious that this issue can be a cornerstone of soft law on regulating artificial intelligence systems.

RIGF
RUSSIAN INTERNET GOVERNANCE FORUM
RIGF
RUSSIAN INTERNET GOVERNANCE FORUM
RIGF

SESSION 2. EMERGING TECHNOLOGIES. ARTIFICIAL INTELLIGENCE AND ETHICS

During the session Emerging Technologies. Artificial Intelligence and Ethics moderated by Karen Kazaryan (RAEC) and Anna Abramova (MGIMO), experts discussed the importance of a responsible approach to developing AI in such areas as medicine, industrial production and transport. They acknowledged that this approach provides for identifying mechanisms to delegate process management to AI and minimize existing risks. Ethics and artificial intelligence were among the key discussion topics at different levels, both national, international and sectoral. It is becoming increasingly obvious that this aspect may serve as a pillar when building a foundation for soft law in AI regulation.

Karen Kazaryan confirmed that the majority of discussion platforms are currently concerned about ethics and AI. Numerous experts from around the world are working on the implementation of AI, a technology that can help people and businesses at large. AI can also contribute to eliminating digital inequality, promoting inclusivity and providing access to technology.
Anna Abramova added that there are more than 100 documents on ethics at this point, which is an issue of heated debates. As AI is developing, both its potential and risks are becoming more apparent. Therefore, it is necessary to maintain balance between the regulatory efforts and promoting the technological progress.

Jan Kleijssen (Council of Europe) stressed that AI is creating numerous opportunities but that it is also a source of new discrimination practices as new categories and new objects of discrimination are emerging right now.
Elza Ganeyeva (Microsoft) offered a detailed picture of the basic principles of dealing with AI that were adopted by Microsoft five years ago. She emphasized the importance of verifying the practical implementation of these principles in each particular case.

Andrey Kuleshov (MIPT) noted the importance of defining terms, subjects and objects of law in AI regulation, which would help professionals and society discuss AI using a language understood by everybody. “ This is exactly what a code of ethics is for. This code must be human-centered, risk- oriented and based on the principle of commensurate liability.”

“Thirty major AI developers have their corporate codes of ethics, the purpose of which is to make the AI technology safe and trustworthy. Self- regulation and development of ethical principles is the most reasonable approach. We are working with the AI Alliance on creating a universal Russian code of ethics. Our goal is to produce a set of rules that would be reasonable for every person,” concluded Andrey Neznamov (Sberbank). The session was also attended by Andrey Ignatyev (Center for Global IT Cooperation), Alexander Tyulkanov (Skolkovo Foundation) and Maxim Fedorov (Skolkovo Institute of Science and Technology).

SESSION 3. REGULATION: DATA SOVEREIGNTY

The second day of RIGF 2021 opened with the session “Regulation: Data sovereignty” moderated by Mikhail Yakushev (Higher School of Economics). Participants discussed the concept of data sovereignty and its relation to data security, cloud computing, technological sovereignty and data management at the macro-level.

Bertrand de la Chapelle (Internet & Jurisdiction Policy Network) noted that a state has both rights and responsibilities when it comes to internet policy. Any internal decision concerning the internet made by a state will also affect external actors, which should always be remembered. “Although we are dependent upon Big Data to conduct our economic life and our private life, we are not familiar with the particular nature of that and we are approaching it from an outdated perspective.

Not only governments set the rules but also major platforms have their terms of service for people who are outside the country where they are incorporated. We need to find a new architecture and a new government framework that allows for legal interoperability between different actors.” Thomas Schneider (OFCOM) said that digital transformation raises fears in people of losing control over their lives. “We need to make sure that people trust the solutions proposed. If they don’t, they will either go on the street to protest against governments or against companies and their digital technologies,” he warned. He believes that the concept of digital sovereignty that implies the state’s absolute control over data makes it more difficult to take advantage of the digital technologies that develop thanks to free exchange of data and opinions. "We think it makes little sense to build new digital walls but it makes much more sense to work together with everybody nationally and internationally on rules that earn the trust of people and businesses that create a balance of power and control so that all can profit from digital innovation”.

