UA: UKRAINE ANALYTICA

Issue 1 (27), 2022

- WORLD ORDER
- RUSSIAN WAR
- POLICIES AND PROPAGANDA

UA: UKRAINE ANALYTICA

Issue 1 (27), 2022

WAR

Editors
Dr. Hanna Shelest
Dr. Mykola Kapitonenko

Publisher:
Published by NGO "Promotion of Intercultural Cooperation" (Ukraine), Centre of International Studies (Ukraine), with the financial support of the Representation of the Friedrich Ebert Foundation in Ukraine and the Black Sea Trust for Regional Cooperation – a Project of the German Marshall Fund of the United States.

UA: Ukraine Analytica is the first Ukrainian analytical journal in English on International Relations, Politics and Economics. The journal is aimed at experts, diplomats, academics, students interested in the international relations and Ukraine in particular.

Contacts:
website: http://ukraine-analytica.org/
e-mail: Ukraine_analytica@ukr.net
Facebook: https://www.facebook.com/ukraineanalytica
Twitter: https://twitter.com/UA_Analytica

ISSN 2518-7481

500 copies

BOARD OF ADVISERS

TABLE OF CONTENTS

RUSSIA'S WAR ON THE INTERNET

Verena Maria Wingerter
DCSO Deutsche Cyber-Sicherheitsorganisation

Russia's most recent aggression has resulted in its geopolitical, financial, economic, as well as online isolation. Russia's Internet is changing rapidly due to censorship and surveillance regulation; laws introducing technical requirements for the independent functioning of the Internet; Western sanctions; and the exit of key IT providers from the Russian market. But efforts to create a self-reliant Russian Internet are not new. Over the last decade, Russia has introduced regulations to shape a distinct online sphere. This paper provides an overview of Russian Internet governance, examines the cyber aspect of the ongoing war, and analyses the current developments and their effects on cyberbalkanisation.

Introduction

Russia has achieved a reputation for exploiting the open nature of the Internet by spreading misinformation, meddling in foreign elections, and conducting cyber-attacks, both for destructive purposes and espionage. While Russia exploits the open nature of the Internet abroad, at home the state is far more restrictive in its approach. Russian authorities are aware of the risks for regime stability associated with an open and free Internet, and have enacted increasingly restrictive regulations in order to maintain regime stability by preventing public uprisings such as the 2011 protests against Putin's regime, as well as controlling political narratives. As a result, the Russian Internet is characterised by censorship, surveillance, and state control. Moreover, Russia introduced legal and technical requirements to disconnect its infrastructure from the global Internet.

Russia's war against Ukraine has accelerated these critical developments: more repressive censorship laws create a distinct Russian online sphere. The exit of key international Internet infrastructure providers adds to the increased risk of cyberbalkanisation; the fragmentation of the global Internet into distinct online spheres.

> ***Russia has achieved a reputation for exploiting the open nature of the Internet by spreading misinformation, meddling in foreign elections, and conducting cyber-attacks, both for destructive purposes and espionage***

This paper examines the effects of Russian and Western actions on the open and free nature of the Internet. It summarises the history of Russian Internet governance, highlights the online dimension of Russia's war, and evaluates its effect on the global Internet and the threat of cyberbalkanisation. While current developments indicate a disintegration of the global Internet, policy makers can still establish a common understanding of Internet regulation to safeguard global connectedness.

Russian Internet Governance: Overview

The Internet arrived in Russia in 1990 and developed freely throughout the 1990s and 2000s. However, already in 1998, the surveillance and wiretapping system used by the KGB to intercept phone communication, the System for Operative Investigative Activities (SORM), was expanded to cover Internet communication. The agency in charge of this new surveillance technology was the domestic intelligence service FSB, under its then director and the current president, Vladimir Putin.[1]

In 2011, disputed election results triggered the biggest political protests since the end of the Soviet Union. These 2011 protests were facilitated by the Internet and its ability to gather support and coordinate protest efforts.[2] To maintain regime stability, the Russian authorities shifted in their position towards the Internet, and enacted increasingly restrictive regulations. Within a year, a bill intended to protect children from harmful information was adopted, which introduced a blocklist operated by the federal communications regulator Roskomnadzor.[3] The blocklist required Internet service providers (ISPs) to block access to contents deemed inappropriate or harmful by courts, the legislature or Roskomnadzor itself.

