# Internet Way of Networking Use Case

## Interconnection and Routing

September 2020

## How regulatory policy on routing and interconnection, and reduced autonomy of operators impact the Internet Way of Networking

In a number of countries, there is a trend towards regulatory control of how Internet operators manage network interconnection and routing. Interconnection and routing choices are critical decisions taken for local and operational reasons to ensure network resilience and optimal traffic flows. In this use case, we will look at different facets of this trend in three countries – China, Russia, and the United States – where decreasing autonomy of networks on interconnection and routing undermine two critical properties of the Internet Way of Networking:

- An Open and Accessible Infrastructure with a Common Protocol
- Decentralized Management and Distributed Routing

The closer the Internet gets to operating in a way that matches these critical properties, the more open and agile it is for future innovation and the broader benefits of collaboration, resiliency, global reach, and economic growth. The further the Internet is from the Internet Way of Networking, the less it resembles the global Internet with all the benefits that would otherwise bring.

Many critiques of China's small number of network choke points, or Russia's "Sovereign Internet" law, have drawn attention to their political, social, or economic impacts. In August 2020, the U.S. Administration's proposed "Clean Network program" also raised concerns from the technical community about its misalignment with the program's intended goals and how damaging it could be for the open architecture that underpins the Internet Way of Networking. This use case uses the critical properties of the Internet Way of Networking as an additional lens to look at how these developments affect the Internet's infrastructure and asks how these laws or policies will impact the Internet if they continue or spread.

China's distorted, hierarchical network topology severely impacts its global reach and sets limits to collaborative 'internetworking'. Russia's routinized reporting, and the ongoing trend of centralizing control, drastically reduce the autonomy and agility of its Internet service providers, making its networks less resilient at precisely the moment they need to be more resilient. Some of the requirements of the U.S. Clean Network program hinder the interconnection among the networks, the growth of the Internet communication infrastructure, and, as the consequence, its services and opportunities.

While China's network topology only somewhat resembles the Internet in its critical properties, Russia's networks are still recognizably the Internet. However, if new powers to centralize decision-making and routing are used to

reshape Russia's networks to match national borders, the country risks no longer being part of the global Internet, potentially matching China's model of a national "intra-net". Limitations imposed on interconnections as suggested by the Clean Network program will increase the risk of fragmentation of the Internet into a "splinternet".

## Interconnection and Routing in Russia

The Internet in Russia is quite vibrant, with plenty of regional and international interconnections and over five thousand networks operating in the country.[1] About one third of these are local Internet registries, meaning they get address space directly from RIPE NCC, the regional Internet registry in Europe. Because the address space is not assigned to these networks by their upstream provider, they can switch transit providers more easily and in general have higher autonomy over their connectivity choices than similarly sized networks in China.

However, the 2019 "Sovereign Internet" law,[2] which aims to address perceived threats to the national network from abroad, gives regulators the ability to cut off the international connectivity or services (e.g. cloud services) that the Russian Internet depends on. Network operators will have to provide the regulator, Roskomnadzor,[3] with network diagrams, technical characteristics of the communication facilities where "*technical means of countering threats*" (TMCT) will be installed, information on communication channels (number, physical properties, throughput, average, and maximum load), and the locations of planned installations of TMCT.

Not only will operators now be required to install Roskomnadzor's TMCT on their systems and routinely provide detailed routing information to the regulator, operators will also have to give Roskomnadzor remote access to the TMCT. If the regulator decides there is an immediate security threat to the public communications network, it can use the TMCT to impose changes on traffic routing, close and reserve communication lines and channels, directly contact users and change the configuration of communications. In effect, when Roskomnadzor (acting with the Ministry of Communications and the Federal Security Service – FSB) declare a communications emergency, the regulator can directly control the routing and other decisions of operators.

Both the routine requirements and emergency capabilities foreseen by the 2019 law will inevitably alter interconnection and routing in Russia and undermine critical properties of the Internet Way of Networking.

## Which critical properties are affected by these developments?

### Critical Property 1 - An open and accessible infrastructure with a common protocol

The "permissionless" model of the lowest possible technical barrier to entry is made possible when there are no unnecessary barriers to connect to the Internet. However, the Sovereign Internet law requires network operators and Internet exchange points (IXPs) to provide detailed routing and other operational and business-confidential information to the regulator. This requirement goes far beyond typical requirements for businesses to be licensed, as it means sharing detailed technical information on an ongoing basis. It appears to require a cumbersome administrative process for connecting to the Internet and optimizing connectivity patterns, day to day. The requested data is often very dynamic, consistently changing in response to local conditions – for example changes in routing to use a more optimal path, link outages, or redirecting data flows across the backup links. The mismatch between this bureaucratic regime and the nature of such information creates a barrier to an open and accessible infrastructure and may also interfere with operational decision-making about interconnection, undermining Critical Property 3.