SESSION 3. REGULATION: DATA SOVEREIGNTY

Milos Vagner of the Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor) described the agency's approach: "We look at data sovereignty through the lens of digital sovereignty and believe that it is both the right and responsibility of the state to determine the rules for data circulation on its territory. These rules can ensure that data work for the benefit of the country and can protect personal data and people's personal information. It is our current belief and we will continue to proceed from the premise that in Russia, compliance with our laws is more important than observing foreign laws".

Nikolai Dmitrik (Moscow State University) pointed out that the main asset of the modern economy is focus and having to comply with the legislation of several countries at the same time often stalls the development of international companies. "The principle of sovereignty in cyberspace has been replaced with the principle of legal certainty," the speaker said.

Aleksandra Orekhovich (Internet Initiatives Development Fund) pointed out that in developing personal data regulation and the concept of digital sovereignty, it was important to understand who the data sovereign was. "The existing concepts fueling the development of the internet in Russia are based on the idea that the state is the sovereign and data proprietor. But I think that if we fit the individual as a data owner into the governance concept where the individual becomes a full-fledged proprietor of their data so that they are able to manage and control it, this will lead to business development and a balance between the interests of the individual and the state," she added.

Natalia Velikorodnyaya (MTS) agreed with her colleague and added that the state cannot be a sovereign with respect to data. The state must perform a regulatory function and create conditions for individuals to protect their personal data and for businesses to be able to work with data.
In his summary of the session, Mikhail Yakushev (Higher School of Economics) expressed hope that data regulation will be a frequent subject of discussion not only at future internet governance events but in everyday life and work as well.

SESSION 4. DIGITAL PLATFORMS: THE RULES OF THE GAME

Hosted by: Competence Center for Global IT Cooperation.

Digital platforms have become an integral part of our life. They provide numerous opportunities for public authorities, businesses and individual users, and are a powerful driver of economic growth. At the same time, the fast-growing role of transnational internet giants in economic and political processes poses a serious question about their responsibility toward the users and the state.

Equal competitive conditions must be created for domestic and foreign developers operating on the digital technologies and services market. Often, the companies operating in national jurisdictions are carrying an incomparably heftier tax and legal burden, whereas foreign corporations not only boast significant economic resources, but also get away with circumventing national legislation. This is the case in Russia, and this state of affairs negatively affects the domestic IT industry.

A situation where foreign companies evade taxes, fail to provide reporting and ignore court rulings is unacceptable for the state. Major players must be legalized in thenational legal field and have official offices in the host countries. This is a critically important step if we want to build an effective dialogue with them.

Talking points:

- How to create an environment of trust on online platforms and maximize the use of their capacity in the interests of digital transformation of the economy and for the benefit of individual users?
- What might mutually acceptable and fair national legislation for foreign digital platforms look like?
- How to enforce fair taxation of multinational internet companies and ensure their compliance with the competition rules?
- What common ground can be found in the approaches of Russia, foreign countries and integration associations to ensuring responsible market behavior of transnational internet companies?

SESSION 4. DIGITAL PLATFORMS: THE RULES OF THE GAME

The afternoon of April 8 at RIGF 2021 was devoted to digital platforms and ways to build trust in supply chains. During the session on Digital platforms: the rules of the game, hosted by the Competence Center for Global IT Cooperation, the participants agreed digital platforms have become an integral part of our lives and provide numerous opportunities for public authorities, businesses and individual users, and are a powerful driver of economic growth. At the same time, the rapidly growing role of transnational tech giants in economic and political processes poses a serious question about their responsibility toward the users and the state.

