RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Surveying the Impact of Sanctions on the RIPE NCC

October 2022

The RIPE NCC, as the Regional Internet Registry (RIR) for Europe, the Middle East and parts of Central Asia and a membership association under Dutch law, has been managing the impact of EU sanctions on its core registry function for the past decade. This impact occurs at both an operational level (affecting the RIPE NCC's relationships and interactions with its members) and at a global governance or systemic level (affecting the trust in and viability of the global registry system as currently constituted).

In an effort to better map and understand the full extent of these impacts, the RIPE NCC is currently funding a research project being undertaken by Dr Farzeneh Badii of Digital Medusa. The outcome of this research will be finalised in the first quarter of 2023, and it will look more broadly at the impact of sanctions on core Internet functions (not restricted to the Internet number registry system).

This document is an interim survey of the impact of sanctions, specifically from the RIPE NCC perspective.

Background: The RIPE NCC and its Role

The RIPE NCC, a not-for-profit organisation, is one of the world's five Regional Internet Registries (RIRs). It is an association with more than 20,000 members as of May 2022 and membership is governed by a publicly available Standard Service Agreement. Members of the RIPE NCC can be natural or legal persons and are usually Internet Service Providers (ISPs) or other entities that operate their own networks, such as governments, universities or large corporations. Members are usually based in the geographical working area of the RIPE NCC, which is Europe, the Middle East and parts of Central Asia, including Russia. Blocks of IP addresses are delegated to the RIPE NCC (and the other four RIRs) from the IANA registries, which are maintained by the Internet Corporation for Assigned Names and Numbers (ICANN), an organisation based in the United States of America. The relationship between the RIPE NCC and ICANN is governed by contractual obligations.

The RIPE NCC is exclusively responsible for allocating and registering (blocks of) IP addresses to its members within its geographical service region. The members then sub-allocate these to their customers or use them in their own networks. IP addresses are required for every device that connects to the Internet. For this reason, IP addresses must be unique. The RIPE NCC has no influence over the nature of these devices or the applications they run. It is the RIPE NCC's responsibility to maintain an accurate and up-to-date registry to ensure uniqueness of IP addresses (as part of a globally coordinated system of regional Internet number registries).

The primary purpose of the RIPE NCC is therefore to act as a registry of Internet number resources. The purpose of this registry is to ensure that all stakeholders operating on the Internet can validate which parties are the legitimate holders of distributed Internet number resources, including IP address space. This is the key defining characteristic upon which the entire governance model of Internet number resource distribution for the open Internet was founded. To jeopardise this governance model would be to seriously undermine the stability, reliability and sustainability of the global Internet.

Background: The RIPE NCC and Sanctions

A detailed background on the RIPE NCC's management of sanctions can be found in this article by the RIPE NCC's Chief Legal Officer, Athina Fragkouli:
https://labs.ripe.net/author/athina/how-sanctions-affect-the-ripe-ncc/

To summarise: In 2012, the RIPE NCC confirmed with Dutch authorities that the registration of Internet number resources was not subject to country-specific sanctions; however, EU financial restrictions on designated persons and entities do apply. In 2019, the RIPE NCC was alerted to the fact that two sanctioned entities may be receiving services from the RIPE NCC, and in 2020, the Dutch Ministry of Foreign Affairs (MFA) confirmed that they understood IP resources to be economic resources, as defined in the EU sanctions regulations, meaning that the registrations of any sanctioned entities must be frozen.

Operational Impact

Since 2019, the RIPE NCC has taken several important steps in relation to sanctions compliance management:

- We have significantly upgraded our due diligence procedures, working with third party tools to more reliably identify any business connections with individuals or entities on the EU sanctions list. Details of this upgrade can be found here: https://labs.ripe.net/author/felipe_victolla_silveira/using-third-parties-to-automate-our-due-diligence

- We have committed to publishing regular transparency reports, detailing not only the number of RIPE NCC members whose resources have been frozen due to sanctions, but also the number of potential cases identified and investigated: https://www.ripe.net/search?use_cb_request_state=1&SearchableText=%22RIPE+NCC+Quarterly+Sanctions+Transparency+Report%22&cb-status-current=on

- Slides 17-19 in the following report, delivered at RIPE 85 in October 2022, provide the latest updates on the RIPE NCC sanctions situation: https://ripe85.ripe.net/presentations/79-RIPE-85-Operational-Update.pdf

At the time of writing, a total of **eight** RIPE NCC members and End Users have been identified as being on the EU sanctions list and have had their resource records frozen. However, as documented in the transparency reports linked above, the number of members identified as potentially on the sanction lists is significantly higher (932 cases, as of the Q4 2022 Sanctions Transparency Report). To ensure we remain compliant with sanctions, the provision of additional resources to these members is frozen until they have been fully investigated and cleared, which has the potential to disrupt their business.

