|  |  |
| --- | --- |
| **Council Working Group on International Internet-related Public Policy IssuesSeventeenth meeting – 19-20 January 2022** |  |
|  |  |
|  | **Document CWG-Internet-17/3-E** |
| **7 January 2021** |
| **English only** |
| Contribution by the Russian Federation |
| PROPOSALS TO DISCUSS THE CHALLENGES AND LACK OF OPERATIONAL ACTIVITY ORGANIZATIONS/OPERATORS OF CRITICAL INTERNET INFRASTRUCTURE(first phase) |
|  |

## 1. Introduction

At the 15th CWG-Internet meeting held in January 2021, the Russian Federation proposed to discuss the status of international governance of the critical Internet infrastructure ecosystem, including systems providing domain names and Internet addresses. Continuing this topic, at the 16th meeting of the CWG-Interne the Russian federation presented risk analysis of the existing Internet governance and operational model. This proposal implied further discussion and, if necessary, development of concrete measures to mitigate risks and save the integrity of the Internet public core. It was proposed to hold a discussion of this document with the involvement of all interested parties through an open consultation process, and then identify the risks that are realistic and highest priority. Such a discussion did not take place, despite the existing challenges and problems in the international Internet governance system.

Due to the growing importance of political, economic and criminal threats in Internet ecosystem, it seems advisable to consider the risks already presented earlier one by one and discuss each of the mentioned risks in detail at the CWG-Internet meetings. During such successive discussions Member-States can assess the realism, priority, possibility of neutralization of such threats and, if necessary, further actions.

## 2. Discussion

The Internet is a key infrastructure of the emerging global information society and digital economy. Digital services impact on the political, economic and socio-cultural spheres of the human life at all levels - from global to national/regional. Therefore, today Internet governance is one of the most relevant and important topics in international relations. Due to the growing importance of the Internet ecosystem (including all levels from technical infrastructure to digital services), specific issues related to Internet governance and the management of certain areas of digital services are included in the international political agenda:

• information security;

• privacy protection;

• regulation of e-commerce;

• intellectual property protection;

• respect for human rights in the information society;

• bridging the digital divide

• and others.

However, until now, legal relations on the Internet are not sufficiently regulated at the international level. To date, there are no universal international legal agreements in international law that could regulate Internet governance issues. The problem lies not only in the lack of consensus at the international level, but also in the global nature, multilevel and multilateral participation in the formation of legal regulation related to the Internet. At the same time, the reality of today is that there is no meaningful discussion on most problems and there are no prospects for achieving specific regulatory solutions. That is why the Russian Federation constantly offers to discuss these issues in the CWG-Internet, as the most suitable platform.

The cross-border nature of the Internet dictates the need for international and even global regulation. However, instead of an open, broad dialogue on the internationalization of the Internet governance system, we see a number of dangerous trends for the global network. We would like to highlight two main ones.

Firstly, the dependence of organization/operators of critical Internet infrastructure providing over national functions on the decisions of one national administration has turned from a potential threat into a real fact. The most striking example is the recent blocking by the national court of bank accounts and, accordingly, the operational activities of the Regional Internet Registry (RIR) AFRINIC, which performed over national, unique functions. That is, organizations that perform the role of operators of critical Internet infrastructure currently do not have the status of international organizations with immunity to decisions of the national administration of its jurisdiction.

Secondly, the growth of autonomous, unsynchronized national initiatives on Internet regulation, while mandatory for the cross-border application. The most striking example is the General Data Protection Regulation of the European Union (GDPR), which has had an extremely impact on the ICANN operational activity related to WHOIS service. As a result of which ICANN has been spending significant resources for the third year on the process of bringing its operating activities to GDPR requirements and the result has not yet been achieved. It should be noted that ICANN will also have to spend resources on implementing the requirements of other national regulators in this area as the next stages after the implementation GDPR. The lack of coordination of national Internet regulation is the most serious challenge and the reason for the fragmentation of the global network that already has begun.