The moderator, Vadim Vinogradov (Higher School of Economics), invited the participants to suggest ways of creating an environment of trust on online platforms to maximize their potential; how to enforce fair taxation of multinational internet companies and ensure their compliance with rules on competition; what common ground can be found in Russia’s approaches and those of other countries in order to ensure responsible market behavior by transnational internet companies.

Vladimir Tabak (ANO Dialog) defined digital platforms and added that digital platforms help people solve real problems by optimizing the process, and they should primarily be utility- oriented. “From where I stand, recent years have shown that the concept of a digital platform has a dual reputation. On the one hand, we have seen many projects that were digital for the sake of being digital. On the other hand, there are other projects that, due to a few simple online processes, are really helpful in greatly reducing the time needed to solve problems offline. For me, the definition of a digital platform is quite simple – it is a platform that helps people solve problems offline by optimizing these processes online. This is the essence of a digital platform and the concept that we are trying to implement in our work,” the speaker said.

SESSION 4. DIGITAL PLATFORMS: THE RULES OF THE GAME

Bella Cherkesova, Deputy Minister of Digital Development, Communications and Mass Media of Russia, noted that IT companies are gradually ceasing to be mere parts of technological infrastructure. They now have a tremendous influence on the audience. They are constantly improving their technological solutions for targeting information and achieving great results in managing the audience's attention. "At the end of last year, Russia adopted legislation to regulate social media. In particular, they concern sanctions on websites whose owners restrict the dissemination of socially significant information. It was a prompt response to the recent challenges. Nevertheless, a number of issues remain unresolved," she added.

Lucien Castex from AFNIC noted that there is still no single definition of a digital platform. In his opinion, this situation significantly slows down the development of general regulation. At the same time, there are several vectors of regulation – such as combating the spread of illegal content or regulating the activities of information intermediaries – which are not country-specific and are treated in a similar way in almost all countries.

Vladimir Gabrielyan (Mail.Ru Group) pointed out that the internet is changing very quickly, and digital platforms are rapidly changing along with it. Legislation regulating tech companies and digital platforms has often become irrelevant by the time it comes into effect. Vadim Glushchenko from the Competence Center for Global IT Cooperation noted that the problem of the relationship between digital platforms and the state and society is global and does not only concern Russia; the contradictions between them are deepening everywhere.

SESSION 5. BUILDING A SYSTEM OF TRUST IN SUPPLY CHAINS

Trust for IT products and services is gaining value amid the developing digital transformation. At the same time, it is not always possible to investigate the producer for compliance with basic security principles. The global community is looking for working cooperation mechanisms between states, IT communities, manufacturers and researchers to develop norms, standards and rules that can regulate this sector.

States should develop and implement measures to promote the role of the private sector and civil society in improving security when using ICT and the security of ICT, including the entire cycle from production to sale. It is necessary to develop open cooperation between all parties, including governments, international organizations, enterprises, IT communities and research institutes as the main stakeholders, and to use a wide range of instruments such as laws and rules, social responsibility, ethics, oversight and self-discipline, as well as norms and standards.

Topics for discussion:

- The basic principles of securing supply chains
- How can security for digital products be improved?
- Detecting vulnerabilities and responsible management: how to promote/improve the attractiveness of the idea of the coordinated detection of vulnerabilities?
- How can public policies help?
- What are the limits of businesses’ responsibility when responding to digital threats?

SESSION 5. BUILDING A SYSTEM OF TRUST IN SUPPLY CHAINS

The second day of RIGF 2021 ended with the session on Building a system of trust in supply chains, moderated by Nikolai Zubarev from ANO Digital Economy.

Experts noted in their remarks that trust for IT products and services is gaining value amid the developing digital transformation. At the same time, it is not always possible to investigate the producer for compliance with basic security principles. The global community is looking for workable mechanisms of collaboration between states, IT communities, manufacturers and researchers to develop norms, standards and rules that can regulate this industry.

Andrei Yarnykh from Kaspersky Lab said that trust is the most important currency, especially in matters of information security. Stanislav Fesenko (Group-IB) added that trust ensures stability; it can and should be assessed from the financial point of view, and it is extremely important to build trusted supply chains in those areas of economic development on which the stability of our state depends.