Prior to the 2014 Winter Olympics in Sochi, new security measures were introduced with significant effects for online privacy, such as the "blogger law" requiring all websites with more than 3,000 daily visitors to register with the government,[4] or regulations requiring identification of public Wi-Fi users.[5] More importantly, however, SORM was expanded to include social network monitoring, as well as the introduction of SORM-3, which differs from previous systems in that it consistently analyses all Internet traffic, while simultaneously storing and collating users' metadata to create individual profiles.[6]

In 2016, the anti-terrorism legislation[7] included highly controversial stipulations for internet service providers (ISPs), requiring them to store user communication for six months and related metadata for three years. These laws envisioned that all encrypted data had to be accessible for the government, either through government backdoors or encryption keys.[8] Further censorship measures saw the banning of virtual private networks (VPNs) in 2017[9]

1 A. Soldatov, I. Borogan, *The Red Web: The Kremlin's War on the Internet,* Public Affairs: New York 2017.

2 S. White, I. McAllister, *Did Russia (Nearly) have a Facebook Revolution in 2011? Social Media's Challenge to Authoritarianism*, "Politics", 2014 Vol 35(1), pp. 72-84, DOI: 10.1111/1467-9256.12037

3 D. Turovsky, *This is how Russian Internet censorship works*, "Meduza", 13 August 2015, [https://meduza.io/en/feature/2015/08/13/this-is-how-russian-internet-censorship-works].

4 N. Maréchal, *Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy*, "Media and Communication", March 2017: Vol5(1), pp. 29-41, DOI: 10.17645/mac.v5i1.808

5 *Passport now required to use public Wi-Fi in Russia*, "Russian Legal Information Agency (RAPSI)", 8 August 2014, [http://rapsinews.com/legislation_news/20140808/271879206.html].

6 J. Kerr, *The Russian Model of Digital Control and Its Significance, [in:] N.D. Wright (ed.) AI, China, Russia, and the Global Order*, Air University Press: Maxwell 2019, pp. 62-74.

7 The anti-terrorism laws of 2016 are commonly referred to as 'Yarovaya Laws' named after Irina Yarovaya, then Head of the Parliamentary Committee for Security and Anti-Corruption.

8 D. O'Brien, E. Galperin, *Russia Asks for The Impossible with Its New Surveillance Laws*, "Electronic Frontier Foundation", 19 July 2016, [https://www.eff.org/deeplinks/2016/07/russia-asks-impossible-its-new-surveillance-laws].

9 A. Barbaschow, Putin bans VPN use in Russia, "ZDNet", 31 July 2017, [https://www.zdnet.com/article/putin-bans-vpn-use-in-russia/].

and the attempted blocking of the popular messaging app Telegram, which managed to evade the ban eventually lifted in 2020 by concealing its traffic source behind Google and Amazon's hosting services, thereby constantly changing its IP addresses. This cyber-dodging tactic resulted in collateral damage, such as the temporary blocking of VKontakte, Facebook, and Twitter.[10]

> ***To maintain regime stability, the Russian authorities shifted in their position towards the Internet, and enacted increasingly restrictive regulations***

Another regulation of the utmost importance is the Law on an Autonomous Internet, better known as Sovereign Internet Law, adopted in 2019. The law mandates a Russian Internet able to function independently, and does so via three key stipulations:

- It requires Internet traffic to be routed through special servers that can function as so-called kill switches, meaning they can disconnect Russia from the global Internet. These routing requirements allow Russian authorities to monitor and control cross-border traffic and react to severe threats impacting the stability, security, and integrity of Russia's Internet.[11]
- It requires ISPs to install "technical equipment for counteracting threats" (TSPU).[12] This TSPU system allows for deep packet inspection, an intrusive filtering method able to block specific contents. The system was reportedly used for the first time in March 2021 to "throttle Twitter traffic" for Russian users.[13]
- It requires the introduction of a national domain name system controlled by Roskomnadzor. The domain name system (DNS) is often described as the telephone book of the Internet and is the essential mechanism by which computers reachable through the Internet are identified.[14] The DNS is global in nature and the backbone of the connected, global Internet. It is unclear whether national domain name systems will be compatible with the global DNS.

In 2020, the Russian Ministry of Digital Development, Communications and Mass Media introduced a new bill targeting encryption protocols to ensure the continued effectiveness of Russia's filtering methods.[15] In the wake of the war against Ukraine in 2022, freedom of speech has further been restricted both offline and online.