In this regard, in the list of threats proposed by the Russian Federation for priority consideration, we would like to highlight two interrelated risks:

• the dependence of organizations/operators of critical infrastructure, in particular Regional Internet Registry (RIR) on the decisions of one national administration;

• restrictions on access to internationally used infrastructure (violation of the principle of non-discriminatory access).

The above risks are discussed in more detail in the prepared Appendix 1. Realizing that not all issues related to the governance of critical Internet resources need to be addressed within the ITU, however, however, in the absence of international platforms suitable for preparation of practical urgent solutions, the CWG-Internet seems to be the most valuable platform for discussion between Member States and all interested parties.

## 3. Proposal

The tasks of the CWG-Internet are Identify, study and develop matters related to international Internet-related public policy issues. ITU Council Resolution 1305 defining the public policy issues to be addressed in the CWG-Internet contains the topic “The security, safety, continuity, sustainability, and robustness of the Internet”. This makes appropriate to organize work on the analysis of risks of the existing Internet governance and operational model, preparation of recommendations and further draft international legal acts in line with ITU responsibility.

In this regard, within the framework of the topic "The security, safety, continuity, sustainability, and robustness of the Internet", it is proposed:

1. Conduct the following open consultations with all interested parties on the topic "Reliability and stability of the operational activity organizations/operators of critical Internet infrastructure: key and challenges of their operating activities, in particular the risks of being in national jurisdictions."

2. Invite Member States to present at the 18th CWG-Internet meeting their vision of the risks for reliability and stability of existing model of the operational activities organization/operators of critical Internet infrastructure.

3. Invite Member States to present at the 18th CWG-Internet meeting their inputs and proposals on possible ways to overcome existing challenges and neutralize risks for operational activity organizations/operators of critical Internet infrastructure (see Appendix 1).

4. Invite Member States to present at the 18th CWG-Internet meeting their views on what international structures and procedures can overcome the existing challenges and risks for operational activity organizations/operators of critical Internet infrastructure.

Appendix 1

Inputs for risk analysis of the existing model of the operational activities organization/operators of critical Internet infrastructure

## 1. Issue

1.1 The dependence of the organization/operators of critical Internet infrastructure (in particular Regional Internet Registries) on the decisions of one national administration (jurisdiction of registration).

1.2 Restrictions on access to internationally used infrastructure (violation of non-discriminatory access).

## 2. Potential treats

2.1 Operational activities of the organization/operators of critical Internet infrastructure (for example, the Regional Internet Registry) may be limited by a decision of the national administration and/or a court decision of the country in which this organization/operator is located. As a consequence,

• restrictions for all partners of this organization/operator of critical Internet infrastructure, which result in restrictions for end users;

• violation of the integrity and connectivity of the public core of the Internet.

Operational activity of the organization of the critical infrastructure operator[[1]](#footnote-2)

2.2 Access to critical infrastructure for actors from other countries will be completely or partially restricted by a decision of national administration or a court decision. As a consequence, restrictions for counterparties from other jurisdictions of this organization/operators of critical Internet infrastructure.

## 3. Rational

The institutionalization of Internet governance mechanisms was carried out by the US government in the mid-90s and was, in principle, adequate to the scale and importance of the Internet at that time. Since then, the importance, scale and level of penetration of Internet services in all spheres of life: in public services, in the economy, in people's daily lives have increased many times, and the principles and mechanisms of global network governance have remained the practically same. Thus, a vulnerable and unstable Internet governance model has developed for operational activity of organization/operators of critical Internet infrastructure, including Regional Internet Registries. It seems that necessary to consider the basic level of the global network governance organization, to which, first of all, must be include the addressing system and unique identifiers, that is, the system of IP addresses and DNS.

In the existing Internet governance model the organization/operators of critical Internet infrastructure are national legal bodies under control of particular jurisdiction and are not immune to the decisions of national administrations. It is already possible to give examples when the decision of one national administration negatively affects the activities of other countries using the Internet.

