Internet Impact Brief

Impact of Ukraine's Requests to Block Russia's Access to the Internet

Natalie Campbell
Carl Gahnberg

18 March 2022
Version 1.0

Abstract

On 28 February Ukraine's Deputy Prime Minister asked the Internet Corporation for Assigned Names and Numbers (ICANN) to impose a number of sanctions *vis-a-vis* the Russian Federation. The request was for Russian country-code Top Level Domains (ccTLDs) .RU, .SU and .рф to be removed from the DNS root zone, to help revoke TLS certificates for those domains, and to shut down DNS root servers located in Russia.

The Deputy Prime Minister sent a similar request to the Réseaux IP Européens Network Coordination Centre (RIPE NCC). The request was to revoke its Russian members' right to use IPv4 and IPv6 addresses. ICANN and RIPE NCC rejected Ukraine's requests, noting the importance of their neutrality in geopolitics to ensure global communications are available to everyone.

This Internet Impact Brief shows how politically motivated actions to prevent people from accessing the global Internet would cause significant harm to the open, globally connected, secure and trustworthy Internet.

Methodology

The Internet owes its strength and success to a foundation of critical properties that, when combined, represent the Internet Way of Networking (IWN). This includes: an accessible Infrastructure with a common protocol, a layered architecture of interoperable building blocks, decentralised management and distributed routing, a common global identifier system, and a technology neutral, general-purpose network.

To assess whether the proposed actions have an impact on the Internet, this report will examine its impact on the IWN foundation the Internet needs to exist, and what it needs to thrive as an open, globally connected, secure and trustworthy resource.

Introduction

The Russian invasion of Ukraine on 22 February 2022 has drawn global criticism. Some 141 countries supported the UN General Assembly's call for Russia to "unconditional[ly] withdraw" its military forces from the territory. Many countries have imposed sanctions to demonstrate solidarity in opposition to the war. Measures have ranged from freezing assets of individuals, to disrupting the financial system, trade and other important sectors of the economy. To escalate pressure on Russia to change course, several governments, companies and institutions are proposing actions to try "disconnect" Russia from the global Internet.

On 28 February, Ukraine's Deputy Prime Minister wrote a letter to the CEO of the Internet Corporation for Assigned Names and Numbers (ICANN), asking ICANN to impose a number of sanctions *vis-a-vis* the Russian Federation. ICANN's primary role, through the Internet Assigned Numbers Authority (IANA) function, is to maintain the central repository of IP addresses, coordinate its global supply, and to manage the root zone registries of the Domain Name System (DNS). Specifically, the request was for Russian country-code Top Level Domains (ccTLDs) .RU, .SU and .рф to be removed from the DNS root zone, to help revoke TLS certificates for those domains, and to shut down DNS root servers located in Russia.

The Deputy Prime Minister also sent a similar request to the Réseaux IP Européens Network Coordination Centre (RIPE NCC), asking for the revocation of its Russian members right to use IPv4 and IPv6 addresses. RIPE NCC is one of five Regional Internet Registries that distributes Internet numbers resources on behalf of their respective stakeholder communities. They allocate blocks of IPv4 and IPv6 address space to Internet services providers and other organizations in need of address resources in their service region.

ICANN and RIPE NCC rejected the requests. Each noted the importance of their Internet governance roles to remain neutral to ensure access to global communications are not influenced by geopolitical conflicts.

What Ukraine's Requests Would Look Like

ICANN and RIPE NCC have both clearly explained that the requested actions are not subject to management decisions, but are governed by established community policies and procedures that prevent unilateral actions by the organization themselves. In ICANN's case, the request to disable root servers in Russia is out of scope, as the operations control resides with independent operators and the request to revoke TLS certificates would be the purview of various certificate authorities.

However, **for the purpose of illustrating the potential impact of Ukraine's request, this analysis will focus on the requested actions themselves, regardless of whom has authority to enact them.** This is especially important in light of ongoing calls from some governments to re-arrange the existing governance system to one in which many of the requested actions would be under multilateral control — and consequently subject to political decisions.

Requests Directed to ICANN

Ukraine's request to ICANN to revoke all Russian web domains, to invalidate associated TLS/SSL certificates, and to shut down DNS root servers operating in Russia requires some interpretation with regards to the requested actions. As more detailed information is not available, we summarize below our assumptions about their practical implementation, as well as the direct effects involved.

- **Revoke, ".RU", ."SU" and ".рф"**: While the request does not specify in detail the meaning of "revoke" in this context, our assumption is that it would either involve either a re-delegation of ownership of the domains to a new entity, or more likely the removal or de-delegation of the domains from the DNS Root Zone Database. In the latter case, the consequence would be that eventually queries for names in those domains would no longer resolve, making it impossible to reach a resource or service using its domain name.