10 I. Khurshudyan, *How the founder of the Telegram messaging app stood up to the Kremlin – and won*, "The Washington Post", 28 June 2020, [https://www.washingtonpost.com/world/europe/russia-telegram-kremlin-pavel-durov/2020/06/27/4928ddd4-b161-11ea-98b5-279a6479a1e4_story.html].

11 A. Epifanova, *Deciphering Russia's 'Sovereign Internet Law': Tightening Control and Accelerating the Splinternet*, "DGAP Analysis", 16 January 2020, [https://dgap.org/sites/default/files/article_pdfs/dgap-analyse_2-2020_epifanova_0.pdf].

12 Ibid.

13 C. Cimpanu, *Academic: Russia deployed new technology to throttle Twitter's traffic*, "The Record", 6 April 2021, [https://therecord.media/academics-russia-deployed-new-technology-to-throttle-twitters-traffic].

14 A. Epifanova, *Deciphering Russia's 'Sovereign Internet Law': Tightening Control and Accelerating the Splinternet*, "DGAP Analysis", 16 January 2020, [https://dgap.org/sites/default/files/article_pdfs/dgap-analyse_2-2020_epifanova_0.pdf].

15 C. Cimpanu, *Russia wants to ban the use of secure protocols such as TLS1.3, DoH, DoT, ESNI*, "ZDNet", 22 September 2020, [https://www.zdnet.com/article/russia-wants-to-ban-the-use-of-secure-protocols-such-as-tls-1-3-doh-dot-esni/].

The trajectory of Russian Internet governance shows a clear progression towards more surveillance, blocking, and user restrictions. The Kremlin further displays a preference for decreasing dependency on foreign actors and developing a Russian Internet sphere,[16] which could sustain itself independently from the global Internet, thereby increasing the risk of cyberbalkanisation.

Russia & the Internet: Fear of Cyberbalkanisation

Cyberbalkanisation applies the controversial term of balkanisation, understood as "the tendency of an area to divide into smaller parts, which are uncooperative or even hostile to each other,"[17] to cyberspace. Such cyberbalkanisation can refer to regulations concerning access to contents and business models, to specific software, or to hardware and network infrastructure. Developments in Russia indicate a decoupling on all three accounts:

- Regulations concerning access to contents and business models mean that different regulatory frameworks require organisations to adjust their business models. Censorship regulations and the law requiring the local storage of personal data, introduced in 2015, have led to a distinct Russian Internet experience.
- Regulations concerning specific software refer to a regional fragmentation of software usage, for example by banning certain software often on grounds of national security, or by demanding certain software to be deployed. For example, a 2019 law demands the pre-installation of Russian software on all IT devices sold in Russia, resulting in a fragmentation of business models and online experiences.[18] Another possible reason for cyberbalkanisation with regards to specific software is the market exit by a software provider.
- Regulations of specific hardware and network infrastructure highlight the risk of incompatible hardware and network infrastructure leading to cyberbalkanisation. While Russia relies on China for its 5G infrastructure, the Law on an Autonomous Internet clearly states the intent to develop their own Internet infrastructure. Namely, the efforts to introduce technical equipment into Russia's Internet infrastructure and to create a national Domain Name System, which guarantees the continued functioning of the Internet in case of global disconnection, prove that the risk of cyberbalkanisation is real.

Russia's War in Ukraine: The Online Dimension

Russia's war against Ukraine has not just affected global geopolitics, but also the cyberspace landscape. Long before the recent escalation, the conflict was already being fought online. Sometimes described as Russia's cyber testing lab, Ukraine has been a target of historically significant cyberattacks, most notably those targeting its power grid in 2015 and 2016.[19] Ukraine

16 See also: *Doctrine of Information Security of the Russian Federation*, "The Ministry of Foreign Affairs of the Russian Federation", 5 December 2016, [https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163].

17 S. Tanase, *VB2018 paper: Internet balkanization: why are we raising borders online?* "Virus Bulletin", 2018, [https://www.virusbulletin.com/virusbulletin/2019/02/vb2018-paper-internet-balkanization-why-are-we-raising-borders-online].

18 *Russia bans sale of gadgets without Russian-made software*, "BBC News", 21 November 2019, [https://www.bbc.com/news/world-europe-50507849].

