

Gosplan for Packets:
Why a Whitelisted Internet Cannot Coordinate the Society It Controls

By Mark Gushchin

Helsinki, Finland

2026

In March 2026 the mobile internet in central Moscow went dark, and stayed dark for nearly three weeks. When pieces came back, they came back on the state's terms. A phone could reach a government-compiled "whitelist" – the Gosuslugi portal, a few banks, the domestic marketplaces and social networks – and nothing else. Whatever wasn't on the list had simply stopped existing. Officials blamed drone threats, plausibly enough – but the real novelty was the change in default. For two decades Russian censorship had worked by subtraction: find an enemy, block it, move to the next. A whitelist runs the other way: everything is forbidden unless someone in authority has said otherwise.

My claim is that a network like this is not a more refined censorship tool. It is something older: the socialist calculation problem brought back to life, ported from the planned economy to the routing of packets. A state can take the wires. What it cannot do is coordinate the society that lives on them, and it fails for the reason Gosplan failed: the knowledge the job requires sits nowhere it can be gathered and held. The evidence doesn't come from any opposition manifesto. It comes from the planner. Having banned the tools of open connection for ordinary Russians, the state buys those same tools for itself, because the walled network it builds for everyone else cannot carry its own business. Hypocrisy is the boring reading. The useful one is that the state is telling us, through its purchases, that the wall does not work.

The argument leans on something Hayek pointed out in 1945 and nobody has since overturned. The knowledge a society uses to coordinate itself is never sitting in one head. It is broken into fragments across millions of people, much of it tacit – competence you have in your hands but can't write down. Markets move it around through prices. A price takes the circumstances of thousands of strangers and compresses them into a single number a fourth stranger can act on without ever learning what produced it. A network does something similar. When a user picks a service, a counterpart, a protocol, a time of day, the choice is itself a signal about what that person needs, and exists only because it was made. Forbid the choice and the signal doesn't turn up elsewhere instead. You just don't get it.

A whitelist assumes the reverse: that an authority can know ahead of time which connections a society will need, and write them down. The modern version – the one that lends the whitelist whatever intellectual respectability it has – runs like this: with enough surveillance and a capable model, the centre can finally compute the list that markets used to discover. This is the old calculation problem in new clothes, and it breaks in the old place. An optimiser can only chew on the data it is handed, which records what people did under the constraints they already faced, never what they'd have chosen under conditions the censor didn't allow. Train a model on a censored network and it learns the censorship, not the shape of what people want. Computation doesn't speed discovery up; it swaps discovery for a forecast, and the thing forecast is a past the forecasting froze in place. You can't read off a discovery your prohibition prevented.

Three more Austrian ideas turn this from a grumble into a diagnosis. Take Huerta de Soto's split between static and dynamic efficiency. Static efficiency asks a tidy question: given these resources and ends, is the allocation good? The dynamic question matters more: does the system let people stumble onto ends and means nobody had imagined yet? The case for a market was never that it clears cleanly at any instant. It is where entrepreneurial discovery happens, messily, inventing things people didn't know to ask for. Judge the whitelist by static tidiness and you file it under

“shorter menu,” missing the point: the loss isn’t a few missing dishes. You can freeze discovery and still keep perfect order. The order is real. What’s gone is the part of the future that hadn’t shown up yet.

The second idea is Mises on how intervention reproduces itself. You bring in a control to fix one problem; it creates distortions of its own; those become the reason you need the next, larger one. There is no natural stopping point: every failure gets read not as “the method was wrong” but as “the last dose was too small.” The third is what the prize question puts on the table: what changes once control is written into code rather than enforced by men with truncheons. Code can flip a whole society’s default in an afternoon. A free order runs on permitted-unless-forbidden. A prison runs on forbidden-unless-granted. The whitelist is that flip turned into infrastructure – and in Russia it comes at the tail end of a long spiral of failed controls, not the start.

Russia is the starkest live experiment in what happens once the state writes the code, so the mechanics deserve stating right. It did not copy China. It couldn’t. China’s Great Firewall sits at a handful of international gateways – an option only if your network grew up centralised around a few chokepoints, which the Russian one didn’t. It grew up tangled and plural. So Russia built the mirror image. Under the 2019 “sovereign internet” law it pushed filtering boxes, the TSPU, down into the guts of essentially every provider in the country.

The most-cited measurement comes from Xue and colleagues, at the ACM Internet Measurement Conference in 2022. They located more than a million Russian endpoints behind these devices, seventy percent within two network hops of the user. The boxes are in-path and stateful. They watch for the server name in a TLS handshake, the destination address, the fingerprints of QUIC. Placement is the whole point. A control one or two hops from your phone is faster and more precise than one at a national border, and because the boxes are managed centrally though physically scattered, that precision scales by decree. You upgrade the policy once and it lands everywhere.