- **Revoking TLS/SSL certificates for ".RU", ."SU" and ".рф" domains:** Transport Layer Security (TLS) certificates (sometimes referred to by an older name of "SSL certificates") are used to certify the ownership and authenticity of cryptographic credentials, which are used to set up an encrypted communication between two parties. Its most familiar use is for secure web browsing using HTTPS, in which a given website offers a public key that enables the user's browser to establish an encrypted connection to the website. In this context, the TLS certificate provides assurances that the public key to set up the encrypted communication is indeed issued by the domain owner, and not by a third-party that seek to impersonate the website or eavesdrop on the communications. Revoking TLS certificates can happen for various reasons, but in this scenario it would mean that other participants in the system would no longer recognize TLS certificates for the Russian domains, and in consequence not be able to establish a secure connection (for example, many browsers would block access to the website automatically). Another way that this request could be interpreted, namely that Russian-based certificate authorities (CAs) are withdrawn from the lists with trusted CAs that are used by e.g. web browsers, is out of scope for this paper — even though the impacts are very similar.

- **Shut down root servers in Russia:** The system of root servers, the authoritative name servers that serve the DNS root zone, is built around redundancy. In the IANA system there are 13 named authorities (none of which are located in Russia) in the delegation data for the root zone, meaning that they each make available a copy of the Root Zone Database. Thus, if one of them goes down, there are 12 other operators that have a copy of the Database and can fulfil the query function. Furthermore, while there are 13 named authoritative root servers, that does not mean there are only 13 physical servers. In fact, each of those root servers is comprised of networks of multiple servers (each with their own copy of the database) that handle the millions of DNS queries they receive. Some of these so called *anycast nodes* are hosted in Russia. Thus, the anycast root servers in Russia are consequently just local instances serving from their copy of the database, in order to respond more quickly to nearby devices. Shutting these root servers down would not hinder access to a root server, but would only add latency (delay) for some queries of the root zone from some Russian networks, as those queries would have to travel further on the network before being answered by a non-Russian root server. Besides, it is trivial for network operators to run a local instance of the root DNS database (i.e., RFC 8806), rendering this measure completely ineffective.

Requests Directed to RIPE NCC

Ukraine officials requested that RIPE NCC do their part to stop Russia from spreading propaganda by removing Russia's root servers, and withdraw the rights of its Russian members to use IPv4 and IPv6 addresses. The effect from shutting down root servers located in Russia was described earlier, but the request to revoke rights of using IPv4 and IPv6 addresses requires some further elaboration.

The role of RIPE NCC is to provide technical and administrative support in the distribution of IPv4 and IPv6 addresses on behalf of the IANA, and in accordance to policies set by its members in the RIPE community (of which its Russian members form part). This authoritative coordination is required to ensure that each network on the Internet has a unique set of IP addresses. Revoking the rights to IPv4 and IPv6 addresses does not imply that these Russian networks would no longer be able to send and receive traffic, as these address resources would not magically disappear from their equipment. It would however mean that RIPE NCC might stop providing services such as signing Route Objects or providing reverse DNS services which will have a delayed effect on the ability to route traffic or to use some services offered on the Internet. Furthermore, and as described in the analysis below, it may also result in two networks announcing the same IP addresses — which ultimately risks fragmentation at the most fundamental level in the Internet’s infrastructure.

How Ukraine's Requests Could Harm What the Internet Needs to Exist

The requests would significantly harm three of the five Critical Properties of the Internet Way of Networking.

Critical Properties of IWN	Impact
CP 1: An Accessible Infrastructure with a Common Protocol that is open and has low barriers to entry	**Requests to RIPE NCC:** When Registries cannot serve members from a given jurisdiction that community cannot grow its access to the Internet since they cannot get new resources, which undermines the accessibility of the global infrastructure.
CP 3: Decentralized Management and a Single Distributed Routing System which is scalable and agile	**Requests to RIPE NCC:** Network operators need to be able to rely on the stability of the registry to properly reflect who uses what addresses. If IP addresses get withdrawn from the registry they will continue to be used by the Russian network operators. As a result, network operators and other stakeholders on the Internet may see two parts of the Internet using the same numbering resources, which would cause routing failures and a high degree of confusion that may undermine the system as a whole.
CP 4: Common Global Identifiers which are unambiguous and universal	**Requests to ICANN:** If ICANN were to de-delegate Russian ccTLDs from the root zone, it would remove those domains from the shared set of identifiers that is the DNS, which means that resources linked to those domains would no longer be accessible using the DNS system. Workarounds that would follow would cause ambiguity and a fragmented view of the DNS namespace. **Requests to RIPE NCC:** If RIPE NCC were to revoke IPv4 and IPv6 registry services to members in Russia, it could prevent networks from having a consistent view of which identifiers are in use. The resulting ambiguity would undermine the trustworthiness of the registry, and fragment the global Internet.

How Ukraine's Requests Would Harm What the Internet Needs to Thrive

In addition to harming key parts of the Internet's foundation, the requests would significantly impact nine Enablers of an Open, Globally Connected, Secure and Trustworthy Internet.