19 A. Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* Doubleday: 2019.

was also seriously affected by the NotPetya worm, which caused global losses of at least USD 10 billion.[20] Thus, it should come as no surprise that several Russian state-backed cyber actors launched over 200 coordinated cyber-operations immediately prior to the Russian ground invasion of Ukraine.[21] Private cybersecurity vendors also observed a correlation between cyberattacks and kinetic attacks, as well as a preference for primarily targeting critical infrastructure and Ukrainian government organisations with destructive campaigns.[22]

Russia's war efforts not only focus on Ukraine but also target its own information sphere. New regulations have imposed strict censorship rules concerning reporting on the war

As a consequence of attacks from Russian IP addresses, the world's largest certificate authority for digital certificates or TLS/SSL certificates, essential for secure and reliable Internet communication, announced that it would pause the "issuance and reissuance of all certificate types affiliated with Russia and Belarus."[23] In response, Russia announced the creation of a domestic certificate authority,[24] which raises concerns about increased surveillance and censorship and increases the risk of cyberbalkanisation.

Russia's war efforts not only focus on Ukraine but also target its own information sphere. New regulations have imposed strict censorship rules concerning reporting on the war. This impacts not only Russian journalists but any Russia-based individual, as well as foreign media outlets operating in Russia. As a result, Russian media reflects the propaganda of the Russian state with the fear of retribution, while other reporting is being censored, and many foreign outlets have suspended their operations in Russia as a direct consequence of the new regulations.[25] Thus, the online experience of Internet users within and outside of Russia differs significantly.

Immediate Consequences of Russia's Invasion: Cyberbalkanisation

Russia's war against Ukraine has not only changed geopolitical realities but also had an impact on the isolation of the Russian Internet and its efforts at cyberbalkanisation. Most visible is the exit of many Western firms from Russia. Almost 1,000 firms across all business sectors have halted their Russia operation and are in

20 Ibid.

21 T. Burt, *The hybrid war in Ukraine,* "Microsoft", 27 April 2022, [https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks].

22 Ibid.

23 SSSCIP Ukraine (@dsszzi), *In response to the evolving geopolitical situation in Ukraine DigiCert is pausing issuance and reissuance of all certificate types affiliated with Russia and Belarus.* "Twitter", 11 March 2022, [https://twitter.com/dsszzi/status/1502204367784624130].

24 T. Brewster, *Big Web Security Firms Ditch Russia, Leaving Internet Users Open to More Kremlin Snooping*, "Forbes", 11 March 2022, [https://www.forbes.com/sites/thomasbrewster/2022/03/11/russiansexposed-to-more-surveillance-and-cybercrime-as-web-security-giants-leave-over-ukraine-invasion].

25 O. Darcy, *CNN, BBC, and others suspend broadcasting from Russia after Putin signs law limiting press*, "CNN Business", 5 March 2022, [https://edition.cnn.com/2022/03/04/media/bbc-cnn-russia-putin-media-law/index.html].

the process of withdrawing their assets.[26] This also applies to IT firms, such as Oracle, IBM, and Intel that all suspended their operations. While these companies provide products widely used in business settings, the suspension of operations by two key Internet backbone carriers has had severe effects on the available Internet bandwidth in Russia. Lumen (formerly CenturyLink) and Cogent are both top international transit providers for Russian telecom giants Rostelecom and TTK, as well as all three major mobile operators, MTS, Megafon, and VEON.[27] A disconnect on the scale of the Russian operations is unprecedented in the history of the Internet, and has increased fears for the decoupling of Russia from the Internet and for cyberbalkanisation.

To that end, Ukraine requested the revocation of Russia's top-level domain .ru, as well as its Cyrillic equivalent, thereby removing all Russian IP addresses and effectively disconnecting Russia from the global Internet. Revoking Russia's top-level domain equates to blocking its root server in the domain name system (DNS), thereby blocking access for Russian Internet users and creating significant risks for Internet traffic routed through Russia.[28] The non-profit Internet Corporation for Assigned Names and Numbers (ICANN), responsible for managing the top-level domains of the DNS, denied Ukraine's request, which would have split the Internet and set a dangerous precedent for further conflicts.[29]

Russia has also taken action increasing the likelihood of cyberbalkanisation. In particular, a leaked directive issued by the Russian Ministry of Digital Development, Communications and Mass Media has stoked fears of decoupling Russia from the global Internet. The directive outlined technical measures that operators of state websites have to implement. These measures include switching to DNS servers located on Russian territory, switching to the .ru top-level domain, and removing all foreign hosted JavaScript code.[30]

Further, Russia's strict censorship regulations increasingly alter the Russian online experience.[31] Russia is also rerouting Internet traffic in occupied Ukraine, specifically in the Kherson region, through Russian Internet infrastructure, which also highlights this trend towards cyberbalkanisation.[32] Overall, Russia's activities indicate a perceived need for control of its online sphere.