Laid out in order, the chronology reads like a Misesian spiral transcribed into statute. The 2012 website blacklist proved trivial to dodge. So in 2015 came Revizor, to check that providers really blocked what they claimed. That wasn’t enough; the 2016 Yarovaya laws ordered operators to retain traffic and surrender encryption keys. Retention didn’t give the centre command over flows, so the 2019 law mandated the DPI boxes. Then the boxes got used: a throttling of Twitter in 2021, staged as a demonstration; the wholesale blocking of foreign platforms after the 2022 invasion; and, from 2025, a sustained campaign against VPNs. By Human Rights Watch’s count, 469 services were blocked by early 2026, the three most popular protocols gone since December 2025; an autumn decree let the regulator order blocks without notice. The 2026 whitelist is the next rung up. Every tool’s failure becomes the case for a more invasive replacement – exactly the dynamic Mises described, and the one the builders themselves invoke when they talk approvingly of “continuous modernisation.”

In economic terms, the cost keeps climbing, never converging on a finished system. In September 2024, Reuters and the Russian Forbes reported a plan to spend close to sixty billion rubles (over six hundred million dollars) between 2025 and 2030 just to upgrade the filtering – more, in that one line, than Roskomnadzor’s entire 2023 budget. On top sits a 2.27-billion-ruble machine-learning filter to degrade particular traffic more surgically. The boxes already installed must be rebuilt constantly just to keep pace with traffic growth. None of this is freedom-suppression that eventually pays for itself. It is dynamic inefficiency in nearly pure form: scarce capital and

engineering talent poured into wrecking coordination rather than producing it, on a machine reconstructed continuously just to stay in place. Lewis Carroll's Red Queen now runs the censorship office, sprinting flat out to stand still.

Blocking by default also wrecks things the planner never meant to touch, because the network being carved up is shared. April 2018: Roskomnadzor, trying to kill Telegram, blocked some nineteen million IP addresses at once – most belonging to Amazon, Google and Microsoft, where Telegram was sheltering. Telegram survived. What didn't survive was much of unrelated Russian life – shops, banking, ticketing, even Google's reCAPTCHA, none of it connected to the target. One software firm put the collateral damage near a billion dollars; the president's internet adviser suggested the regulator apologise. The censor couldn't tell its enemy apart from the infrastructure its own economy ran on. And that was one clumsy block on a single afternoon. A whitelist makes that incapacity permanent: permit only what's named in advance, and you've by definition switched off everything you lacked the foresight to name.

Here the planner refutes itself in the most literal place imaginable: its own budget lines. While it criminalises VPN advertising, fines providers, pushes them from app stores and commits tens of billions of rubles to blocking them, the state has been quietly buying VPNs for itself. Working through the federal procurement database, Top10VPN found 236 public contracts for VPN technology signed by state bodies after the invasion, worth over eight hundred million rubles. Novaya Gazeta put 2024 alone at more than fourteen billion rubles of state spending on VPN access. The Kremlin's spokesman has admitted, on the record, to using one. A Roskomnadzor official, announcing another batch of bans, specified that only VPNs "used to bypass blocking" were the problem – the same tool is contraband in your hands and a line item in theirs.

This is praxeology at its sharpest: what an actor does reveals the preferences his words deny. The state's institutions need connectivity that is open, fast and routable, and they prove it by paying for it – on the very market they are otherwise trying to abolish. The planner can't live inside the network he is building for everyone else. In 1920 Mises argued that rational calculation under full socialism is impossible because the planner has cut himself off from the prices that carry a society's knowledge. The Russian state has cut itself off from the open connections that carry it today, and copes the only way it can: by reaching onto the grey market it spends its days policing. The walled internet can't coordinate even the planner's own affairs, never mind a whole society's.

The other half of the story is what ordinary users do in response, and the right lens isn't heroism; it's Kirzner's alertness. Each time one method gets spotted and shut, somebody notices the gap and a new one appears. The catalogue is inventive: camouflaged transports like VLESS tucked inside an ordinary TLS 1.3 session, obfuscated tunnels such as AmneziaWG, domains that rotate faster than they can be blacklisted, traffic smuggled through the relay servers of platforms the state has itself blessed. One published tool routes through the TURN servers behind VK's own calling feature, turning a state-approved service into an unapproved exit. None of these is a grand act of resistance. Each is a small, entrepreneurial discovery of a route the planner didn't think to close.

The censor's counter-moves are where its real nature shows. Late in 2024 Cloudflare switched on Encrypted Client Hello, designed precisely to hide the server name deep packet inspection feeds on. Within a month the TSPU began silently dropping every packet carrying ECH. The privacy upgrade hadn't beaten the filter; it had handed it a clean new thing to match. And the matching no longer confines itself to protocols. Connections to foreign data centres the system treats as suspect

get choked off after a few kilobytes, however the traffic is dressed up. The censor now asks a second question on top of “what protocol are you speaking” – namely, “who are you speaking to.” Bit by bit the blacklist is inverting into its mirror image: the default is suspicion, and connection the exception that must earn its way.

