MANOHAR PARRIKAR INSTITUTE FOR DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

MP-IDSA
Issue Brief

Russia–Ukraine Conflict and Geopolitics of Data Routing

Krutika Patil

April 29, 2022

Summary

The Russia–Ukraine conflict, as well as Russia's 2014 annexation of Crimea, draw light on the geopolitics of data routing and the usage of the Border Gateway Protocol (BGP) as a tool of control. BGP is used by states to monitor and ensure censorship, block users and websites, carry out cyberattacks on other internet infrastructures, and hijack traffic from other networks. Russia created a sovereign internet network named RuNet, out of concerns that the West can constrict its access to global internet and to ostensibly protect its citizens from alleged disinformation campaigns and cyberattacks. Russia, though, has not been fully successful in achieving the objectives which led it to create the separate network.

Introduction

Russia's military operations in Ukraine brings to the foreground the geopolitics of data routing and the manner in which states use data routing in contested areas to assert their power. In the aftermath of the 2014 Russo-Ukrainian conflict, Russia gained control over the Crimean internet network, as well as that of the Donbas region. Through data protection laws and various other measures, Russia gradually created a Sovereign Internet/RuNet that gave it complete control of all Internet Transit Points in that region through which data packets flow in the network.[1] Even before Russian troops set foot in Donbas in the current conflict, Russia had complete control over the region's internet network.[2]

Internet Architecture and Data Routing

The shaping of cyberspace by both Russia and Ukraine is based on the technical principles of data routing. As per the International Telecommunication Union (ITU), the Internet is "a collection of interconnected networks using the Internet Protocol which allows them to function as a single, large virtual network".[3]

As shown in Figure 1, these interconnected networks are called Autonomous Systems (ASes). An Autonomous System (AS) itself is a network that manages the internal routing of data, distributes Internet Protocol (IP) addresses, and sets standards for access policies.[4] Data or Internet routing is the assignment of a path for the data package through which this package reaches its destination.[5] Currently, data routing happens through a routing protocol called Border Gateway Protocol (BGP), which is used in inter-domain routing for ASes. A Regional Internet Registry (RIR) allocates Autonomous System Numbers (ASN) to its ASes and IP addresses to the users within the ASes. An AS establishes a BGP exchange-of-data session with other ASes. These BGP sessions are Transmission Control Protocol (TCP) sessions

[1] Justin Sherman, **"Reassessing RuNet: Russian Internet Isolation and Implications for Russian Cyber Behavior"**, Atlantic Council, 12 July 2021.

[2] Holly Ellyatt, **"Battle for Donbas: 3 Reasons Why Russia is Shifting Its War Machine to East Ukraine"**, *CNBC*, 19 April 2022.

[3] **"A Handbook on Internet Protocol (IP)-Based Networks and Related Topics and Issues"**, *International Telecommunication Union*, 2005.

[4] Frédérick Douzet et al., **"Measuring the Fragmentation of the Internet: The Case of the Border Gateway Protocol (BGP) During the Ukrainian Crisis"**, 12th International Conference on Cyber Conflict (CyCon), Vol. 1300, IEEE, 2020.

[5] **"Data Routing"**, IBM, 5 April 2022.

between two routers connecting different ASes. TCP is essential to manage and keep the connections open.[6]