It is important to note that activities specifically undertaken to ensure compliance with EU sanctions represent a significant additional cost for the RIPE NCC, including third-party legal and administrative support, extensive staff time, and the fact that such resourcing diverts from other important activities and functions within the RIPE NCC.

Additionally, there is an indirect though serious impact concerning the RIPE NCC's relationship to financial institutions. As our Chief Legal Officer noted on the RIPE Labs blog:

> *Financial institutions in the Netherlands have also been working on their compliance with sanctions and anti-money laundering legislation. This comes after two banks received heavy penalties for non compliance. This has resulted in increased "Know Your Customer" (KYC) efforts, which can lead to restrictions for their customers. Dutch banks do not accept payments from EU sanctioned entities and in some cases from countries they identify as "high risk".*

This situation has meant that the RIPE NCC has faced significant challenges in receiving membership funds from entities that are not specifically sanctioned by the EU, but which are located in countries that banks identify as "high risk" due to the complexity and dynamic nature of the EU sanctions regime.

Systemic Impact

While the impact of sanctions on RIPE NCC operations is manageable, the non-operational impact is potentially far more significant.

Many of the core public functions of the Internet (including the Domain Name System and management of number resources including IP addresses and Autonomous System Numbers) are administered by organisations in the private sector, governed according to multistakeholder policy processes. This is an example of the "multistakeholder approach" that was endorsed by the United Nations in the "Tunis Agenda for the Information Society" (2005), and which has been strongly supported by many governments (including the Netherlands) as the appropriate basis for governance of core functions of the global Internet.

The adoption of sanctions by states in which these organisations are domiciled is increasingly disrupting (or threatening to disrupt) the management and administration of these core Internet functions. A focus of the research being done by Dr Badii is to look at how sanctions are

causing these disruptions, the short- and long-term effects, and possible strategies to minimise such disruption.

Considering this situation specifically from the RIPE NCC perspective and, as noted above, the coordination of a global number registry system, is critical to the stable and reliable operation of the Internet. Such a system is fundamentally based upon a general agreement among all Internet stakeholders regarding which registries are the authoritative record of who holds (and is entitled to use) which number resources. Should this agreement break down, the global Internet would quickly run into operational dysfunction, with no clarity on which network is using (or is entitled to use) which addresses. Such ambiguity could see multiple networks attempting to connect using the same addresses; at a minimum, it would seriously undermine the accuracy that could be assumed or expected from the authoritative registry system.

Private sector organisations with responsibility for management of core Internet functions, such as the RIPE NCC, are necessarily domiciled in a specific state. And while one of the factors in selecting where to base such organisations is the stability and utility of that state's civic institutions (especially its judicial system, which is an essential means of ensuring accountability), there is also a presumption that domestic political positions will not affect or hinder the organisation's ability to carry out its remit in relation to the global Internet. Sanctions, which are developed and applied for political reasons, are counter to this presumption, and as such, they actively undermine trust that the RIRs, as multistakeholder organisations in the private sector, can carry out their vital administrative role free of political interference.

The issue has already been specifically raised by governments, notably the Russian Federation in its contributions to the ITU's Council Working Group on International Internet-related Public Policy Issues (CWG-Internet).

- 16th Meeting of the CWG-Internet (23 September 2021)
    - *Contribution by the Russian Federation - Risk analysis of the existing Internet governance and operational model*
- 17th meeting of the CWG-Internet (19-20 January 2022)
    - *Contribution by the Russian Federation - Proposals to discuss the challenges and lack of operational activity organizations/operators of critical Internet infrastructure (first phase)*

The second contribution notes:

> *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.*
> *…*
> *[A] 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. 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.
…
The example of [the RIPE NCC] 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 [sic] 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).

While the CWG-Internet declined to discuss the issues raised, the contribution, in referencing current rather than hypothetical issues relating to national jurisdiction over the bodies responsible for core Internet functions, represented a significant escalation in the arguments of those who want to see a governmental, multilateral arrangement take over responsibility for such governance matters. As UN Member States progress towards the 20-year review of the World Summit on the Information Society (WSIS) in 2025, the commitment to a multistakeholder approach to Internet governance (as enshrined in the Tunis Agenda for the Information Society, published in 2005) will be a key issue for negotiation and debate.

It is clear that the application of sanctions is undermining global trust in the ability of multistakeholder organisations and structures to effectively manage core Internet functions across multiple jurisdictions, including the global Internet number registry system. We recognise that sanctions are a governmental tool, and the decision on how to apply sanctions is ultimately one for state authorities. Our hope is that by clearly identifying this detrimental effect, the governments responsible for applying sanctions (many of whom are strong supporters of the multistakeholder approach) will be open to working with the relevant stakeholders to minimise the impact of sanctions on these functions and the organisations responsible for them.