ECONSTOR
Make Your Publications Visible.

A Service of

ZBW Leibniz-Informationszentrum Wirtschaft
Leibniz Information Centre for Economics

Payande, Imad; Charkameh, Hadyeh

Article

From .com to .gov: The internet's inevitable nationalist turn

Internet Policy Review

Provided in Cooperation with:
Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin

Suggested Citation: Payande, Imad; Charkameh, Hadyeh (2025) : From .com to .gov: The internet's inevitable nationalist turn, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 14, Iss. 3, pp. 1-8, https://doi.org/10.14763/2025.3.2029

This Version is available at:
https://hdl.handle.net/10419/330349

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.

https://creativecommons.org/licenses/by/3.0/de/deed.en

WWW.ECONSTOR.EU

Mitglied der Leibniz-Gemeinschaft

INTERNET POLICY REVIEW

Volume 14 **Issue** 3

RESEARCH ARTICLE

OPEN ACCESS

From .com to .gov: The internet's inevitable nationalist turn

Imad Payande *Laboratory for Data and Governance Research (D4G-Lab)*
Hadyeh Charkameh *University of Roehampton*

DOI: https://doi.org/10.14763/2025.3.2029

Published: 19 August 2025
Received: 19 July 2025

Funding: The authors did not receive any funding for this research.
Competing Interests: The author has declared that no competing interests exist that have influenced the text.
Licence: This is an open-access article distributed under the terms of the Creative Commons Attribution 3.0 License (Germany) which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. https://creativecommons.org/licenses/by/3.0/de/deed.en
Copyright remains with the author(s).

Citation: Payande, I., & Charkameh, H. (2025). From .com to .gov: The internet's inevitable nationalist turn. *Internet Policy Review*, *14*(3). https://doi.org/10.14763/2025.3.2029

Keywords: Internet shutdown, Digital sovereignty, Cyberwar, Censorship, Iran

Abstract: This essay examines Iran's most extensive internet disruption since 2022, imposed during the June 2025 conflict with Israel, when missile strikes quickly evolved into coordinated cyberattacks on banking, radar, and communications systems. Drawing from direct experience during the blackout, it traces how connectivity collapsed through staged throttling, protocol suppression, and full reliance on the National Information Network. What began as a technical containment strategy also became an improvised shield against foreign intrusion – one shaped as much by sanctions-driven hardware shortages and reliance on insecure gray-market equipment as by military calculus.By situating Iran's shutdown alongside wartime digital restrictions in places like Ukraine, the essay reframes shutdowns as contested acts of defense in a securitised internet. It explores how the shift from an open, decentralised network toward nationalised, politically bordered infrastructures is accelerating under the pressures of war, sanctions, and private platform power. Ultimately, it argues that the "state of exception" once theorised by Schmitt and Agamben is becoming the default operating mode online, eroding universal digital rights. In such moments, ideals like internet freedom survive only if continuously defended and reinvented, even when survival demands compromises unthinkable in peacetime.

I. When war turns the internet into a state of exception

On June 23, as the nationwide internet blackout entered its second week following the June 13 Israeli strikes and subsequent cyberattacks, a friend studying abroad messaged me[1] in distress: she hadn't heard from her mother in Iran for days, just two brief phone calls, each under four minutes. Her mother, in her sixties, couldn't configure Telegram proxies or navigate blocked URLs. That day, I spent hours trying to get a single Google Meet link to her, but domestic messaging apps blocked it, and SMS failed. Meanwhile, another friend was on the phone, dictating a 100-character VPN configuration, letter by letter, to his father-in-law in a village in Zanjan. But the damage didn't stop at strained communication. The blackout seeped into every layer of society, dragging entire livelihoods into uncertainty. I watched as most businesses stalled, their teams paralysed without stable access. Startups that once thrived on internet operations went dark overnight. Friends and colleagues messaged me in frustration, trying to coordinate very basic tasks, like managing servers or responding to clients, none of them possible.

This scene played out just days after Israel launched a series of strikes inside Iranian territory on June 13, 2025. Four days later, the battleground had turned digital: On June 17, a series of coordinated cyberattacks targeted Iran's banking systems, radar infrastructure, and internal communications. In response, the government of Iran enacted the most comprehensive internet disruption since 2022. The mechanics were familiar: DNS injections, national routing protocols, selective throttling, and full reliance on the National Information Network. In form, it resembled the infrastructural censorship deployed during the 2022 protests, when authorities in Iran shifted from brute-force blackouts to subtler, systemic controls. But this time, it wasn't the protest that triggered the darkness. It was war. A calculated wartime shutdown, engineered to seal digital borders in the face of foreign sabotage.

