Internet Impact Brief

How Refusing Russian Networks Will Impact the Internet

Natalie Campbell
Carl Gahnberg
18 March 2022
Version 1.0

Abstract

On 4 March, the Washington Post reported that Cogent Communications, a leading Internet backbone provider, would stop providing service to its Russian clients. In its role as a transit provider, charging other networks to carry traffic to the rest of the Internet, this action will result in one less path for international connectivity being available for Russian networks. However, as one of the largest transit providers in the world, the impact could be significant, as many of Cogent's Russian customers are also some of Russia's largest networks — including the state-owned telecom Rostelecom.

This action was later followed by another large transit provider Lumen (formerly CenturyLink) announcing a similar decision to cut ties with its Russian clients.

This brief uses the Internet Impact Assessment Toolkit (IIAT) to assess how actions to block networks from accessing the global Internet cause significant harm what the Internet needs to exist and thrive, and the ability of people to use it as a critical lifeline and a resource for good.

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 scenarios presented 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.

Context and Assumptions

Context

Cogent and Lumen both said their decisions to stop providing service to Russian clients were largely related to their ability to operate commercial operations in Russia in light of sanctions against Russia's financial system. However, both Cogent and Lumen also cited security as an additional consideration for stopping their operations. While these actions can be seen as extreme business decisions necessitated by an extreme situation, some commentators see these actions as political decisions in response to Russia's aggression against Ukraine.

As countries, institutions, and companies worldwide look for ways to support Ukraine in a time of crisis, we must avoid attempts to 'disconnect' Russia from the Internet. The Internet is for everyone, and making sure it stays that way means we have to support the neutrality of those responsible for its inner workings. We recently demonstrated how Ukraine's requests to block Russia's access to ccTLDs and registry services would undermine the neutrality of governance bodies and hinder their efforts to ensure the Internet remains open to all.

Cogent and Lumen have withdrawn their respective paths between Russian networks and the rest of the Internet. This Internet Impact Brief brief will examine the consequences of actions, which appear to be motivated by political considerations, on the open, globally connected, secure and trustworthy Internet. To this end, we will examine **additional scenarios** in which Internet networks take politically influenced actions to block others from access to the global Internet's infrastructure — either self-imposed or as a result of government mandates.

Assumptions

It is important to emphasize that the backdrop to this analysis is the case of network and service operators taking actions due to geopolitical conditions. That does not require the operators acting themselves in a political way. It might be, for instance, that a network operator does not wish to turn down a connection, but it believes it is required to do so because of uninsurable risk or due to government-imposed sanctions or any other reason that derives from overall political conditions.

The precise reasons for the operator's action, and whether it decides to take action on its own or due to government requirements, do not appear to affect the analysis. As such, we describe three potential scenarios and a set of associated assumptions that will underpin the impact analysis:

Scenario 1: "Pull the plug" — Networks cut direct peering or transit relations with other networks from a certain jurisdictional home or area of operations.

The actions taken by Cogent and Lumen are a species of this scenario. When direct relationships with Russian networks are cut, the Russian networks have fewer paths of interconnection to the rest of the Internet. At a practical level, this implies that the peering or transit network refuses traffic from the Russian network, or quite literally disconnects the hardware.

Scenario 2: "Erasing my spot on the map" — Networks along the routing path refuse routing announcements originating from certain networks due to their jurisdictional home or area of operations.

This action is a related yet distinct scenario in which networks on the Internet would filter out so-called "routing announcements" from Russian networks. Every connection to the Internet uses at least one Internet Protocol address to identify the connection end point. These addresses are clustered into blocks addressed by a "prefix" that specifies the size of the block. Blocks of addresses are assigned to network operators, each of which runs an "autonomous system", often abbreviated "AS". Each AS is identified by an "Autonomous System Number" or "ASN". Routing relationships are expressed on the Internet through the Border Gateway Protocol (BGP). BGP provides a way for AS "A" to announce to other ASes the ASNs that can be reached by directing traffic towards "A". These announcements may indicate direct connection ("A is connected to B") or may indicate indirect connection ("A is connected to B which is connected to C and D, and D is connected to E and F"). This information helps create a map for how to reach different parts of the Internet. By filtering out routing announcements originating from Russian networks with whom they have no direct connection, networks in the Internet core could effectively distort the map by omitting paths to those networks, and in an extreme case effectively prevent Russian networks from reaching parts of the Internet.[1]

Scenario 3: "I'll connect you to the Internet – except these networks"— Edge networks refuse routing announcements originating from certain networks due to their jurisdictional home or area of operations.

This action is identical to Scenario 2. The difference is that the action is taken by an edge network, like an Internet service provider or mobile operator, that (mostly) does not further propagate routing announcements itself. In this scenario, routes are filtered to restrict users of that edge network from sending or receiving traffic from a network on the Internet.

[1] Note that this type of filtering could happen at a more granular level than AS Number, e.g. by filtering on IP prefixes within a given AS.