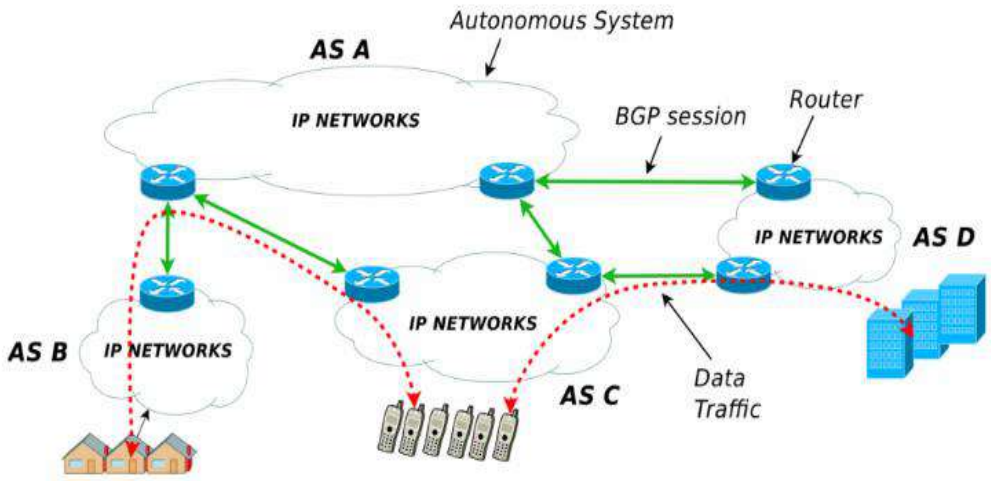

Figure 1. Internet Architecture with ASes and BGP

Source: **"A BGP Guide for the non-Network Engineer"**, Catchpoint, 7 November 2019.

Geopolitical Nature of ASes and BGP

Autonomous Systems are Internet Service Providers that can be controlled by governments, universities, or companies. Each AS has an administrator that communicates and agrees to a path followed by data packets to other ASes which is made possible through a BGP. As of 5 April 2022, 1,90,928 active ASes are constituting the Internet, as per the Regional Internet Registries Statistics.[7] These ASes have geographical limitations and need common infrastructure like cables to be operational. Also, an AS might have BGP agreements with multiple ASes but not necessarily with all ASes on the Internet. Hence, these agreements need human intervention that might be of political, commercial, or geographical nature. Although these agreements are generally confidential, the BGP needs ASes to communicate with each other for coordinated routing which is done through constantly releasing connectivity update messages. Therefore, through these updates, the cyberspace around these ASes can be mapped and assessed.

In the initial stages of the growth of the internet, the protocol for routing followed a more decentralised structure. Any system on the network was a possible gateway. However, as the networks became more complex, there was a visible hierarchy

[6] Tom Scholl, **"Internet Routing and Traffic Engineering"**, Amazon Web Services, 15 December 2014.

[7] **"Regional Internet Registries Statistics"**, RIR Delegations & RIPE NCC Allocations.

between paths taken by the data packets and some transit points became more important than others based on commercial, political, and geographical reasons.[8] Geopolitical reasons can impact the number of gateways a region has. For example, a remote island like Tonga is connected to the world only through one submarine cable via Fiji, hence, limiting its number of gateway entries severely.[9] China's Great Firewall[10], Iran's Halal Internet[11], and Russia's Sovereign Internet[12] are all based on the efforts of these states to better control data and content flow through a combination of techniques including IP blocking, DNS tampering and hijacking, and deep packet inspection and keyword filtering.

The BGP was created in 1989 for the regulation of data gateways or transits between ASes. The ASes receive directions on which path to take to reach the specified IP address. These directions are based on routing policies of BGP rules and the path preference set by an AS administrator. The BGP is controversial in the sense that it was formed from a utilitarian perspective without keeping security in mind and hence, can be exploited for traffic hijacking (re-routing of traffic through malicious transit points), obfuscation of cyberattacks, censorship, internet shutdowns, and cyber espionage.[13]

Who governs the internet?

The absence of a central organisation to oversee internet operations does not imply that everyone can have unrestricted access. For example, IP addresses and hostnames are finite and are bound by technical and geographical restrictions. The delegation of hostnames and IP addresses was controlled by the United States (US) until 2009, when the US government gave autonomy to ICANN to operate independently. The US Department of Commerce still played a role in reviewing the operations of ICANN till 2016. Another entity called the Internet Engineering Task Force (IETF) consists of experts that develop and approve protocols needed for Internet functioning and is considered to be free of political interference, unlike ICANN. Nonetheless, ICANN does not have the authority to debar any actor from the Internet.

---

[8] Kevin Limonier et al., **"Mapping the Routes of the Internet for Geopolitics: The Case of Eastern Ukraine"**, *First Monday*, 19 April 2021.

[9] Krutika Patil, **"Tonga Calamity: Impact of Natural Disasters on Submarine Cables"**, MP-IDSA Comment, 1 February 2022.

[10] **"The Great Firewall of China"**, *Bloomberg News*, 6 November 2018.