This shift made me confront a fundamental question: How long can we defend the ideals of internet freedom and democratic openness in times of extreme crisis? When critical infrastructures are militarised and digital lifelines become targets, states, whether democratic or authoritarian, face excruciating choices. Carl Schmitt once argued that the sovereign is the one who decides on the exception. Today, I've come to see that the exception is no longer an anomaly; it is the operating logic of a securitised internet. As philosopher Giorgio Agamben warned, we now live under a "state of exception" that has become the dominant paradigm of rule. In a war of existential threat, the first casualties are our normal legal norms, be-

1. All statements made in the first person singular refer to Imad Payande.

cause necessity knows no law. In this situation, I witnessed that the ideal of an open internet is sacrificed in the name of survival.

II. The great shift: From open commons to nationalised networks

The internet, once a borderless haven of free expression and global connection, is currently undergoing a radical reconfiguration. What began as a Cold War experiment in resilient communication, has, over the decades, evolved into the nervous system of the global economy, information flows, and political life. Yet under the pressure of war, sanctions, and the geopolitics of digital infrastructure, I see an accelerating shift: from a decentralised, open-ended architecture (".com") to a state-centered, securitised, and politically bordered infrastructure (".gov").

Authoritarian states are not the only architects of this transformation. While countries like Russia and Iran have led efforts to establish national firewalls, legal controls, and infrastructural centralisation, recent wars have revealed a far more complex and morally ambiguous landscape. For instance, Ukraine has also taken steps to limit mobile connectivity in areas vulnerable to drone activity, attempting to prevent Russian UAVs from exploiting civilian telecom signals. The parliament of Ukraine is considering giving the military real-time shutdown powers in combat zones. Here, internet shutdowns are not tools of repression but acts of tactical defense. As one Ukrainian official put it: "Sooner or later, society will have to decide what is more important: stable internet or safe cities."

This tradeoff reflects the emerging reality of digital sovereignty in wartime, a reality I have come to understand more deeply as conflicts unfold. In such moments, infrastructure becomes dual-use, openness becomes some kind of vulnerability, and civilian networks become military targets. The very features that once made the internet a space of emancipation, resilience, decentralisation, and mobility could now be liabilities in kinetic conflict. Mobile SIM cards, once celebrated for facilitating access, are repurposed by enemy drones. Satellites like Starlink, crucial to Ukraine's military coordination, also raise critical questions about private power and growing public dependence. What does it mean when a sovereign nation must rely on a billionaire's bandwidth to survive? These are not merely rhetorical questions; they have become real dilemmas for governments facing the weaponisation of digital infrastructure. It's precisely these challenges that, in my view, are driving many countries, almost inevitably, toward embracing digital sovereignty both as a concept and a practice.

III. Iran's blackout: The anatomy of a digital siege

According to data from Cloudflare Radar, Iranian internet traffic dropped sharply between June 14 and June 18 (see Figure 1). This decline occurred in three stages: an initial wave of soft throttling and partial restrictions, followed by a near-total blackout, and finally a gradual, phased return.

On June 13, HTTP/2 and HTTP/3 protocols still dominated traffic flows. It indicates a relatively modern network aligned with global standards. But by June 15, while the volume of HTTP requests increased dramatically, which suggests users were urgently trying to access information, the actual data transferred dropped sharply. This discrepancy points to deliberate throttling at the application and transport layers, likely via Deep Packet Inspection (DPI). HTTP/3, the most secure and speed-optimised protocol, was rapidly suppressed. Based on the fifth report on the quality of the internet in Iran, published by the Tehran Electronic Commerce Association, a source close to the government indicated that a formal decision had been made to block HTTP/3 and IPv6 nationwide.