---

26 *Almost 1,000 Companies Have Curtailed Operations in Russia – But Some Remain*, "Yale School of Management", 15 May 2022, [https://som.yale.edu/story/2022/almost-1000-companies-have-curtailed-operations-russia-some-remain].

27 D. Madory, *Cogent disconnects from Russia*, "Kentik", 4 March 2022, [https://www.kentik.com/blog/cogent-disconnects-from-russia].

28 S. Vaughan-Nichols, *Ukraine asks for Russia to be kicked off the internet*, "ZDNet", 1 March 2022, [https://www.zdnet.com/home-and-office/networking/Ukraine-asks-for-russia-to-be-kicked-off-the-internet].

29 S. Vaughan-Nichols, *ICANN rejects Ukraine's request to block Russia from the internet*, "ZDNet", 3 March 2022, [https://www.zdnet.com/home-and-office/networking/icann-rejects-ukraines-request-to-block-russia-from-the-internet].

30 NEXTA (@nexta_tv), *#Russia began active preparations for disconnection from the global Internet*, "Twitter", 6 March 2022, [https://twitter.com/nexta_tv/status/1500553480548892679].

31 A. Troianovski, *Russia Takes Censorship to New Extremes, Stifling War Coverage*, "The New York Times", 4 March 2022, [https://www.nytimes.com/2022/03/04/world/europe/russia-censorship-media-crackdown.html].

32 M. Hunder, T. Balmforth, *Russia reroutes internet traffic in occupied Ukraine to its infrastructure*, "Reuters", 2 May 2022, [https://www.reuters.com/world/europe/russia-reroutes-internet-traffic-occupied-ukraine-its-infrastructure-2022-05-02].

The Way Forward?

The Internet was designed to allow for the open and free exchange of information; however, developments worldwide are challenging this very idea. Russia's efforts to create an independently functioning Internet, even decoupling from the global DNS, pose the biggest threat to the global Internet infrastructure to date. While countries such as China and its Great Firewall have created their own Internet sphere, these states continue to subscribe to the internationally administered DNS. In comparison, Russia's recent attempts to establish a national DNS, which can function independently from the global DNS, would change the underlying structure of the Internet and allow for the complete segmentation of Russia's Internet.

However, it is important to note that it is not only authoritarian regimes that pose challenges to the global Internet. Also, Western powers such as the European Union, its member states, and the United States have enacted significant regulations, increasing the likelihood of cyberbalkanisation. Both data localization requirements and the General Data Protection Regulation (GDPR) have impacted the business models of organisations active in the EU. Additionally, the EU requires the takedown and blocking of certain online content. This content moderation is justified on the grounds of countering disinformation and hate speech and alters the online experience of Internet users in the EU. The United States has also adopted measures in line with cyberbalkanisation, most prominently, its banning of Huawei on grounds of national security.

Regulating technologies is a difficult endeavour, and so, recommendations must be contextually aware and flexible. A one-size-fits-all approach rarely works in international politics, and the issue of cyberbalkanisation is no different. Nonetheless, policy makers can take action to improve the current situation with regards to Russia and its decoupling of the Internet.

- Russia is effectively shaping a distinct Russian online sphere. Western states criticise authoritarian measures such as surveillance or censorship readily, however, policies such as content moderation and surveillance also apply to their Internet infrastructure. Thus, an honest conversation on Internet regulation is necessary to establish universally applicable standards of content moderation vs censorship, determine the legitimate use of surveillance, and address issues of privacy and national security. If Western states and democratic nations coalesce around a shared understanding of the challenges at hand, they can work towards preserving the interconnectedness of the Internet.[33]
- The recent Russian policies target the distribution of information about the war and Russia's standing in the world, to control the narrative and maintain regime stability. While it has become harder for Russians to access information about the war, this is not yet impossible. Solutions such as virtual private networks (VPNs) can help circumvent Russia's blocking measures. Companies can support these efforts by not geoblocking users behind VPNs. Most effective, however, would be the provision of information via technologies still allowed in Russia. To be