Case 1

On July 23, 2021 AFRINIC received an [order of the Supreme Court of Mauritius dated July 13 , 2021](https://cloudinnovation.org/attachmentlist/%287%29Court%20Ruling%20and%20our%20appeal.pdf)[[2]](#footnote-3) to freeze the organization 's bank accounts . AFRINIC funds held in bank accounts at SBM Bank (Mauritius) Ltd and Mauritius Commercial Bank Ltd in the amount of 50 million US dollars, were frozen. AFRINIC CEO Eddy Kayihura immediately issued an [official video message](https://youtu.be/VmJNnVS-lo4)[[3]](#footnote-4) to community members and partners to highlight the issue. In a video message, Mr. Kayihura noted that, despite the prevailing legal circumstances, the registrar continues to operate in the same mode, serving users both in Africa and around the world, however, it is not yet able to fulfil a number of financial obligations (in particular, the payment of salaries to employees) for an indefinite period. If banking restrictions remain in place for several months or more, the organization's activities will have to be stopped, since it will not be able to carry out its work and provide operational activities. The bank accounts were blocked by a court decision as part of a lengthy trial initiated in 2020 by one of the members of the organization – the network operator [Cloud Innovations Ltd](https://cloudinnovation.org/)[[4]](#footnote-5), registered in Seychelles and providing services in many African countries. The company is the third largest member of AFRINIC and serves millions of end users worldwide. The company also owns a pool of IP addresses, which, as it was revealed in 2020 during the AFRINIC audit, were misappropriated and used for other purposes than stated in the establishing documents. To date, the accounts have been unblocked, but the trial is not over.

Case 2

Another case of limiting the cross-border activities of organizations operating critical infrastructure can be attributed to the implementation by RIPE NCC of EU sanctions directives (see [report on the situation with the implementation of sanctions by RIPE NCC Managing Director Hans Peter Holen](https://ripe83.ripe.net/programme/meeting-plan/ncc-services-wg/)[[5]](#footnote-6)). RIPE NCC, which is a company registered in the Netherlands, that is, in one of the EU countries, is obliged to comply with all sanctions decisions taken in the EU. This means that RIPE NCC cannot allocate new resources to entities under sanctions and the resources allocated to such entities must be frozen in the RIPE database. At the same time, there are no exceptions that RIPE NCC could use to continue working with entities that have fallen under sanctions despite the fact that the organization performs unique over national functions. To date, RIPE NCC has frozen cooperation with a number of organizations from Iran and Syria.

In this regard, RIPE NCC will continue its actions aimed at implementing EU sanctions and monitoring members to identify entities to which sanctions may be applied. As part of ensuring transparency and accountability of RIPE NCC's activities on the implementation of the sanctions regime, quarterly reports on the implementation of sanctions are published (see the [RIPE NCC Quarterly Sanctions Transparency Report](https://www.ripe.net/publications/docs/ripe-768/)[[6]](#footnote-7)).

The example of these two cases shows that the above-mentioned risks are already being realized in practice. And with a high probability process of development the national legislation in the field of Internet regulation will lead increase the influence of such decisions on the work of operational activities organization/operators of critical Internet infrastructure.

It seems appropriate to consider at the CWG-Internet meeting ways to solve the problem of the dependence of organization/operators of critical Internet infrastructure in different countries on the decisions of one national administration and the subsequent restriction of access to internationally used Internet infrastructure (violation of the principle of non-discriminatory access).

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Suggested translation of ITU translators for the following sentence:

Операционная деятельность организации оператора критических ресурсов. [↑](#footnote-ref-2)
2. [https://cloudinnovation.org/attachmentlist/(7)Court%20Ruling%20and%20our%20appeal.pdf](https://cloudinnovation.org/attachmentlist/%287%29Court%20Ruling%20and%20our%20appeal.pdf) [↑](#footnote-ref-3)
3. AFRINIC CEO addresses the freezing of AFRINIC Financial Accounts, <https://youtu.be/VmJNnVS-lo4> [↑](#footnote-ref-4)
4. Cloud Innovation Limited, <https://cloudinnovation.org/> [↑](#footnote-ref-5)
5. <https://ripe83.ripe.net/programme/meeting-plan/ncc-services-wg/> [↑](#footnote-ref-6)
6. https://www.ripe.net/publications/docs/ripe-768/ [↑](#footnote-ref-7)