1 https://stat.ripe.net/RU

2 "On Amendments to the Federal Law 'On Communications' and the Federal Law 'On Information, Information Technologies and Information Protection'", 22 April 2019, http://publication.pravo.gov.ru/Document/Text/0001201905010025

3 The Federal Service for Supervision of Communications, Information Technology, and Mass Media

### Critical Property 3 - Decentralized management and distributed routing

This critical property of the Internet Way of Networking means that each network can make independent decisions on how to route traffic to its neighbours, based on its own needs, business model, and local requirements. Crucially, there is no centralized control or coordination, but rather each operator makes its own decisions and collaborates freely with those it chooses.

The requirement described above for operators to inform the regulator about routing changes may also interfere with the operational ability to optimize routing day to day or even moment to moment. Any changes in routing that may be necessitated by operational or business reasons now involve sharing potentially sensitive information with the regulator. It is unclear if this measure will apply to downstream routing changes that affect the communication path, a common occurrence in network operations. For example, a Russian Internet service provider (ISP) may contract with another network to provide transit – essentially connectivity to the greater Internet – for its traffic. If that provider changes its routing, algorithmic decision-making could choose a path that brings traffic outside of the country – a perceived threat of making it vulnerable for interception or blocking. These kinds of operational decisions are constantly taken in real-time – and often by contracted partners – to deliver responsive and resilient routing, but the new law seems to require a notification procedure that is out of step with how traffic is routed operationally.

The 2019 law further undermines decentralized management of networks by allowing the regulator to alter the operational setup of a network remotely. Besides creating a single point of failure and operational uncertainty, it may have unforeseen consequences, including outages and security breaches.

During an incident when the regulator believes there is a threat from abroad, operators may not be able to control their own routing. Some interconnection decisions will be restricted and others required, based on centrally made decisions that remove the autonomy and ability of operators to reflect local conditions and operational and business needs.

Further, centralized routing decisions in an emergency scenario are likely to be slower and less responsive or agile than in normal times because the regulator will need to carry out complex modelling using data from multiple sources – some of it inadequate or out of date – to make decisions for many different operators. This will almost certainly yield a slower and potentially inadequate reaction compared to one where each operator acts independently based on its own real-time understanding of network conditions. Far from dealing effectively with an external threat to security, stability, and integrity of public communications systems, this measure seems destined to reduce resilience, increase response times, and reduce quality of response.

Overall, the 2019 law seriously undermines decentralized network management and the distributed nature of Internet traffic routing, both in routine times and in potential emergencies. The result will be a considerable decrease in the network's agility and resilience, an attack on the autonomy and expertise of operators, and a significant threat to the collaboration, optimized connectivity and global reach that Russia's Internet operators and users rely on.

## Interconnection and Routing in China

Three operators, China Telecom, China Unicom, and China Mobile are the leading Internet service providers in the country, with the most comprehensive national infrastructure. They serve about 70% of home broadband Internet users in China and provide much of the backbone network used by smaller access providers. The three companies also control international connectivity, running the gateways in Beijing, Shanghai, and Guangzhou that funnel all Internet traffic in and out of China. Aside from their monopoly over international gateways, the dominance of a national market by three incumbents is not unique to China. However, the interconnection regime among these companies, and between them and other Chinese access providers, creates an unusually hierarchical network topology that undermines decentralized management and distributed routing.

In much of the world, large operators predominantly use settlement-free network peering arrangements – agreements where no money changes hands as both networks exchange similar amounts of traffic with one another – rather than paid interconnection to manage traffic flows among themselves. In China, however, settlement fees for interconnection are the norm. Until July 1, 2020, China Mobile – with a slightly smaller public Internet network than the other two incumbents – paid significant fees to China Unicom and China Telecom to deliver its traffic. Now, China's Ministry of Industry and Information Technology has ordered an end to fee-paying between the top firms and ordered all three to cut their interconnection fees to two smaller network operators (China Broadcast Network and CITIC ASP) by at least 30%. This brings China's peering relationships between networks closer to globally accepted peering practices, but it also highlights the central role the state plays in planning the interconnection landscape and defining its pricing models.