[11] **"Iran Creates "Halal Internet" to Control Online Information"**, *Reporters Without Border*, 6 September 2016.

[12] Alena Epifanova, **"Deciphering Russia's "Sovereign Internet law": Tightening Control and Accelerating the Splinternet"**, German Council on Foreign Relations, 16 January 2020.

[13] Frédérick Douzet et al., no. 4.

Amidst the Russia–Ukraine conflict, the Ukraine Government sent a request to ICANN's Government Advisory Committee for revoking the Russian Internet country code '.ru' and its Cyrillic equivalence but this request was rejected. This rejection notwithstanding, it is within the capabilities of ICANN and the Europe and Central Asia's Regional Internet Registry to take back all IP addresses assigned to Russia, essentially causing Russian websites to disappear from the Internet.[14]

Russia–Ukraine Internet Infrastructure

The connections that bind Russia–Ukraine internet networks are some of the most complex in the world, involving thousands of small ASes which have evolved based on 30 years of shared historical dependencies. During the time of the USSR, the emerging network in the region was isolated as the the global internet had not formed fully and was exceptionally centralised with hardly any gateway connections with the rest of the world. When the USSR disintegrated, due to the paucity of bandwidth, there was an urgent need to have more ASes for connectivity across the region. This led to a disorganised proliferation of small ASes with not much governmental supervision leading to the unusual complexity of the network. The internet grew faster than the Russian and Ukrainian governments' response to tame these ASes, causing much anxiety. Their inability to control the internet infrastructure due to the never-ending demand for more connections and access led the two countries to aggressively shape the routes of data circulation within their respective nations, especially Russia with its 'Sovereign Internet' initiative.[15]

In December 2019, Russia successfully conducted a test of disconnecting its network from the global internet as an attempt to 'test its cyber defences'. This test was based on the Sovereign Internet/RuNet law passed by the Russian Government in November 2019.[16] The law is implemented and monitored by Roskomnadzor, a Russian federal communications agency. Under the law, it is mandatory to install certain tracking software and hardware at all internet gateway points across Russia. The tracking data is then sent to a 'central monitoring facility' that has the power and authority to block the flow of data it deems a threat to Russia's sovereignty. The law also lets Russia isolate RuNet from the Global Internet Infrastructure/ World Wide Web in case it anticipates a cyberattack from its adversaries.[17] Using a technical process called 'Deep Packet Inspection (DPI)'[18], the central monitoring facility will

[14] Brian Fung, **"Ukraine's Request to Cut Off Russia from the Global Internet Has Been Rejected"**, *CNN*, 3 March 2022.

[15] Kevin Limonier et al., no. 8.

[16] Frédérick Douzet et al., no. 4.

[17] Justin Sherman, no. 1.

[18] Chris Brook, **"What is Deep Packet Inspection? How It Works, Use Cases for DPI, and More"**, *Data Guardian*, 5 December 2018.

analyse the internet traffic while blocking or redirecting 'problematic' data packets instantaneously.

The Russian government has stated that the legislation is in response to the US's 2018 National Cybersecurity strategy that aims to 'build a more lethal joint force' and 'compete and deter in cyberspace'.[19] While Russian analysts justify their country's concern vis-à-vis US big tech companies' influence, the flipside is that the Russian government now has complete control over what its citizens consume online.[20] Also, Russian fear of the US cutting it out from the global internet is not in-sync with her accusation of the US using its big tech companies' platforms to influence Russian citizens.[21] This is because it would have been in American interest to keep Russians connected to the global Internet to influence them. Russia's Sovereign Internet law is based on politics surrounding data routing which has led to further fragmentation of the Internet in the region.

On the Ukrainian side, its Internet architecture is split between the two global powers—the US, with a few European ASes and Russia. It is connected to Russia through 95 ASes (comprising Rostelecom, Rascom, and Transtelecom) and to the US via 22 ASes, mainly through the Hurricane Electric AS. Ukraine's connections with Russia have fallen sharply since the 2014 Russo-Ukrainian conflict. From 2019 onwards, the US has increased its AS connections with Ukraine mainly due to Russia's attempts to control the data flow in Eastern Ukraine, especially in the Donbas region.[22]

Russian Virtual Control in Crimea and Donbas

In the 2014 Russo-Ukrainian conflict, the regions of Crimea and Donbas, situated broadly on the eastern and southern sides of Ukraine, were vociferously fought over by Russia and Ukraine (Figure 2). Following this, Crimea came under Russian control and the territories of Donetsk and Luhansk in Donbas came under the authority of Russian-backed separatist groups. Russia also has control over the region's water and energy supply, internet access, and crucial infrastructure. By 2018, Russia had

[19] **"Summary: Cyber Strategy 2018"**, *US Department of Defense*, 18 September 2018.