Yelena Bocherova (Acronis-Infosecurity) spoke about the scope of business responsibility when responding to digital threats and raised the question of who should inform and educate users about information security rules.
Artyom Kungurtsev (Moscow Department of Information Technology), in turn, noted that, as representative of the public sector, the Department of Information Technology should be able to quickly pick up on the vulnerabilities that emerge on a regular basis. He invited vendors to think about this and make changes to the existing government contacts – to offer a bug bounty program for the warranty period. “We want the products that we use for government projects to be as securely protected as possible,” he added. Ghislain de Salins, OECD and Oleg Sedov (Rostelecom-Solar) also spoke about ways to create trusted supply chain systems. “Trust is an important aspect of the economy,” Ghislain de Salins concluded.

SESSION 6. ATTRIBUTING CYBERATTACKS ON THE INTERNET. MYTHS BUSTING

The past four years have seen unprecedented growth in the number of accusations of interfering in the work of government agencies, democratic institutions, major companies and critical infrastructure all over the world by Russian, Chinese, North Korean, Iranian and other hackers. At the same time, such accusations (or the media reports) often lack evidence and are based only on the IP addresses of the alleged cybercriminals or the VPN gateways they use in a certain language.

Topics for discussion:

- The image of the enemy. Is attribution a technical of geopolitical issue?
- Is univocal identification of cybercriminals possible on the internet?
- Highly Likely: Approaches to attributing cyberattacks (CAM, CAR, Q Model, WOMBAT, etc.)
- What technical methods, in addition to IP and DNS addresses, autonomous systems or time zone, are used in attributing cyberattacks?
- False Flag: Disguising as other hacker groups. Real cases
- Felix Edmundovich: Should a cyber investigator be a linguist?
- Various jurisdictions: What are the difficulties in interstate interaction between law enforcement agencies when investigating cybercrimes?
- How can attributing cyberattacks be improved?

The third and final day of RIGF 2021 opened with the session on Attributing cyberattacks on the internet. Myths busting. The moderator, Alexei Lukatsky from CISCO, delivered opening remarks pointing out the special relevance of this topic today due to a rapid growth in the number of accusations of cyberattacks against various countries. The speaker suggested considering whether unequivocal identification of cybercriminals is possible on the internet at all, what approaches are used in attributing cyberattacks, and what difficulties law enforcement agencies encounter with interstate exchanges during the investigation of cybercrime.

Alexander Kalinin (Group IB) cited some examples of attribution of attacks by large hacker groups. He spoke about the company's experience in investigating cyber incidents and emphasized that while each of the attribution elements taken separately – signature, hosting and registrar, graph analysis or additional indicators – might mean nothing, all taken together, they can actually lead to attributing a cybercrime.

SESSION 6. ATTRIBUTING CYBERATTACKS ON THE INTERNET. MYTHS BUSTING

Sergei Golovanov from Kaspersky Lab agreed with his colleague. He shared examples of recent incidents and added that attributing an attack is critical to further prosecution of the perpetrators and trial. “Attribution is everyone’s responsibility, including witnesses, specialists and experts. Experts can express their opinions, but experts working with material evidence cannot afford any guesswork – they have to use a clear methodology, and the examination process must be reproducible,” he said. Attribution requires clear evidence, verified by experts, and not the personal opinion of an individual. Furthermore, before calling someone a criminal, the case must be brought to court.

Liis Vihul (Cyber Law International, Estonia) spoke about the approaches to attributing cyberattacks in international law and the difficulties encountered in the investigation of cross-border crimes. She noted that, to be able to claim that some action took place in a country’s cyberspace, evidence needed to be presented – not only technical information but also other things such as reports from various organizations, research etc. Only then can the evidence base be considered complete.

