Österreichisches Institut für Internationale Politik
Austrian Institute for International Affairs

Trends in International Politics 2023

No end in sight to the global sprint towards digital sovereignty in 2023 (and beyond)

Trend Report 5 / January 2023

Katarina Vehovar

Katarina Vehovar is a Slovenian alumna of Sciences Po Paris's School of International Affairs (PSIA) and King's College London who has been researching governance and practices of policymaking in contemporary Russia – as well as divergences in East-Central European states' trajectories since 1991 more generally – ever since she first began university studies at Sciences Po in 2016. During her graduate studies of International Security in France, which were rewarded with a summa cum laude mention in 2020, she specialised in the evolution of Transatlantic relations, EU-China relations and politics in the Western Balkans. This was complemented by an MSc in Russian and Eurasian Politics and Economics at King's Russia Institute, which she completed with honours in 2021, and a Schuman traineeship at the European Parliament's Liaison Office in Ljubljana, where she gained first-hand insight into the EU's public diplomacy initiatives. Working at the oiip on its "Europe and Its Neighbourhood" programme, Katarina will endeavour to complement existing scholarship on great power competition by examining the ramifications of Russia's full-scale invasion of Ukraine in February 2022 both on Western Balkan states' foreign policy agendas, as well as on the EU as it seeks to (re)frame itself as a geopolitical actor and offer the region an enhanced European perspective.

Impressum:

Österreichisches Institut für Internationale Politik – oiip,
Austrian Institute for International Affairs
A-1090 Vienna, Währinger Straße 3/12, www.oiip.ac.at, info@oiip.ac.at

Even a cursory glance at headlines in *Foreign Affairs* – "How AI Makes Dictators More Dangerous", "The Insidious Cyberthreat" and "The Autocrat in Your iPhone" - suggests that 2022 was not the best year for cyber optimists who profess a belief in technology's democratising power (González 2022). Digital authoritarian systems and "spin dictatorships" continue relying just as much on information manipulation as coercion to consolidate their power (Guriev 2022). Meanwhile, concerns over the use of sophisticated mercenary surveillance systems and invasive AI technology in democracies are also mounting (Deibert 2022).

By exacerbating the security dilemma between powers like the US, EU Russia and China, these trends are fuelling the proliferation of "techno-nationalist narratives" that policymakers in both democratic and authoritarian states are using to legitimise their efforts to gain greater control over the digital space (González 2022). For all these reasons, the near-universal push towards greater digital and technological sovereignty will be one of the most important trends in 2023 and beyond.

A renewed push for digital sovereignty in autocracies and democracies alike

Despite passing the ambitious Sovereign Internet Law in 2019, Russia's quest to achieve full digital sovereignty has been hampered by sanctions on high-tech imports and an unprecedented brain drain of highly-skilled professionals from the domestic IT industry (Prince 2022).

Yet the setbacks triggered by its full-scale invasion of Ukraine last February are highly unlikely to usher in an era of greater internet freedom. Quite the contrary: the national media watchdog Roskomnadzor even *accelerated* the deployment of monitoring systems across Russia throughout the past year, initiating its harshest crackdown on VPNs yet last June (Budnitsky 2022). This shows that authorities have no intention of lifting the "digital iron curtain". In fact, the only major change we can anticipate in 2023 is Russia switching from its (over)reliance on Western know-how to an over-dependence on tech imports from China. The latter is (in)famous for its own expansive censorship system (a.k.a. the "Great Firewall"), which it has been reinforcing continually since its Ministry of Public Security introduced the first measures to regulate domestic Internet usage back in 1997 (Wilde 2022).

Because of rising great power competition and mounting concerns about Chinese cyber-espionage, we can expect calls for greater economic protectionism – and efforts to accelerate technological decoupling from China - to amplify in 2023. A case in point: just this past December, Japan and the Netherlands agreed in principle to support US curbs on Chinese chipmaking (Rao 2022). Meanwhile, Chinese firms such as Huawei are already rushing to building entirely domestic supply chains.

Concerned about their lack of control over international flows of data, we can also expect Western states to start rethinking their own relatively *laissez-faire* approach to internet governance. Already in the past three years, we saw that "digital sovereignty" has become synonymous with resilience for EU member states like Germany. Similarly, the proliferation of hybrid threats has spurred the European Commission into advocating for greater resilience in critical technology areas.