Enablers of OGST	Impact
Easy and unrestricted access	**Requests to ICANN:** If ICANN were to de-delegate Russian ccTLDs, services that are uniquely named by names in the sanctioned top level domains would no longer be accessible. If those services have names in non sanctioned domains they may still be accessible, but with increased friction as users may not be aware of its availability under other domains (e.g. that a service blocked under ".ru" is still available under ".com"). **Requests to RIPE NCC:** When IP registration services are revoked there will be friction over time, and accessing the Internet or services may become more difficult.
Collaborative development, management, and governance	**Requests to ICANN and RIPE NCC:** Actions in both scenarios would undermine a system that is premised on trust in the allocation of scarce resources according to shared multistakeholder policies and the maintenance of a registry that reflects who is in fact legitimately using the addresses. Unilateral actions undermine established multistakeholder governance processes of the Internet's technical infrastructure.
Unrestricted reachability	**Requests to ICANN:** The de-delegation of Russian ccTLDs would make associated resources no longer available through the "RU", ."SU" and ".рф" domains. **Requests to RIPE NCC:** As described above, if an IP address block allocation gets withdrawn from the registry, the network operator that was using it might carry on using it. This could create a situation where some networks continue to recognize the Russian network operator's use of the addresses, while others do not. This would result in fragmentation whereby reachability is dependent on what networks recognize what addresses. There is no protocol for Internet-scale re-use of the same addresses by two unrelated and uncoordinated network operators, and no protocol for switching between two different sets of networks that do not mutually

	interoperate. So the effects of this network split would be difficult to mitigate.
Available capacity	**Requests to RIPE NCC:** When registries cannot serve members from a given jurisdiction, that community cannot get new resources, which would degrade the available capacity. However, as long as addresses already in use by the Russian networks are still recognized by the routing system it would not impede issues like latency and traffic volumes.
Data confidentiality of information, devices, and applications	**Requests to ICANN:** Revoking TLS certificates would mean that browsers could not establish a secure connection to websites that depend on the revoked certificates. While most browser would block access, users could still connect by overriding their browser setting. If this becomes a habit (and the UX allows for it) it will change the way that people will respond to phishing and make the Internet less safe.
Integrity of information, applications, and services	**Requests to RIPE NCC:** Reverse DNS and RPKI are both registry services that would be revoked. Depending on the effects, network operators, also outside Russia, may disable DNSSEC and or RPKI validation to keep services running. As a result, trust in the technical system designed to make the Internet more secure may deteriorate long term, not only in Russian networks.
Reliability, resilience, and availability	**Requests to ICANN:** De-delegating ccTLDs to remove them from the root zone would hinder reliability, resilience and availability of the network due to the downtime for domain name holders/networks. Even if they were to be delegated to a new steward/owner, that process could be lengthy and onerous. **Requests to RIPE NCC:** Ambiguity in the address registry leads to a less reliable Internet - Address blocks might be hijacked, and filters might not be appropriately applied, leading to growing inconsistency.
Accountability	**Requests to ICANN and RIPE NCC:** Internet governance institutions such as ICANN and RIPE NCC have long strived to remain neutral to distance Internet infrastructure administration from geopolitical influence and ensure global communications are fair and accessible to everyone. For either of them to accommodate the requests would significantly erode trust in the multistakeholder model and Internet governance policies the

	Internet has relied on to remain open, globally connected, secure and trustworthy. Further, Internet address registries provide mechanisms for the Network providers to keep each other accountable. The premise for this accountability mechanism is for the registry to be accountable.
Privacy	**Requests to ICANN:** Revoking TLS certificates would mean that browsers cannot establish a secure connection to Russian websites. Most browsers would block access to websites who don't have TLS certificates. However, users could override their automatic browser security functions to access Russian websites, which would pose a significant risk to privacy online.

Summary and Recommendations

As countries worldwide look for ways to support Ukraine in a time of crisis, we must resist calls to disconnect Russia from the Internet. While it is understandable that people are seeking ways to support victims of geopolitical conflict, we cannot achieve this by harming a critical lifeline for civilians.

Actions to politicize connectivity and management of the Internet's infrastructure — regardless of the reason — threaten the Internet and everyone's ability to use it as a resource for good. As this Internet Impact Brief has demonstrated, the recent requests from Ukraine officials to ICANN and RIPE NCC would significantly hinder critical elements the Internet needs to exist, and several of the features it needs to remain open, globally connected, secure and trustworthy.

Furthermore, it is important to note that even if the proposed actions may be reversible, the impact of politically motivated actions to cut people's access to the global Internet may not be. Once a precedent that undermines multistakeholder governance processes is set it legitimizes dangerous actions by regimes seeking to control Internet access in the future.

Ultimately, politicizing the management and operations of the Internet will splinter it along geographic and political lines.

The Internet is for everyone. To make sure it stays that way, we must support the independence and neutrality of the governance bodies and institutions responsible for its workings. Making an exception on the norms of the current governance system would set a dangerous precedent that would erode trust and could ultimately lead to the demise of a global communications resource and our ability to use it as a force for good.