



20 October 2022
Oleksandr Fedienko
People's deputy of Ukraine
Member of the Committee of the Verkhovna Rada of Ukraine on matters of national security,
defense and intelligence

RE: Committee of the Verkhovna Rada of Ukraine on Digital Transformation Request for Dialogue on Protecting Ukrainian Internet Number Resources

Amsterdam, 20 October 2022

Dear People's Deputy Oleksandr Fedienko,

We would like to again extend our deep concern for the people of Ukraine and particularly those working to maintain stable Internet operations at this time. We also want to thank you for your letter dated 11 October 2022. This forms an excellent basis for us and the rest of the RIPE community to work together to resolve this urgent matter.


The RIPE NCC is aware of the concerns that Internet resources could be transferred away from their rightful holders during periods of war and distress. To this end, we have published an article (see appendix) that outlines some of the difficulties and provides an overview of what we are currently doing to mitigate the problem. The article also assesses some of the various options that have been proposed to further address it.

As the article makes clear, we share the goal of protecting resource holders in Ukraine during the war. As you acknowledge in your letter, the RIPE NCC must act within the limits of RIPE policy. With this in mind, we will present our analysis of the situation at the RIPE 85 Meeting during the RIPE NCC Services Working Group session at 14:30 UTC+2 on 26 October. On the same day, from 09:00-11:30 UTC+2, the Address Policy Working Group will meet to discuss matters of policy, and we suggest that this would be a good forum to raise these matters.

We think this is a good opportunity for us to discuss the issue with the RIPE community and with RIPE NCC members. We welcome your participation in these sessions as well as that of resource holders from Ukraine.

Finally, I want to restate our commitment to working together with all stakeholders to reach an outcome that will meet the needs of our members in Ukraine.

Sincerely,

DocuSigned by:

9A1BE60A20724D8...

Hans Petter Holen
Managing Director
RIPE NCC

Appendix: Protecting Resource Holders in Distressed Areas

 labs.ripe.net/author/athina/protecting-resource-holders-in-distressed-areas/



Since the war in Ukraine escalated, people have raised concerns about the risk of illegitimate registry update requests being submitted to the RIPE NCC. In this article, we explain what we have been doing to minimise this risk so far and look at some additional measures we could implement.

The concern

When we talk about ‘illegitimate requests’ in this context, we are mostly concerned with requests to update the registry that do not reflect the resource holder’s true intention, possibly submitted in response to threats or made under false pretenses.

Although these concerns are arising because of the war in Ukraine, they can be relevant to other countries affected by political disputes, international conflicts or war. In fact, there are countries in our region that have been in distress for many years or even decades. Since we serve a large region, any mechanism that seeks to address this matter should be provided in similar situations and not only in Ukraine.

What needs to be achieved

Before we look at how we can address this matter, it is important to be clear on what we want to achieve. Our commitment has always been to support local network operators in a neutral, impartial and transparent manner in line with RIPE policies. We want to prevent illegitimate updates to the registry while allowing legitimate updates to be processed.

Requests in doubt

As mentioned above, this concern is about registry update requests (such as transfer requests) with questionable legitimacy due to circumstances in the region. For example, if the request comes from an area with armed conflicts or that is in disarray, one may suspect the request was made under threat or under false pretenses.

When the RIPE NCC receives update requests, we perform due diligence checks to ensure their validity. These checks are described in our public documentation. For example, we check the authority of the person submitting the request, the authority of the persons signing the transfer agreement, the registration of the companies involved with the relevant authorities, and we may also check identity documents of either or both parties. For areas in distress, we apply stricter checks, such as reviewing the validity of documents submitted and some of the claims that accompany the request.

However, there is no way for us to check whether the person submitting the request or signing the agreement was under threat or misled at the time.

Having said that, based on our due diligence procedure, we explicitly reserve the right to check the validity of submitted documentation by requesting additional documentation or information from third parties if we have doubts about its correctness.

Understanding the concerns people have about the risk of illegitimate transfers, we assume that all requests coming from distressed areas are questionable. We therefore perform additional due diligence checks by default and we can potentially apply extra measures as well.

Accordingly, there are two basic questions we need to address:

- How can we identify an area as 'distressed'?
- What extra measures can we apply to requests coming from areas in distress?

Areas in 'distress'

When evaluating whether an area is in distress and if we should apply stricter due diligence checks, we want to be impartial and fair. Concepts like 'in distress', 'occupied' or 'disputed' can be interpreted differently and be subject to disagreement. It is also worth noting that the location of the resource holder can not be determined simply by reviewing entries in the RIPE Database.

To determine whether an area is in distress, rather than applying 'common sense' and attempting to assess the nature of a local situation ourselves, we would prefer to use an independent, publicly available source which provides a solid basis for these decisions. We are looking for neutral maps and sources of data for this and we welcome suggestions from the community.