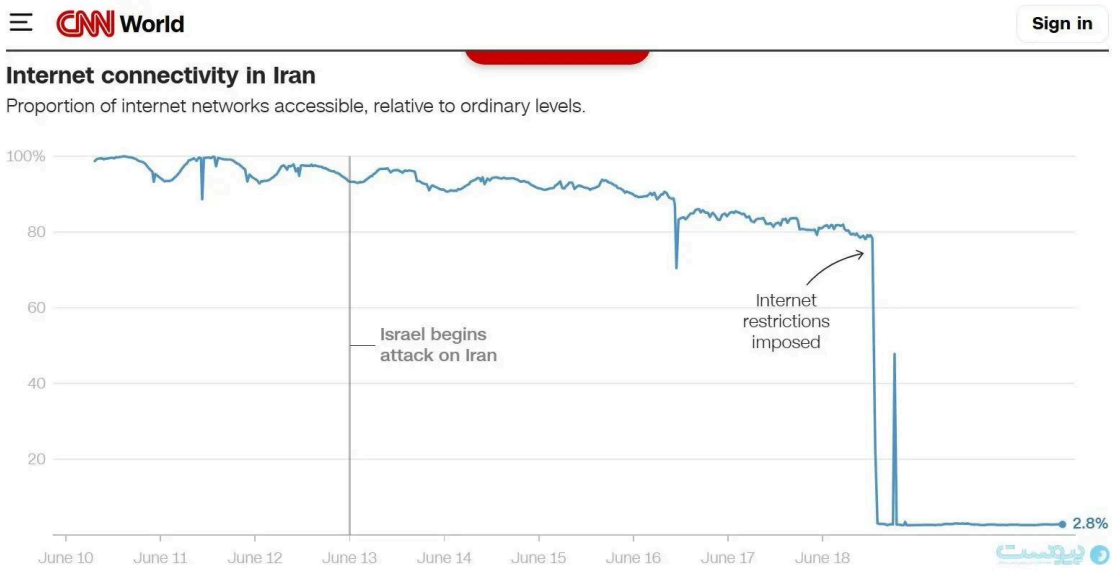

FIGURE 1: Internet access in Iran dropped to 2.8% after Israel's June 13 attack and state-imposed restrictions. (Source: CNN World based on Cloudflare Radar).

The blackout reached its peak on June 18. Less than 3% of Iranian users had access to the global internet (see Figure 2). In such a situation, internal services such as banking apps and domestic platforms remained partially operational through the National Information Network, but external connectivity ceased entirely. However, there were a few exceptions, like foreign diplomatic centers, Starlink users, or elite organisations with dedicated infrastructure.

