RONDELI FOUNDATION

GEORGIAN FOUNDATION FOR
STRATEGIC AND INTERNATIONAL STUDIES

# POLITICAL CHALLENGES AND CURRENT THREATS OF INTERNET FRAGMENTATION

VLADIMER SVANADZE

EXPERT OPINION 221

საქართველოს სტრატეგიისა და საერთაშორისო ურთიერთობათა კვლევის ფონდი
GEORGIAN FOUNDATION FOR STRATEGIC AND INTERNATIONAL STUDIES

# EXPERT OPINION

VLADIMER SVANADZE

## POLITICAL CHALLENGES AND CURRENT THREATS OF INTERNET FRAGMENTATION

221

2024

The publication is made possible with the support of the US Embassy in Georgia. The views expressed in the publication are the sole responsibility of the author and do not in any way represent the views of the Embassy.

Technical Editor: Artem Melik-Nubarov



ISSN 1512-4835
ISBN

## Introduction

The positive process of rapid development of the Internet and Internet technologies is accompanied by certain risks that pose a threat to the unity and security of the global Internet network, its stability and sustainable growth.

Although the unity, security, and stable development of the global Internet are important issues acknowledged by countries within the United Nations framework, some nations persist in creating a national-level Internet policy. This policy aims to control both domestic and external users of the Internet space, seeking to gain an advantage at the international level in using the Internet space as a tool of enforcement. This approach contributes to the fragmentation of the Internet into distinct parts, posing obstacles to its unity and stability.

The article aims to demonstrate the political influence of individual countries on Internet fragmentation and, consequently, the potential threats such fragmentation poses to the unity, security, and stable development of the global Internet.

To begin, when addressing the unity, security, and stability of the global Internet network, it is essential to reference the Internet Governance Forum (IGF) convened by the Secretary-General of the United Nations. This forum was preceded by the adoption of the Tunis Agenda for the Information Society in 2005, which played a pivotal role in shaping the discourse.

The agenda notably defined the term “Internet governance” and acknowledged the collaborative involvement of stakeholders in various capacities. Specifically, the Tunis Agenda for the Information Society states, “Internet governance is the development and application by governments, the private sector, and civil society of their roles, common principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet” (Tunis Agenda for the Information Society, 2005).

It should be noted here that Paragraph 72 of the Tunis Agenda establishes the mandate of the Internet Governance Forum, the first section of which is formulated as follows:

a) ***Discuss public policy issues related to key elements of Internet governance in order to foster the sustainability, robustness, security, stability and development of the Internet*** (Paragraph 72 of the Tunis Agenda, 2005).

The United Nations General Assembly recognizes the importance of the Forum in promoting the sustainability, unity, resilience, security, stability and development of the Internet.

**Forms of Internet Fragmentation**

The escalating use of the Internet and its technologies has heightened its significance and dependence on it. Furthermore, the Internet, and cyberspace in general, have encountered a new threat, namely the establishment of complete control by individual autocratic governments and the rise in cybercrimes. These challenges disrupt the unity and stability of the Internet, jeopardizing its secure and consistent developmental process. This situation is at odds with the Tunis Agenda adopted by the United Nations Assembly.

In recent years, there has been a rising concern that the Internet is at risk of disintegrating into loosely connected fragments. Several disconcerting trends, spanning technological development, Internet policy, and the commercial activities of states, along with the current international situation, permeate the Internet network across its distinct layers, influencing what is termed "Internet fragmentation." However, it is important to note that there is still no widespread understanding of what constitutes "fragmentation," or what risks it poses to the integrity, stability, and security of the Internet, commonly referred to as cyberspace.

This raises the question: What is "Internet fragmentation," and how can this term or practice be defined? Internet fragmentation, also known as the Splinternet, stands in stark contrast to the open, secure, and stable globally unified Internet that we currently enjoy. It refers to the division of the Internet into isolated networks controlled by governments and corporations.

Moreover, considering recent global events linked to ongoing hostilities and conflicts, the Internet space is increasingly susceptible to physical disruptions. This directly jeopardizes the unity, security, and stable development of the Internet.