The honest thing – what separates this from wishful thinking – is that most of these tools lose. Whatever is uniform and centralised is exactly what a stateful classifier is built to catch. To the TSPU, a single popular protocol or a reliable fallback server is just a fingerprint waiting to be matched. The whitelist is built to be hostile here: a global relay everyone depends on can simply be left off the list and starved. Centralised resistance fails for the very reason centralised planning fails. It offers the centre one fixed thing to compute against.

The people actually fighting say as much. Reviewing the opposition’s tactical-voting app, its engineers reported that any fixed backend died quickly, and that staying reachable meant signed-configuration discovery, domains rotated out before they could be listed, and monitoring from dozens of probes inside Russia. Their blunt conclusion: a centralised circumvention effort is expensive, brittle and short-lived, while only distributed, adaptive methods last. Coming from the resisters, not the regime, the verdict carries more weight, not less. What endures is never a particular tool. It is the dispersed, endlessly mutating activity of finding the next one. If liberty survives here, it survives as a process – the one form no authority can locate on a map and switch off.

Worth saying where this is heading, even if it hasn’t fully arrived. Put a network that gates connection by permission next to a central-bank digital currency that gates payment, and you have a single architecture where both speech and exchange happen only by explicit grant. Russia is laying both rails: the whitelist on one side, a programmable digital ruble on the other. Bagus read the euro as a device for redistributing claims and concealing losses; run the same logic forward and the calculation problem reaches its furthest form, stretched from prices to packets to money itself. Every transaction becomes an application to be approved. And every application is one more chance for the answer to come back no.

The strongest objection comes from the east. China has run pervasive internet control for two decades and shows no sign of falling over, so – the rejoinder goes – the state can clearly just win. Granted. The Austrian claim was never that tyranny is brittle and collapses by Tuesday. Control can last a very long time. The real question is what it buys you.

What it buys is endurance, and endurance is not coordination. A controlled network can be rock-stable and still be poor, because its real cost is the one Bastiat told us to look for: the unseen. The seen is whatever the state can point at: the approved apps that load, the traffic that flows. The unseen is the company never started, the connection nobody got to make, the discovery foreclosed before anyone knew enough to want it. None of it shows up in a statistic, which is why a planner can mistake a frozen system for a healthy one. China has bought stability and surrendered the open-ended discovery that keeps a network alive – with no instrument to measure what it gave up. And the architecture wasn’t even chosen: Russia would have preferred China’s tidy border model but couldn’t, because its network had grown the wrong shape years before, forcing the costlier distributed design. What it produces is stagnation wearing the costume of order.

A state that writes the code does not lose by collapsing. Its servers keep humming, the whitelist resolves, the approved apps open on cue. It loses the way every planner loses, without need of a

blackout: it can command the network yet coordinate nothing through it; it can forbid by default yet never know what to permit; and so it ties itself to an endless, compounding chase after a process it was built to be incapable of computing. Each failed block ends up financing a more expensive one. Each walled network turns out to need an unwalled exception – which the planner quietly buys for himself. Those fourteen billion rubles of state VPN spending are not an embarrassment at the margin of the project. They are closer to its epitaph, written by the project’s own accountants.

So what does digital interventionism do to the prospects for liberty? Not what its boosters hope, and not what its gloomiest critics fear. It doesn’t extinguish freedom, nor leave it where it found it. It moves the whole contest onto new ground. Once the architecture of power is code, the question of liberty narrows into something stranger: will a society be allowed to discover what it needs? Discovery is the one thing no authority can hand out in advance – until it has been made, nobody knows what it is. The planner, of all people, knows it least of all.

Sources

Theory. Hayek, “The Use of Knowledge in Society” (1945); Mises, “Economic Calculation in the Socialist Commonwealth” (1920), *Socialism* (1922), *Interventionism: An Economic Analysis* (1940) and *Human Action* (1949); Huerta de Soto, *The Theory of Dynamic Efficiency* (2009); Kirzner, *Competition and Entrepreneurship* (1973); Bastiat, “What Is Seen and What Is Not Seen” (1850); Bagus, *The Tragedy of the Euro* (2010).

Evidence. Xue et al., *ACM IMC* (2022); Epifanova / DGAP (2019); Ermoshina and Musiani, *First Monday* (2021); RSF and Meduza (2018); Reuters (Sept. 2024); TAdviser (Jan. 2026); Top10VPN (2022); Novaya Gazeta (Oct. 2024); Human Rights Watch (Mar. 2026); AdGuard DNS (Nov. 2024); The Record (2026); ACF report (2026), opposition-linked, corroborated against the neutral sources above.