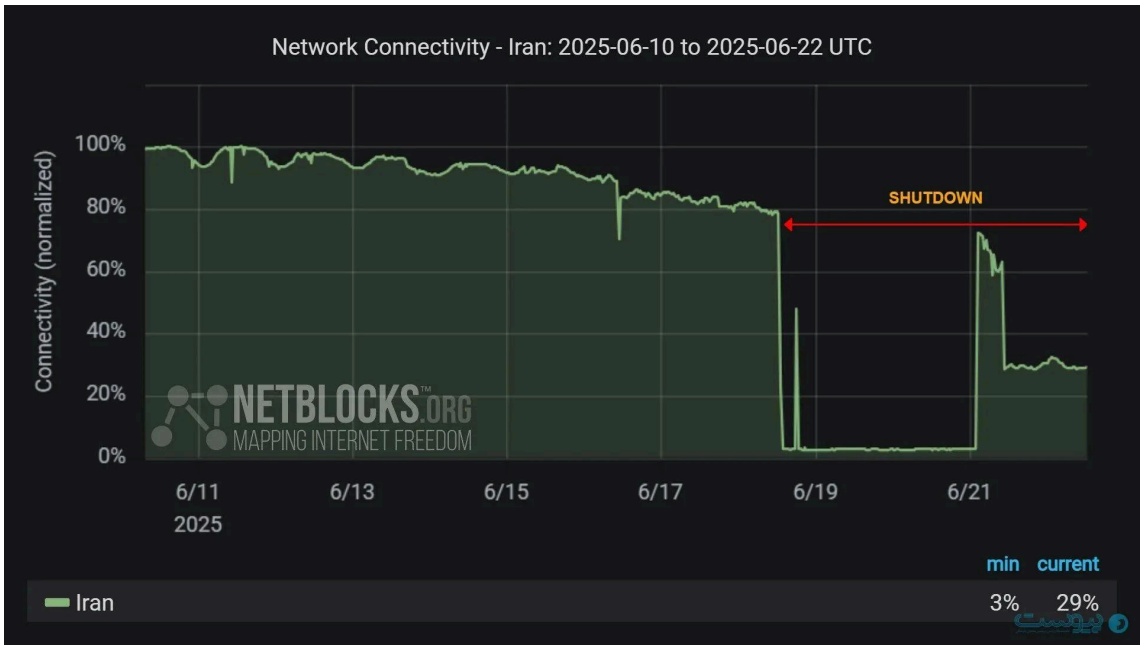

FIGURE 2: NetBlocks data illustrates a nationwide connectivity collapse in Iran beginning June 18, 2025, with levels dropping to just 3% of normal traffic.

After all this, the reopening was controlled and gradual, not sudden or immediate. On June 19, traffic began to rise again selectively. Fixed-line operators in low-risk areas were prioritised. Protocols were rolled back to HTTP/1.x, favoring simplicity and traceability over speed and security. Cloudflare data from June 20–21 shows that while internet traffic began to recover, it remained far below normal levels, which points not to a full shutdown, but to severe throttling that heavily restricted access (see Figure 2).

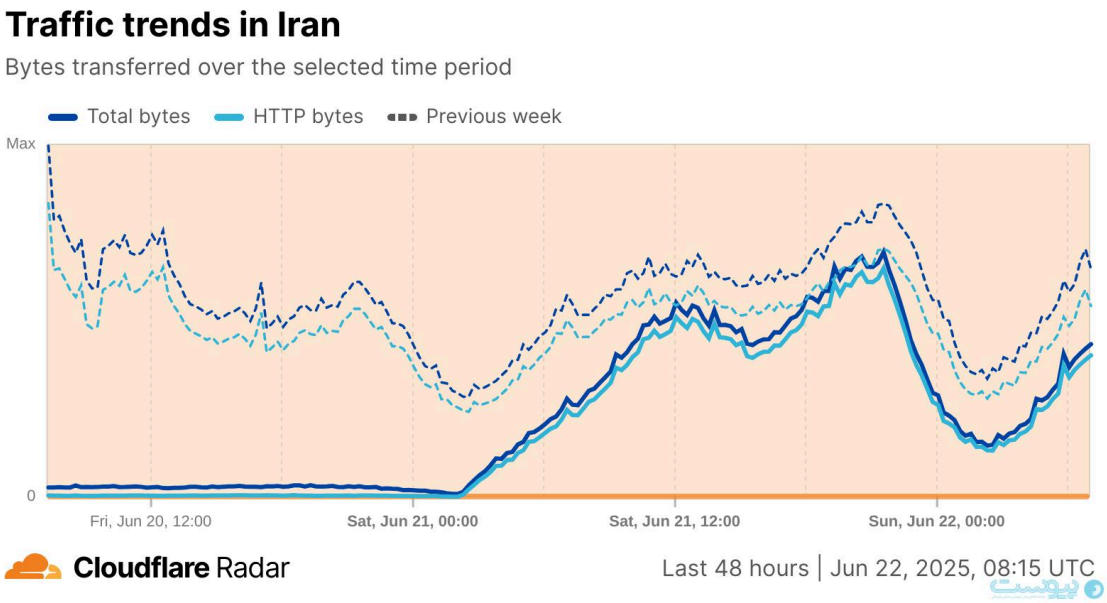

FIGURE 3: Cloudflare data shows a sharp drop in total and HTTP traffic in Iran on June 20–21, 2025, with usage far below the previous week's levels, evidence of protocol-level throttling rather than full blackout.

The result was a fractured internet experience, tailored to maximise state oversight. Fanap Telecom remained heavily restricted, while Irancell and AsiaTech showed signs of recovery only by June 26. Mobinnet, by contrast, lagged behind, operating at 30% of prior capacity.

By July 4th, traffic levels had largely recovered, but users continued to report erratic speeds, severe VPN disruptions, and persistent DNS resolution failures. The network, though technically "online," remained unstable; its architecture still felt like it bore the scars of Israel's cyberattacks. In truth, the internet had returned, but not the one that users remembered. Not the one they could trust.

The shutdown was framed as a necessary move to protect critical systems. These ranged from the power grid and transportation networks to data centers vulnerable to DDoS and intrusion attacks. The blackout went beyond technical containment. It is also intended to preserve operational secrecy by limiting open-source intelligence (OSINT) leaks, managing internal instability, and controlling the flow of information.