By definition, there are three well-known forms of Internet fragmentation:

1. **Technical Fragmentation**: Conditions in the underlying infrastructure that impede the ability of systems to fully interoperate and exchange data packets, and the normal functioning of the Internet;
2. **State/Governmental** fragmentation: Internet policies and actions undertaken by governments of individual countries that aim to limit or prevent certain uses of the Internet, particularly concerning the creation, distribution, or access to information resources;
3. **Commercial fragmentation**: Business practices that constrain or prevent certain uses of the Internet to create, distribute, or access information resources (Komaitis, 2023, 7).

Here, we can include political fragmentation as a fourth type of Internet fragmentation. This form emerges as a consequence of the internal and external Internet policies of various governments, military actions, and the overall unstable global or regional situations. Political fragmentation poses a threat to the unity, security, and stable development of the Internet. Some also categorize it under the term “state fragmentation.”

**Political challenges and current threats of Internet Fragmentation**

When examining each type of Internet fragmentation, various problematic categories and associated forms of fragmentation are considered. However, in this current discussion, greater emphasis is placed on the fourth presumed form of Internet fragmentation, which is intricately linked to national or global security. This form is a direct outcome of the influence exerted by the internal and external Internet policies implemented by individual governments. The focus of this discussion extends broadly to its implications on the unity, stability, and security of the Internet, commonly referred to as cyberspace. This ongoing process significantly contributes to the division of the Internet into fragments, thereby causing the fragmentation of the Internet space.

The article discusses Internet fragmentation, using three countries - China, Russia, and Iran - as examples. All three nations share a similar political or governance system, resulting in nearly identical approaches to ensuring the unity and stability of the Internet. According to current statistics (Duarte, 2023), China leads globally in terms of Internet usage, boasting over one billion users. Russia follows, with more than 130 million Internet users, securing the sixth position, while Iran ranks sixteenth with around 70 million users.

Beyond their political similarities and substantial Internet user base, these countries share a third noteworthy factor: Their active engagement in the Internet and cyberspace, especially concerning global Internet connections. International projects involving fiber-optic cables traverse all three nations. Importantly, the disconnection of any of these countries from the global Internet space would have severe consequences, jeopardizing the unity of the Internet.

*Russia-Ukraine War and Russia's Internet Policy*

When discussing such fragmentation, the conversation often centres around the Russia-Ukraine war and its significant impact on the cyberspace domain. Following the Russian invasion of Ukraine, there emerged a looming threat of Russia being isolated from the global Internet. Although this separation did not materialize, the current war may signify the onset of a more profound fragmentation of the global Internet.

The Law on "Internet Sovereignty" established a distinctive legal foundation pertaining to inclusion and exclusion from the global Internet. Under this law, the Russian government mandates Internet service providers to route traffic through exchange points sanctioned by the federal agency Roskomnadzor (Роскомнадзор).

Additionally, the law grants the same agency the authority to enforce Internet service providers to channel traffic through specialized blocking systems that authorities can utilize to filter and redirect traffic at their discretion (Stokel-Wallker, 2022). Furthermore, since 2021, Russian Internet providers have been obliged to have the capability to handle requests to domain name systems and servers situated within the country. In the event of disconnection from the global Internet network, they will be able to locate and process Internet resources. It is difficult to predict how these systems will operate in reality. Still, the fact is that implementing an

autonomous segment, serving as an alternative analogue to a significant portion of the functions of the global Internet, poses greater technical challenges than political ones.

In response to Russia's military aggression, Ukraine sought to disrupt Russia's connections to the global Internet, thereby restricting its capacity to respond to domestic demands. For this purpose, Ukraine submitted a letter to the Internet Corporation for Assigned Names and Numbers (ICANN), the entity overseeing domain name systems, requesting the cancellation of Top-Level Domains (TLDs) issued in the Russian Federation (such as ".ru," ".рф," and ".su") and the disconnection of DNS root zone servers situated in Russia.

The Ukrainian authorities also appealed to the Regional Internet Registry Network Coordination Center (RIPE NCC) to annul Russian Internet addresses (Campbell, Gahnberg, 2022). However, both organizations rejected Ukraine's requests, and underscored the significance of their neutrality in overseeing the technical aspects of the Internet so as to preserve its global and interoperable nature.