33 S. Feldstein, *Russia's War in Ukraine Is a Watershed Moment for Internet Platforms*, "Carnegie Endowment for International Peace", 3 March 2022, [https://carnegieendowment.org/publications/86569].

specific, Telegram and WhatsApp remain available to Russian users, and news outlets are recommended to use these channels for sharing information on the war and other topics of relevance.[34]

Cyberspace has long been a domain of Russia's aggressive actions against Ukraine, with campaigns over the years crippling the power supply, and affecting government agencies, sensitive information on social benefits, and transportation infrastructure

- Currently, Russia is not able to sustain its own technology needs. A shortage of chips and the effect of sanctions will keep Russia from being self-reliant in the foreseeable future, thus increasing Russia's dependency on China. While the long-term goals of both countries differ widely, the current setup might allow Russia to evade sanctions.[35] Hence, Western countries should develop a clear position on how to address the partnership between China and Russia in cyberspace. Further, they should evaluate the sanctions regime and its effectiveness regularly. Lastly, Western states should develop a common policy towards technology transfers with Russia and address the issue of technology supply shortages proactively.

Conclusion

The war in Ukraine has attracted much discussion about Russia isolating itself in geopolitical, financial, and economic terms, and the same can be said about its online sphere. While the exit of Western firms has certainly accelerated the process, Russia's efforts at establishing an independently functioning Internet predate the conflict. Since 2012, various laws have introduced surveillance and censorship methods under the guise of protecting children and national security.

Cyberspace has long been a domain of Russia's aggressive actions against Ukraine, with campaigns over the years crippling the power supply, and affecting government agencies, sensitive information on social benefits, and transportation infrastructure such as the postal services or Ukraine's railways. Thus, cyberattacks accompanying the current aggression come as no surprise. However, Ukrainian investments in cyber defence and capacity building with the help of their international partners has prevented widespread destruction by cyber means.[36] While it is too early to judge the effectiveness of Russia's cyberattacks, the conflict in cyberspace has simultaneously resulted in stricter control of information online and the decoupling of Russia from the Internet.

Russia's war has most certainly increased the risk of cyberbalkanisation. While this effort to isolate Russia was unsuccessful, Russia's

34 Y. Serhan, *How Western News Is Getting Around Putin's Digital Iron Curtain*, "The Atlantic", 22 March 2022, [https://www.theatlantic.com/international/archive/2022/03/international-news-russia-kremlin-media-censorship/627120].

35 R. Standish, *Interview: Will the Russian Internet Resemble China's 'Great Firewall'?*, Radio Free Europe Radio Liberty (RFE/RL), 22 March 2022, [https://www.rferl.org/a/russia-internet-china-great-firewall-censorship-meta-facebook-instagram/31765408.html].

36 J. Ling, *Ukraine's Digital Battle with Russia Isn't Going as Expected*, "Wired", 29 April 2022, [https://www.wired.com/story/ukraine-russia-digital-battle].

bans on Western social media platforms and the exit of Western firms from the Russian market increase cyberbalkanisation.[37] With the exit of key Internet infrastructure providers, Russia's Internet has suffered setbacks in its reliability and speed. Sanctions targeting high technology imports decrease Russia's ability to become technologically self-reliant. Censorship regulations have already created an own Russian online space distinct from the global information domain.

While Russia is moving towards its own decoupled Internet, Western states lack a cohesive strategy to counter cyberbalkanisation. Differing policies concerning privacy, data localisation, preferences for local high technology solutions, and content management of hate speech and disinformation have resulted in a fragmented Western response to cyberbalkanisation developments. However, if Western states – and democracies worldwide – want to guarantee and protect international connectedness and civil liberties online, they need to find common ground on Internet governance. In the meantime, concrete actions such as providing information to the Russian public and addressing the issue of Russian technology imports can counter the trend of Russia's isolation online and global cyberbalkanisation.

Verena M. Wingerter is a Threat Intelligence Researcher for the Deutsche Cyber-Sicherheitsorganisation (DCSO), where she covers cyber policy and strategy as well as Russian threat activities. She holds an MA in International Affairs from the Hertie School and a BA in Governance from the Albert-Ludwigs-University. She has also studied at the George Washington University, United States, and at MGIMO, Russia.

37 B. Fung, *Ukraine's request to cut off Russia from the global internet has been rejected*, "CNN", 3 March 2022, [https://www.cnn.com/2022/03/03/tech/ukraine-russia-internet-icann/index.html].

Issue 1 (27), 2022
ISSN 2518-7481