But from where I stand, the challenges run deeper than just strategic defense. Sweeping sanctions have cut off access to trusted global vendors. As a result, Iran must rely on gray-market equipment – often smuggled, second-hand, or unsupported, riddled with altered firmware and hidden backdoors – that is often outdat-

ed and full of security flaws. Having watched these developments unfold, I can't help but see how these structural limitations, imposed under the guise of international pressure, have quietly chipped away at Iran's digital defenses. It's painfully clear to me that it is through these cracks that hostile cyber actors, many linked to Israel's covert networks, have launched their most damaging intrusions. In trying to build resilience, Iran has been pushed toward isolation; yet ironically, this very isolation seems to have only made it more vulnerable.

IV. Between repression and necessity

The impacts of sanctions are often invisible, and their true costs remain unseen. They frequently accelerate a nationalist turn in internet governance. In Iran and other sanctioned countries like Russia, access to updates, cybersecurity patches, and foreign digital services has often been restricted. This has led to hardware decay, migration of tech talent, and increased vulnerability to cyberattacks. Yet even amid these pressures, these governments double down on isolationism and promote domestic messengers and platforms that often fail to meet today's internet users' expectations or resilience standards.

Among these, Russia has taken a particularly formalised approach. The so-called "Sovereign Internet Law" mandates that ISPs route all traffic through Roskomnadzor-controlled nodes. In practice, this enables region-specific shutdowns, content filtration, IMEI tracking, and the deployment of national DNS and messaging alternatives. Although the rhetoric is one of security, the practice merges information warfare, censorship, and performative sovereignty.

This pursuit of digital control, however, comes with reciprocal consequences. In 2024, Russia began forcing international hosting companies to follow strict local rules, prompting providers like Germany's Hetzner to pull out of the country. Meanwhile, EU sanctions after the Ukraine invasion banned Russian state media like RT and Sputnik, requiring ISPs to block access. In response, some Western news sites have also restricted Russian users through geo-blocking. The result is a steadily fragmenting internet, shaped as much by global retaliation as by domestic control.

This is not merely a story of repression. From what I have observed, it is also one of desperation, improvisation, and survival. The nationalist turn is not always a result of authoritarian ambition; I believe it can emerge from political fragility. The tragedy is not that the internet has borders. It always had them in its protocols, IP allocations, and centralised naming systems. The tragedy is that we mistook its early openness as permanence, rather than as a temporary byproduct of U.S. mili-

tary liberalism. As missile strikes meet metadata**,** I find myself confronting a hard truth: the internet was never truly borderless. It only looked that way until the wars began.

V. Rights without shelter

Internet shutdowns undeniably restrict freedom, amplify state propaganda, and violate human rights in many ways. Yet, the harsh realities of modern conflict complicate the moral clarity often assumed in digital rights debates.

For countries like Iran, under siege both from within and without, resisting cyberattacks while navigating the consequences of international sanctions presents a cruel dilemma. In my experience, the universal ideals of internet freedom and openness, forged in times of peace, begin to falter in the face of exceptional threats. During the 12-day war, even vocal critics of censorship I spoke to found themselves grappling with uneasy questions: Can any society afford to keep its digital windows open when missiles fly and servers burn?

In those days, survival demanded compromises unimaginable in peacetime. The open internet was sacrificed not out of loyalty to state control but from desperation, as banks, public services, and daily life came under attack, making the National Information Network the only fragile lifeline. Cyberattacks exploited backdoors, compromised patches, and manipulated licenses, pushing Iran into what Agamben calls a "zone of indetermination," suspended between democracy and absolutism. Here, internet freedom ceased to be a universal guarantee, reduced to a conditional offering shaped by power. When no state can or will uphold basic rights, the individual – stripped to bare life – remains exposed to both external assault and internal domination. Under siege, even the most deeply held ideals unravel, surviving only through relentless defense and reinvention.

Published by
Alexander von Humboldt Institute for Internet and Society
CAIS Research for the Digital Age
in cooperation with
CREATe
cnrs centre internet et societe
UOC R&I IN3 Internet interdisciplinary Institute Universitat Oberta de Catalunya
University of Tartu Johan Skytte Institute of Political Studies