China Telecom, China Unicom, and China Mobile have sole control over China's national Internet backbone, and other access providers must buy access from them. Further, the total choke points that these three companies hold on interconnection with all networks outside of China severely limits the access of China's providers and Internet users to the global Internet. The extremely hierarchical topology – or network layout – of China's networks, and the tight control of a tiny number of centrally controlled international gateways, mean the country does not experience or interact with the global Internet, but only a subset of it. The content inspection and filtering carried out by the gateways also has the effect of throttling international traffic, further limiting interaction with the global Internet. China's "internet" is not connected to the Internet in a meaningful way, as its centralized and rigidly-controlled networks undermine the critical properties of the Internet Way of Networking.

## Which Internet properties are affected by these arrangements?

### Critical Property 1 - An open and accessible infrastructure with a common protocol

The only essential condition for a network or individual node to access the Internet is to use its common protocols, including TCP/IP. This "permissionless" model of the lowest possible technical barrier to entry is the basis for the Internet's rapid growth and global reach.

China's hierarchical and costly routing and interconnection model, coupled with a complex licensing regime for networks to operate and connect to the Internet, imposes barriers so significant that they are an impediment to access. Even with recent moves to reduce high interconnection fees, the ability of other providers to build their own independent networks is very limited because of the control by the incumbents of the national backbone. The centralized operational control of the national backbone presents such a closed system that China's smaller providers do not have much choice on how to interconnect and optimize their data flows.

As a result, the Internet infrastructure of China is not able to integrate in the greater, global Internet. The centralized choke points of the three incumbents over all international access means that no other network is able to access the global Internet independently or directly. Networks cannot quickly respond to changing traffic and economic conditions and customer demand. This results in sub-optimal network structure, high pricing, and low resilience.

On the Internet, infrastructure growth happens organically, but in China it is subject to strict rules and conditions imposed by the government to centralize control. This inability of networks to offer global reach lowers the value of the Internet overall for users, as they are barred from accessing all the global Internet has to offer. The network qualities of Critical Property 1 – openness and low barriers to entry - are greatly reduced, and so the benefits they would bring – interoperability and infrastructure growth – are not fully available to Internet users in China.

### Critical Property 3 - Decentralized management and distributed routing

The Internet is a network of networks, with no centralized control or coordination. Operators' ability to make independent decisions about how to route traffic allows each part to quickly adapt to operational requirements and user needs.

Routing in China operates in a way that is very far from this ideal. The hierarchical network structure with the incumbents running the national backbone and acting as choke points for international access mean many fewer options for interconnection. As there appears to be little or no Internet traffic-peering in China, interconnection always involves settlement fees among a small number of incumbents.

Another unusual practice brought about by the small number of powerful incumbents is that few networks own their own blocks of Internet Protocol addresses, and when they do, the ownership of the IP block is transferred to the upstream provider who instead announces and controls the traffic routes the smaller network will use. This means that smaller networks lack number portability – if they switch between the incumbents, they lose their IP numbers – and so they are essentially locked in.

The result of such a hierarchical network topology, where most routing decisions are taken by upstream providers, is that that most networks have little or no control of their routing policy. They cannot make real-time operational decisions on traffic engineering and can only use the default routes provided by the incumbents. This causes operational inefficiencies and poorer quality of service for users, as routing decisions are made at a centralized level. The lack of agility and autonomy – alongside the already limited routing paths available both nationally and internationally from the incumbents – means there is less resilience.

China's operators must work with centralized management and concentrated routing, the very opposite of the properties that make the Internet agile, resilient, and scalable. As a result, they cannot optimize connectivity, choose network partners to freely collaborate with, provide truly global reach to users, or, it appears, provide optimal quality of service.

## The U.S. Clean Network Program

On August 5, 2020 the U.S. Administration announced a so-called "Clean Network program" aimed at mitigating threats to "America's critical telecommunications and technology infrastructure" from "malign actors, such as the Chinese Communist Party (CCP)"[4].

The five new lines of effort for the Clean Network tackle various facets of the Internet ecosystem, from physical infrastructure (cables), network interconnections, to cloud storage and applications.

While the full scope of the program was yet to be released at the time of publication of this Use Case, early details made it obvious how it would affect several properties of the Internet Way of Networking. This Use Case will analyze the Clean Carrier requirement "to ensure untrusted People's Republic of China (PRC) carriers are not connected with U.S. telecommunications networks. Such companies pose a danger to U.S. national security and should not provide international telecommunications services to and from the United States."