Indeed, Ukraine's appeal could establish a precedent for the intertwining of foreign policy and technical administration, potentially undermining the role of these institutions as universally legitimate governing bodies of the Internet space (Campbell, Gahnberg, 2022). It can be said that the disappearance of global consensus on the technical management of the Internet may give rise to new competing institutions, posing fresh challenges and heightened risks to the unity and stable development of the Internet. This process would further contribute to the fragmentation of the Internet.

In fact, since the Russian invasion of Ukraine, the country has yet to be disconnected from the global Internet. The war highlights the great temptation for states to use the technical control they have over the Internet, and the entire infrastructure of the Internet, as a tool of enforcement, helping them to achieve their state goals and gain advantages at the international level. It can be said that the Russia-Ukraine war and the wider geopolitical conflict surrounding it amplify and give a big push to the process of deepening fragmentation of the global digital connection and to making it more fundamental.

*The Iranian Government's Approaches to Internet Control*

When discussing the establishment of control over Internet infrastructure, it is essential to highlight the approaches adopted by Iranian authorities, which essentially reflect political decisions. These actions contribute to certain harm to the unity, security, and stable development of the global Internet, exerting an even greater impact on the ongoing process of Internet fragmentation.

From 2005 to date, cyberspace control in Iran has intensified significantly. Censorship rules have seen a sharp escalation, leading to the blocking of numerous websites. The government has implemented stringent measures to control bloggers, consistently imposing restrictions on their activities. During this timeframe, the concept of establishing a national Internet emerged, facilitated following the impactful cyber-attack on Iran's energy system, known as "StuxNet."

The incurred damage once again prompted the Iranian government to conclude that the creation of a national Internet and the reinforcement of its cyberspace was imperative. The initiative commenced in 2013, with a focus on developing and fortifying the internal infrastructure for banking and financial transactions. Moreover, with government financial backing, alternative domestic social networks were created as substitutes for international platforms. This development has contributed to the government's efforts to exert control over its population in the virtual space. Consequently, in the current Iranian context, access to international social networks has been minimized, leading to the development of national alternative online platforms supported by the government.

*China's Internet Policy and the Great Firewall*

Alongside the expansion of cyberspace capabilities, China's interest in this domain has grown, and exploration of the virtual world has come to assume a prominent position on the country's agenda. In 2015, the Chinese government introduced a new plan concerning its Internet policy, envisioning the nation's economic and technological advancement through cyberspace. An important aspect is that the Chinese media established a new channel dedicated to criticizing the government and addressing existing corruption, prompting the government to respond with substantial institutional changes. Specifically, a regulatory framework was instituted in the country that intended to oversee the media and tighten control over the

Internet space, with special emphasis placed on monitoring both traditional and online radio outlets. A considerable number of Chinese Internet users departed from public online platforms, seeking new alternatives where their voices could be more freely expressed. The government deleted dozens of active political Internet groups and implemented much stricter controls on those supporting liberal ideas.

In August 2014, a new law was introduced, mandating all users to fill in personal data in the registration form on online platforms. According to this law, companies hosting websites for registered users were required to promptly verify the provided information before granting access to the user. They were also mandated to monitor all public accounts and categorize them based on the information provided. Additionally, China extended its control beyond its citizens, imposing restrictions on Internet platform access for foreign nationals, who are required to undergo a lengthy and intricate registration process, during which they must submit their personal information for stringent verification by a dedicated team in the country. Indeed, the Internet policy of the Chinese government aims at partial isolation from the global Internet space, and is known as the "Great Firewall" (Stokel-Wallker, 2022). Despite this, China harbours significant ambitions. When examining its international activities, it becomes apparent that there is a substantial amount of Chinese investment in the Internet space today. An intriguing development is Beijing's plan to lay underwater cables on both the west and east coasts of Africa, facilitating Internet access for the region.

It is noteworthy that China, in actively designing its own national Internet space, is initiating the process of Internet fragmentation; creating a fragmented cyber landscape through its actions, aiming at becoming a dominant country using Internet technologies. All this threatens the unity, security and stable development of the global Internet, and clearly contributes to the process of fragmentation of the Internet.