Igor Zalevsky (Rostelecom-Solar) spoke about how cybercriminals are identified in reality at the request of a specific company. He noted that most customers want to protect themselves from further attacks, while finding the perpetrator who was behind the crime seems less important to them, especially considering that the cost of investigation can be much higher than their losses from the attack.
Summing up the discussion, the experts noted that there are no technical difficulties in investigating cross-border crimes today, but so far, there is no single international judicial body, which is able to handle international cybercrime.

SESSION 7. USER AGREEMENTS WITH INTERNET PLATFORMS: WAY TO PROTECT RUSSIAN INTERNET USERS’ RIGHTS AND THE STATE’S INTERESTS

All internet platforms censor the content and occasionally delete information posted by users and block their accounts. The reasons for such actions are hidden in the depths of user agreements which are not always available in the Russian language (even when an internet platform is oriented towards a Russian-speaking audience and posts advertising in Russian). The user agreement is a civil agreement, subject, as a rule, to foreign law and in most cases not covered by legislation on protecting consumer rights (because the user does not pay directly under the contract).

How can the interests of users be protected under these conditions? Would a national law be enough or is there a need for an international agreement? How can internet platforms be forced to comply with a national or international act?

Topics for discussion:

- Overcoming the inequality of the legal status of the internet platform and the user that all user agreements come with
- Jurisdiction issues: defining the condition where relations between the user and internet platform can be subject to Russian law
- Foreign experience: attempts to introduce regulatory control over the content of user agreements and separate issues (amid scandals with blocking the accounts of public figures)
- Issues of content regulation in light of user agreement terms (grounds for account blocking, detecting illegal information and fraud, etc.)

SESSION 7. USER AGREEMENTS WITH INTERNET PLATFORMS: WAY TO PROTECT RUSSIAN INTERNET USERS' RIGHTS AND THE STATE'S INTERESTS

Overcoming the inequality of the legal status of the internet platform and the user that all user agreements come with was the focus of the next session, User agreements with internet platforms: Way to protect Russian Internet users' rights and the state's interests.

According to moderator Anna Dupan (Higher School of Economics), despite the differences in the phrasing of the user agreements, almost all of them contain a clause stating that the platform has the right to block any user's account or to censor or delete their content without any reason. At the same time, the platform is not liable to the user for any harm caused as a result of such action. More than that, to be able to use the platform, users are required to submit their personal data – in fact, the platform gets unlimited access to their data, and not only to data it actually needs to fulfill the user agreement.

Many Russian users have encountered blocking on YouTube due to incorrect markup of their video content, said Karen Kazaryan from RAEC. The platform has shown no interest in getting to the root of the problem.
Anna Starkova (Rossiya Segodnya) also cited examples of injustice and blockages that RIA Novosti faces as a media outlet using Western websites, and called for the protection of the rights of Russian users and companies. "First of all, we need to build communication with Western social media through their representative offices in our country. Russian internet companies could also help defend the rights of the Russian media and information sovereignty, but to be able to do so, they would have to create platforms that would be superior to their Western counterparts. And we actually have enough potential for that, and it is the only way we can avoid the blocking of individual users and media outlets alike," she said.

Dmitry Magonya (ART DE LEX) noted that internet platforms now have a lot of power over users. "It is imperative for state authorities to regulate the internet platforms. This is happening all over the world. States must find ways to protect the interests of the population in their interaction with tech giants," the speaker said.

SESSION 7. USER AGREEMENTS WITH INTERNET PLATFORMS: WAY TO PROTECT RUSSIAN INTERNET USERS' RIGHTS AND THE STATE'S INTERESTS

Roman Krupenin, representative of Yandex, Russia's largest internet platform, said platforms today are struggling with sometimes conflicting requirements that cannot be met. Many modern services could not work without user data, and personalization is primarily needed for the convenience of the user. "In any case, when working out requirements for platforms, the authorities would need to use the most balanced and differentiated approach," he concluded.