[20] Robert Coalson, **"Explainer: Russia Takes a Big Step Toward the 'Internyet'"**, *RadioLiberty*, 1 November 2019; Glenn Diesen, **"As US Social Media Giants Censor Free Speech Online, Russia & China Lead The Charge To Break Free From American Control Of The Web"**, *RT News*, 9 July 2021.

[21] Ina Fried, **"Groups Warn Biden Administration on Cutting Off Russian Internet"**, *Axios*, 10 March 2022.

[22] Frédérick Douzet et al., no. 4.

succeeded in the complete integration of Crimean and Donbas' network with the Russian network.[23]

Figure 2. Location of Crimea and Donbas

Source: **"Ukraine Says Russia Wants to Destroy Donbas as Mariupol Prepares Final Defence"**, *The Hindu*, 18 April 2022.

Crimea

Before Russia's successful integration of Crimea's economic, bureaucratic, infrastructural, and informational apparatus, Crimea's network adhered to Ukrainian rules and regulations. Post-annexation, Crimea's Internet infrastructure is entirely integrated with the Russian network. The integration started with the Russian-backed Crimean government building the necessary infrastructure to replace the Ukrainian network. This, however, was a very slow and tedious process as Crimea's location ensured substantial dependency on Ukraine's infrastructure. Russia gradually and systematically curtailed reliance on Ukraine through the replacement of ASes and other infrastructure over a period of three years. The systematic overhaul happened in three stages. Firstly, Ukraine's telecom companies and internet service providers started pulling out of their operations from Crimea. Some did it willingly, like MTS Ukraine selling its holdings in Crimea, whilst others, like Ukrtelecom, were forced to shut down their operations, when armed militia restricted the entry of the company's staff inside their facilities.[24] Later, the operations of Ukrtelecom were overtaken by Russia-backed Krymtelekom.[25]

Secondly, Russia attempted to truncate all direct links between Crimea and Ukraine.

[23] Ibid.

[24] **"MTS Ukraine Selling Crimea property"**, *Comms Update*, 13 October 2014.

[25] **"Ukrtelecom Out of Crimea"**, *Comms Update*, 11 February 2015.

Ukrainian actions did not help its case as it put sanctions against ASes (Russian included) operating in Crimea post-annexation. This further diminished Ukrainian control and access to the region and resulted in the creation of small Crimean ASes connected to Russia-registered ASes like Miranda Media, Crelcom, and CrimeaCom.

Finally, Russia aggressively started building telecommunications infrastructure to connect with Crimea. Russia's state-owned telecom company Rostelecom built a 110 Gbps submarine link called the Kerch Strait Cable from Russia to Crimea, costing $25 million. Therefore, from 2014 to 2017, Russia gradually altered Crimea's internet routing routes, essentially moving data through Russia. By mid-2017, no more data paths from Crimea were going through Ukrainian ASes.[26] This signifies that Russia-influenced ASes started operating in Crimea, establishing their BGP agreements, and ousting the Ukrainian network. As a result, since 2014, Crimeans have been watching on the internet what Russians want them to see. For the Russian Federation, the lessons they learned from the Crimean experiment were significant and they wasted no time in applying the same strategy to Donbas.