**Conclusion**

The article explores the threats associated with political influence on Internet fragmentation, citing examples of Internet policies and approaches in Russia, China, and Iran. The Internet policies of these nations primarily revolve around stringent control over both domestic and international Internet users. Additionally, they leverage the Internet as an enforcement

tool for asserting influence at the global level, posing threats to the unity, security, and stable development of the global internet. Notably, these are critical concerns that find consensus among nations within the framework of the United Nations. Consequently, this contributes to the ongoing process of dividing the Internet into separate parts: its fragments.

The article, with the example of the ongoing Russia-Ukraine war, further highlights the deepening of the Internet fragmentation process as escalated by the ongoing hostilities. This escalation results in the physical damage and destruction of Internet connections and associated technologies, leading to the disconnection of local or national Internet networks from the global Internet—a clear manifestation of fragmentation.

The ongoing hostilities also present a direct threat to international fiber-optic cable Internet projects, introducing another dimension to the contributing factors of Internet fragmentation. Given the persisting conflicts in the Black Sea region, it is particularly noteworthy for us to monitor the implementation of similar projects in which Georgia is directly involved and actively participates.

Generally speaking, it should be noted that suspending the process of Internet fragmentation is a challenging task, but it can be achieved through high-level meetings, focused dialogues, and concerted efforts between states addressing the primary factors causing fragmentation, such as cyber espionage, attempts to impose control over Internet infrastructure, and the utilization of Internet technologies as enforcement tools against countries and people.

The interesting statement of the President of the Internet Corporation for Assigned Names and Numbers, on global threats arising from Internet fragmentation should be considered. According to the latter, “The Internet is a single network with a flexible infrastructure, and its fragmentation or attempt to regulate it will lead to its collapse, and this danger is inevitable and real” (Costerton, 2023).

Indeed, this is a warning directed towards the United Nations, whose initiative, through the establishment of the Internet Governance Forum, laid the foundation for ensuring the sustainability, unity, resilience, security, stability, and development of the Internet.

## Bibliography


1. World Economic Forum. 2024. “Global Cybersecurity Outlook 2024.” Insight Report. January, 2024; https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf
2. Duarte, Fabio. 2023. “Countries with the Highest Number of Internet Users (2024).” *Exploding Topics*, November 22, 2023;
3. Svanadze, Vladimer. 2023. “Challenges of Internet Fragmentation and Global Cyberspace.” *Scientific and practical cyber security journal – SPCSJ* № 4 vol. 07, December 2023;
4. Svanadze, Vladimer. 2023. “Cyber Security and the Academic Sector.” *Scientific and practical cyber security journal – SPCSJ* № 4 vol. 07, December 2023;
5. Sullivan, Andrew. 2023. “Misguided Policies the World over are slowly killing the Open Internet”, *Internet society.* 2023;
6. Svanadze, Vladimer. 2023. “Cybersecurity Policy and Strategy of Management.” PhD diss., Georgian Technical University (GTU), Tbilisi.
7. Carnap, Kai Von. 2023. “Fragmentation the Internet-Beyond and Within the Great Firewall.” *MERICS-Mercator Institute for Chinese Studies*, 2023;
8. Meinel, Christopher. 2023. „Russia’s War Against Ukraine is Catalyzing Internet Fragmentation.“ *Council on Foreign Relations*. 2023;
9. Komaitis, Konstantions. 2023. “Internet Fragmentation: Why It Matters for Europe.” *This publication has been produced in the context of the EU Cyber Direct – EU Cyber Diplomacy Initiative project with the financial assistance of the European Union*;
10. Svanadze, Vladimer. 2022. “New Challenges of Cyberspace and Georgia”. ISBN 978-9941-9708-1-8, University of Georgia Press;
11. Tatiana Tropina. 2022. “Internet Fragmentation: What’s at Stake?” *Center for Global Cooperation Research*. November 2022;
12. Stokel-Wallker, Chris. 2022. “Russia Inches Toward Its Splinternet.” https://www.wired.co.uk/article/russia-splinternet-censorship;
13. Weyrauch, David, and Winzen, Thomas. 2020.”Internet Fragmentation, Political Structuring, and Organizational Concentration in Transnational Engineering Networks.” *Global Policy*. October 2020;
14. Drake J. drake, Cerf Vinton G., and Kleinwachter, Wolfgang. 2016. “Internet Fragmentation: An Overwiev.” *World Economic Forum, Committed to improving the State of the World*. 2016.