According to Elena Zayeva (FAS Russia), the accumulated data can strengthen companies' bargaining power and increase competition in the market. "If platforms manage people's personal data in such a way that users understand and exercise their right to switch platforms, then platforms won't overstate their requirements. But for users to know how to use their rights, these rights must be explained to them first," she said.

Yury Kontemirov (Roskomnadzor) also highlighted personal data security, adding that the user should be able to decide whether they agree to the conditions or whether to refuse certain services or conditions the website offers. "We are working to foster a culture of online conduct. Consumers need to understand which resources can be trusted with their personal data, which resources do not carry risks of violation of their rights or leakage of personal data. A person should be able to use the criteria that are proposed as part of various awareness- raising activities aimed at fostering this culture to figure out who can be trusted in the internet landscape," he said.

Summing up the discussion, Anna Dupan from Higher School of Economics noted that the platforms need to be given the opportunity to set the rules of the game themselves, and communicate them to their users. They need to explain to people how exactly their data is used. A dialogue between the platform and the user moderated by the state would help avoid serious problems. There would be no need to deal with emerging problems by blocking users or slowing traffic – they would be addressed by means of dialogue.

SESSION 8. TAKING STOCK. YOUTH SESSION

Representatives from the Youth Session will present statements that were prepared during the session.
Participants in the Youth Forum in Skolkovo will also present reports on the forum and its results.

The Coordination Center's Youth Projects Manager Ilona Stadnik gave an update on the center's projects and activities such as Summer Internet Governance School, Digital Reality Discussion Club, special internet governance course for young people at RIGF and the Coordination Center Youth Council. The Summer Internet Governance School, organized by the Coordination Center together with the International Relations Faculty of the St. Petersburg State University, took place in August and September 2020. It became part of the global movement, Schools on Internet Governance (SIG).

Together with industry experts from the St. Petersburg State University, Higher School of Economics, regional ITU office, the Kaspersky Lab, ICANN and other organizations, participants of the Summer School discussed how the internet infrastructure functions, what approaches there are in the internet governance and what the national legislation's role is in this process.

On the eve of RIGF 2021, young participants attended a special course on internet governance to learn more about the forum's agenda. At the end of the special course, the students formed their own conclusions based on the lectures given by experts, which were included in the Youth Message at the First Russian Youth Internet Governance Forum, which was held in Skolkovo on April 6.

Roman Chukov, Russia's representative in the IGF Multistakeholder Advisory Group and the chair of the Center for Global IT Cooperation Competences, noted that the discussion at the youth forum on April 6 brought together key youth speakers, such as bloggers, tiktokers, and renowned experts on IT, as well as scientists and officials.

SESSION 8. TAKING STOCK. YOUTH SESSION

Irina Trapeznikova noted that there was a lack of people both in Russia and all over the world who could serve as mediators between youth and government bodies, international organizations, and businesses.

“We need a person who will convey the youth’s thoughts to the superiors. And we, the youth ombudsmen, will be engaged in analyzing the existing youth initiatives and announcing them, including at the Youth Internet Governance Forum. I would like to see this initiative carried on and brought to an international level in order to cooperate with colleagues from foreign universities,” she said.

Coordination Center Director Andrey Vorobyev talked about the center’s educational projects: IP&IT Law and DOT Journalism contest and the Explore the Internet & Govern It! online championship among others. He thanked the young participants for their active work and expressed hope that with their help the center’s Youth Council will get a concept reboot.

Alexei Rogdev, General Director of the Technical Center of Internet, added: “It is necessary for us to involve young people in the internet governance in order to have a replacement in the future: young active users who understand what the internet is and know its rules.”

COORDINATION CENTER
FOR TLD .RU/.РФ

RIGF is hosted by Coordination Center for TLD RU

CONTACTS

Address 127083
Moscow, 8 Marta str., 1
bld. 12

Tel. +7 (495) 730-29-71
Fax +7 (495) 730-29-68
Email rigf@cctld.ru