Extra disclaimer for areas 'in distress'

While we are already doing additional checks for requests from areas in distress, we understand that the concern is primarily about requests that might look good on paper but were actually submitted in response to threats or on the basis of deception. As mentioned above, we have no way to be certain about the real intentions of the authorised person. However, from a legal point of view, any agreement or other binding act that takes place under such circumstances is null and void. It is possible for such a transaction to be nullified by a court of law at a later stage. The RIPE NCC can revert a transfer that was based on documents that were later nullified by a court of law. There has been at least one case in the past where a court declared that a transfer agreement was invalid and the transfer was reverted.

Therefore, we want to introduce an additional requirement that requests coming from areas in distress can only be accepted if accompanied by a disclaimer. This would specify that the transfer will be reverted if we receive evidence in the future that the relevant supporting documents have been nullified. This extra disclaimer will accompany the resources in case they are further transferred to a third party. This third party will also have to acknowledge that they are aware of the risk that the transfer could be reverted in the future, as if the initial update never happened.

We consider this approach to be the most appropriate, as it is lawful, in line with RIPE policies and our procedures, and adheres to our commitment to protect local networks.

Other possible solutions

Freeze all updates

One way to protect against illegitimate updates would be to reject all requests from distressed areas. But while this would ensure absolute protection against illegitimate updates, it could be disproportionate, since it would block any legitimate updates which could harm local networks.

This approach also exposes the RIPE NCC to damage claims and liability, especially since RIPE policy does not provide for such exceptional measures. For this reason, we would be very reluctant to apply this approach without a clear mandate from the RIPE community, ideally through a policy proposal.

Freeze button

Another approach could be to provide a 'freeze button' that allows registration information to be locked for a specific period of time (e.g. six months). This solution would give a sense of security to any resource holder foreseeing a threatening situation (in fact, such a solution could be implemented not just for members in distressed areas but for any member with similar concerns).

While this might seem like an easy solution on the surface, we cannot help but anticipate situations where this could be abused. For example, we can imagine cases where malicious employees want to prevent an upcoming transfer. Such a solution would also have some administrative challenges, because who is authorised to activate this freeze would need to be specified. Also, we wouldn't be able to adhere to such a requested freeze when companies are bankrupt, liquidated or in case of a legitimate merger and acquisition.

In any case, if the period of time for the lock is longer than a couple of days, we would again be very reluctant in implementing this solution without a policy proposal.

Review of requests by national governments

We have also seen a suggestion that the governments could verify requests for the duration of a conflict. This would probably be quite effective at minimising the risk of illegitimate transfers, and it would also spare us most of the risks in terms of exposure to liability or damages.

While this has obvious advantages, we must admit that this is not an option that we find attractive. Over the past decades, we have always sought to avoid taking any action that would undermine the self-governance model of the Internet, and to protect network operators from decisions based on political reasons. Such a change would set a significant precedent and could open the door to further government intervention in the future. Whatever mechanisms we develop will likely have to be implemented in all similar cases within our service region, and many of the countries that are in distress are also countries where governments have traditionally sought greater control over Internet operations.

Having said that, if the RIPE community supports this approach, we would only be able to implement it on the basis of a RIPE policy proposal.

A word about areas under dispute

Finally, and although not directly related to the topic of this article, we would like to explain our procedure regarding areas under dispute. We have highlighted in the past our commitment to facilitate the provision of services to network operators in these areas so that our services are not denied for political reasons. The RIPE NCC can neither recognise nor deny one state's authority over a region and our foremost concern is to ensure the accurate registration of Internet number resources.

Our publicly available [due diligence procedure](#) reflects these commitments and concerns. When a request comes from an area under dispute and we need proof that the parties involved indeed exist, we rely on proof of establishment issued by a natural authority that the parties send to us. If the signing party is located in an area claimed by two or more widely recognised states, the RIPE NCC may accept proof of establishment issued by whichever national authority the signing party chooses. If the legal person is located in an

area that is self-proclaimed as an independent state, the RIPE NCC may accept proof of establishment issued by the relevant authorities accompanied by further documentation (e.g. proof of identity of the authorised representative, articles of incorporation etc.)

Discussion at RIPE 85

At the upcoming RIPE Meeting we will be presenting on this topic in the RIPE NCC Services Working Group. We invite anyone to share any concerns about the way we are addressing this matter or opinions on the alternative solutions we have presented. Feedback is welcome in this session (26 October), on the working group mailing list (ncc-services-wg@ripe.net), or on the RIPE NCC Membership Discussion mailing list (members-discuss@ripe.net), or on the RIPE NCC Forum.