Donbas

Where Eastern Ukraine differs from Crimea is the ambiguous political nature of its relationship with Russia and Ukraine, with neither country having complete control over the region. Russia's attempt to control internet routing has been challenging because its network is far more complex with many more actors operating in the region than in Crimea. Reports note that even though there are several direct links between Russia and Ukraine, since 2014, the data flow between these routes has severely dropped.[27] The level of Russian control over Donbas is hard to access but according to research by the University of Paris, there are no data routes between Donbas and Ukraine anymore.[28] Further, a data package from Donbas directly reached Russia without any rerouting. What this essentially means for Donbas locals is that they have slower connectivity for higher prices and complete Russian control on what they are allowed to access online. Furthermore, the Donbas network is now part of the Russian Sovereign Internet/RuNet indicating the possibility of online surveillance, data capture, and censorship.[29] Hence, Russian control over the Donbas network indicates its intention to bring the entire Donbas territory under its influence/ authority.

[26] Sebastian Moss, **"How Russia Took Over the Internet in Crimea and Eastern Ukraine"**, Data Center Dynamics, 25 February 2022.

[27] Frédérick Douzet et al., no. 4.

[28] Ibid.

[29] Sebastian Moss, no. 26.

Is RuNet a Failure?

The Russia–Ukraine conflict, as well as Russia's 2014 annexation of Crimea, draw light on the geopolitics of data routing and the usage of the Border Gateway Protocol (BGP) as a tool of control. BGP is used by states to monitor and ensure censorship, block users and websites, carry out cyberattacks on other internet infrastructures, and hijack traffic from other networks. Russia not only successfully created a Sovereign Internet named RuNet, out of concerns that the West can constrict its access to global internet and to ostensibly protect its citizens from alleged disinformation and cyberattacks, but has also integrated the Donbas and Crimean networks into RuNet. Has the current conflict between Russia and Ukraine reaffirmed the Russian campaign for Sovereign Internet?

Firstly, Russia established RuNet to ensure protection from cyberattacks. Russia's Foreign Ministry alleged that the US and its allies have put together a group of internal "offensive cyber-forces", attacking Russia's critical infrastructure.[30] Therefore, RuNet, it seems, has not been successful in stopping cyberattacks. Secondly, as a result of Russia's military operation in Ukraine, Western big tech companies and their platforms have pulled out of the country.[31] This, of course, does not equate to Russia being barred from the global internet. ICANN and the US have repeatedly stated that the Russian Internet will not be blocked.[32] Therefore, Russian concern of being blocked from the global internet by the West has not materialised. Thirdly, Russian backing of RuNet to protect its citizens from alleged Western disinformation too has not been successful. Reports note that Russians are finding several technical workarounds to bypass the RuNet.[33] Finally, the creation of such splinternets, have made the business of data routing slower and more expensive in Donbas and Crimea, forcing the local governments there to unnecessarily invest in infrastructure for connectivity with Russia.[34] It would seem that Russia has not been able to fully achieve the objectives which led the country to develop RuNet.

[30] **"Russia Blames the US For Cyberattacks"**, *RT News*, 29 March 2022; Monica Buchanan Pitrelli, **"Anonymous Declared a 'Cyber War' Against Russia. Here are the Results"**, *CNBC*, 16 March 2022.

[31] Michael Race and Lucy Hooker, **"Which Companies are Pulling Out of Russia?"**, *BBC News*, 11 March 2022.

[32] Brian Fung, no. 14; Nicol Turner Lee and Samantha Lai, **"Is There Too Little Oversight of Private Tech Companies in the Russia-Ukraine Conflict?"**, *Brookings*, 30 March 2022.

[33] Yasmeen Serhan, **"How Western News is Getting Around Putin's Digital Iron Curtain"**, The Atlantic, 22 March 2022.

[34] Pranav Mukul and Anil Sasi, **"Explained: Why the Russia-Ukraine War Threatens to Splinter the Internet"**, *The Indian Express*, 2 April 2022.

About the Author

Ms Krutika Patil is a Research Analyst at the Manohar Parrikar Institute for Defence Studies and Analyses, New Delhi.

Manohar Parrikar Institute for Defence Studies and Analyses is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defence and security. Its mission is to promote national and international security through the generation and dissemination of knowledge on defence and security-related issues.

Manohar Parrikar Institute for Defence Studies and Analyses
1, Development Enclave, Rao Tula Ram Marg
New Delhi 110 010 India
T +91-11-2671 7983 F +91-11-2615 4191
www.idsa.in
Twitter @IDSAIndia
www.facebook.com/ManoharParrikarInstituteforDefenceStudiesAnalyses