How Politically Motivated Network Actions Impact What the Internet Needs to Exist

If networks start making connectivity decisions under the influence of geopolitics, this could harm two 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	**Scenario 2:** Politically motivated filtering of ASes would effectively deny targeted networks from being seen and addressed on the Internet, which undermines the accessibility of that part of the Internet.
CP 3: Decentralized Management and a Single Distributed Routing System which is scalable and agile	**Scenario 2:** The decentralized management of the Internet routing system works because all parties work towards establishing full mesh connectivity. Once that compact is violated, due to politically motivated filtering, trust in the Internet's ability to provide global connectivity will be undermined.

How Politically Motivated Network Actions Impact What the Internet Needs to Thrive

In addition to harming key parts of the Internet's foundation, politically-motivated network actions would significantly impact seven Enablers of an Open, Globally Connected, Secure and Trustworthy Internet.

Enablers of OGST	Impact
Easy and unrestricted access	**Scenario 1:** This action would lead to increased costs of access since there would be fewer available paths to the Internet. **Scenario 2:** This action would lead to increased costs of access, exacerbated by the fact that a network may need to make interconnection decisions based on their incomplete visibility in the routing table.

	While the impacts in these scenarios are the intent of the actions, placing barriers to entry such as higher cost lead to an Internet that is less open for ordinary users.
Unrestricted use and deployment of Internet technologies	**Scenario 1, 2 and 3:** A key characteristic of the Internet is that a service can use technologies that may be distributed across different networks (e.g. a website may use a login function or database operated by a third-party on a different network). To the extent that such technologies are located in the affected network, this could have implications for other services that rely on those resources. For instance, access to critical services might rely on access to an authorization system in the cloud. By restricting people's ability to use and deploy technologies related to the affected network, these scenarios contribute to an Internet that is less open for everyone.
Collaborative development, management, and governance	**Scenario 2:** This action undermines a routing system that is premised on collaboration and trust amongst networks. A fundamental compact of routing is the agreement to carry traffic and accept AS announcements, and to perform traffic management on technical and economical (self interested) optimizations — not political ones. Restricting the ability of networks to collaborate leads to an Internet that is less open.
Unrestricted reachability	**Scenario 1 and 2:** As long as the targeted network has a connection to another network that will accept its traffic, and unless all transit providers filter, the filtered AS still has a path to the Internet. In this case, reachability is restricted, but not prevented. **Scenario 3:** This scenario restricts the reachability of the filtering networks for the filtered ASes, and vice versa (The Russian network cannot reach my ISP, and I cannot reach the Russian network). While restricting reachability is in line with the goal of the sanction, it contributes to an Internet that is less globally connected for users worldwide.
Available capacity	**Scenario 1 and 2:** Actions in both scenarios restrict the number of available paths that the targeted network can use to reach other parts of the Internet. This will increase latency and decrease available bandwidth, thereby making that part of the Internet less globally-connected.
Reliability, resilience, and availability	**Scenario 1 and 2:** Actions in these scenarios limit the number of available paths that the affected network can use to reach other parts of the

	Internet. This will decrease reliability, resiliency and availability of connectivity of that network, as well as of resources located within the affected network. As a result, this would make the Internet less resilient. **Scenario 3:** This action could affect the availability of other services in the event that key resources are located in the affected network. That is, a user in the edge network applying the filter would not be able to reach resources in the affected network.
Accountability	**Scenario 1 and 2:** Politically motivated actions are always subjective. Therefore, actions to restrict networks from access to the global Internet could be perceived to be arbitrary, unfair or to discriminate against users impacted by the decisions. This is especially a risk for users who aren't the intended target of the action to restrict access to the global Internet. This could also be true in Scenario 3, provided that the user does not have access to a network that does not apply the filter. Politically motivated actions to restrict networks undermines accountability, contributing to an Internet that is less trustworthy for users worldwide.

Summary and Recommendations

In these turbulent times of plague and conflict, it is important to remember that the Internet is an incredible force for good. The pandemic has shown its potential to facilitate global efforts to find new ways of living, working and learning, and solving some of our toughest problems yet. Likewise, many civilians under oppressive regimes and victims of conflict rely on access to the global Internet for reliable information, and as a lifeline to keep themselves safe from harm.

We cannot afford to make the Internet a casualty of geopolitics. This Internet Impact Brief has demonstrated how restricting networks from the global Internet causes significant harm to key elements the Internet needs to exist and thrive.

While geopolitical conflicts may come to an end, we cannot assume that the impact of the politically motivated actions to prevent people from accessing the Internet will be reversed.

Some network collaboration may resume, but there is a significant risk that politically motivated actions to disconnect users from the global Internet set a precedent and trend that play into the hands of regimes seeking to censor, block and control Internet access.

Companies that own and operate parts of the Internet's infrastructure play an important role in the Internet's ecosystem. We each have a responsibility to protect the Internet and the billions of people worldwide who rely on it as a critical resource for good. We must all work to make sure the Internet is open, globally connected, secure and trustworthy for everyone.