Towards even greater fragmentation of the global internet

Regardless of whether they are pursuing digital sovereignty to accrue social and economic resilience or because they share Russian President Vladimir Putin's view that the global internet is a nefarious "CIA project" (MacAskill 2017), states are displaying an increasing readiness to interfere in cyberspace governance to (re)define operational, technical and regulatory standards according to their own geopolitical needs. In 2023 and beyond, this will exacerbate one of the major risks stemming from the unprecedented global push for "digital sovereignty": global internet's "balkanisation" (i.e. fragmentation) into national segments.

Known as "splinternet", this phenomenon is especially pernicious in non-democratic and illiberal states because it stymies internet users' efforts to bypass domestic propaganda and censorship apparatuses (Epifanova 2020). It is by no means a new phenomenon, for the human rights group *Access Now* already recorded 155 internet shutdowns across nearly countries in 2020 – up from 75 in 2016 (Volpicelli, 2021). What is more concerning is the prospect that these shutdowns will become more frequent. This, after all, was witnessed in Russia following the start of its full-scale invasion of Ukraine last February (Thornhill 2022). It is also for this reason that the invocation of "digital sovereignty" - especially by digital authoritarians now rapidly reinforcing modern-day iron curtains – is one of the most important trends to follow in 2023 and beyond.

Bibliography

Budnitsky, S. (2022): Kremlin Tightens Control over Russians' Online Lives – Threatening Domestic Freedoms and the Global Internet. The Conversation (online), https://theconversation.com/kremlin-tightens-control-over-russians-online-lives-threatening-domestic-freedoms-and-the-global-internet-182020 (retrieved: 15 December 2022).

Burwell, & Propp. (2022): Digital Sovereignty in Practice: The EU's Push to Shape the New Global Economy, Atlantic Council (online), https://www.atlanticcouncil.org/in-depth-research-reports/report/digital-sovereignty-in-practice-the-eus-push-to-shape-the-new-global-economy/ (retrieved: 15 December 2022).

Deibert, R. J. (2022): The Autocrat in Your iPhone: How Mercenary Spyware Threatens Democracy. Foreign Affairs (online), https://www.foreignaffairs.com/world/autocrat-in-your-iphone-mercenary-spyware-ronald-deibert (retrieved: 15 December 2022).

Epifanova, A. (2020): Deciphering Russia's 'Sovereign Internet Law. GAP - German Council on Foreign Relations (online) https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law (retrieved 14 December 2022).

González. A. (2022): Digital Sovereignty and Digital Authoritarianism. In *Sciences Po* [Discussant]. 2022 Annual Conference: Digital Sovereignty and Geopolitical Crisis, Paris, France. https://www.sciencespo.fr/public/chaire-numerique/en/2022/12/09/replay-a-look-back-at-the-annual-conference-2022-digital-sovereignty-and-geopolitical-crisis/ (retrieved: 15 December 2022).

Guriev. S. (2022): Digital Sovereignty and Digital Authoritarianism. In *Sciences Po* [Discussant]. 2022 Annual Conference: Digital Sovereignty and Geopolitical Crisis, Paris, France. https://www.sciencespo.fr/public/chaire-numerique/en/2022/12/09/replay-a-look-back-at-the-annual-conference-2022-digital-sovereignty-and-geopolitical-crisis/ (retrieved 14 December 2022).

MacAskill, E. (2017): Putin Calls Internet A "CIA Project" Renewing Fears of Web Breakup. The Guardian (online), https://www.theguardian.com/world/2014/apr/24/vladimir-putin-web-breakup-internet-cia (retrieved: 15 December 2022).

Prince, T. (2022): "A Nail In The Coffin": Tech Workers Are Fleeing Russia And The Impact Will Last For Years. *RadioFreeEurope/RadioLiberty* (online), https://www.rferl.org/a/russia-it-workers-brain-drain/31783558.html (retrieved: 15 December 2022).

Rao, P. (2022): The US Chips Away. Semafor (online), https://www.semafor.com/newsletter/12/13/2022/the-us-chips-away (retrieved: 15 December 2022).

Thornhill, J. (2022): Russia's Digital Iron Curtain Will Fail. Financial Times (online), https://www.ft.com/content/26e88a2b-c7ba-46c7-8191-490188f4757b (retrieved 19 December 2022).

Volpicelli, G.M. (2021): The Draconian Rise of Internet Shutdowns. Wired (online), https://www.wired.co.uk/article/internet-shutdowns (retrieved 19 December 2022).

Wilde, G., & Sherman, J. (2022): Putin's Internet Plan: Dependency With a Veneer of Sovereignty. Brookings (online), https://www.brookings.edu/techstream/putins-internet-plan-dependency-with-a-veneer-of-sovereignty/ (retrieved: 15 December 2022).