## Which Internet properties are affected by these arrangements?

### Critical Property 1 - An open and accessible infrastructure with a common protocol

Measures to mitigate threats to security and privacy of data in transit can result in restricting interconnection with Chinese carriers, effectively prohibiting direct interconnection with China, since only these carriers provide

4 Announcing the Expansion of the Clean Network to Safeguard America's Assets, https://www.state.gov/announcing-the-expansion-of-the-clean-network-to-safeguard-americas-assets/

international connectivity of the Chinese internet. As Ted Hardie said in his reaction to the proposed measures, "interconnection of different networks is the physical underpinning on which the Internet, with all of its services and opportunities, is built. By hindering that interconnection, this initiative strikes at the heart of the Internet as an enterprise. It also puts it at risk in ways which will have a number of unintended and deleterious effects"[5].

As with other cases where interconnections are dictated by a centralized policy and not based on the needs of a network operator and its customers, this has a high potential of resulting in less efficient infrastructure. Because direct interconnection between the U.S. and Chinese networks is restricted, traffic between the U.S. and Chinese nodes will have to take a sub-optimal path or make a detour, negatively impacting performance and resilience of the Internet.

### Critical Property 3 - Decentralized management and distributed routing

From the Internet routing perspective, the proposed restriction does not achieve the announced objective. If the data path is between a node in the U.S. and China, it is inevitable that it will be handled by a PRC carrier, unless the intention is to cut such paths off altogether. Instead, it will take a less optimal route involving other networks. This will result in higher latency and lower resilience without addressing the perceived threat at the ends.

If the intention is to avoid PRC carriers that may pass traffic not destined or originated in China, as in the case of a routing incident in 2010[6], the proposed measures still do not mitigate the threat. Due to the nature of the Internet routing system, such incidents do not require a direct interconnection with a PRC carrier and a U.S. network. For example, a route leak caused by a Swiss network in 2019 unintentionally sent traffic of other networks through China Telecom[7]. An ultimate, albeit absurd, solution to this problem would be to prohibit connectivity with the PRC carriers for all other networks on the Internet. However, other countries are unlikely to agree to this solution, as it would also limit their own ability to connect with China. Attempting to force whole countries off the Internet is just a different form of attack on the critical properties of the Internet. A real solution to the to challenges Clean Network tries to address lies not in controlling the interconnections, but ensuring that the Internet routing protocol, BGP, operates in a secure manner. One way to accomplish this is by implementing MANRS' recommended actions to promote routing security and resiliency[8].

Although the Clean Network program does not touch on routing, a question arises of how U.S. networks should handle routing announcements originated by the PRC carriers? The only sensible answer to this is to handle such announcements in line with the BGP standard and globally accepted routing security practices, such as validating the correctness of routing announcements using RPKI (Resource Public Key Infrastructure, - a system that allows for authentication of route announcements). Any artificially created routing policy imposed on network operators will have a negative impact on resilience, stability and the global reach of the Internet as a whole.

## Conclusion

The evolution of interconnection and routing as described by the trends in this Use Case is far from the ideal expressed in the Internet Way of Networking. As a result, many of the potential benefits – especially collaboration, global reach, and resiliency – are not maximized.

China's networking model does not permit the critical properties that drive so much of the Internet's value. While the scale of China's internal market means Internet users there can afford to forego the value of the global Internet,

5 Thoughts on the Clean Network program, https://medium.com/@ted.ietf/thoughts-on-the-clean-network-program-5f1c43764152

6 China Hijacks 15% Of Internet Traffic? More Like .015%, https://www.forbes.com/sites/andygreenberg/2010/11/19/china-hijacks-15-of-internet-traffic-more-like-015/

7 You won't guess where European mobile data was rerouted for two hours. Oh. You can. Yes, it was China Telecom, https://www.theregister.com/2019/06/10/bgp_route_hijack_china_telecom/

8 Mutually Agreed Norms on Routing Security, https://www.manrs.org/

if other countries adopt this model, they will lose out on countless opportunities for collaboration, connectivity, and the economic growth they drive.

Russia's move to centralize control of routing and formalize an "off-switch" for connection to the global Internet violates two critical properties of the Internet Way of Networking and reduces resilience in moments of potential crisis. If this approach were to spread elsewhere, the ability of the Internet to bring the broader benefits of collaboration, global reach, and economic growth to other countries would be severely threatened.

The measures announced by the Clean Network program by the U.S. Administration will negatively affect the interconnection infrastructure and traffic flows, resulting in decreased performance, resilience and potentially lower security for global users.