Impact of Internet Fragmentation on the Unity, Security, and Stability of Global Internet

Vladimer Svanadze[1] and Maksim Iavich[2]

[1] *Caucasus University, 1 Paata Saakadze str., Tbilisi, 0102, Georgia*
[2] *Georgian Technical University, 68 Merab Kostava str., Tbilisi, 0108, Georgia*

Abstract

The deepening process of fragmentation has become a new challenge for the unity, security, and stable development of the global Internet. That is, it can be said that the Internet is in danger of disintegrating into separate fragments that are weakly connected. Several disturbing trends related to the technological development of the Internet, the Internet policies and commercial activities of individual countries, as well as the current international situation, are called the causes of fragmentation. The process of fragmentation has put the global Internet space in front of a new threat, which is also related to the establishment of total control over it by individual autocratic governments, global ethno-conflicts, and hostilities, as well as increased cybercrimes. All this violates the unity and stability of the Internet and threatens its stable and safe development process. This process also contradicts the Tunisian Agenda adopted by the United Nations Assembly in 2005. Internet fragmentation is a new process and it is a subject of extensive research. This paper briefly reviews the technical, commercial, and governmental forms of Internet fragmentation, and at the same time, focuses on the political aspect of fragmentation. It is the Internet policies and approaches of individual countries that are considered the political part of fragmentation, and in many cases, political fragmentation has an impact on the other three forms of fragmentation. The fact that such global organizations as ICANN and RIPE NCC still manage to maintain an independent position and not turn the issue into a political one deserves attention here because the politicization of the technical management of the Internet represents the danger that may follow the irreversible process of Internet fragmentation. The paper also offers the mathematical model of internet fragmentation. The model can be modified based on the geopolitical landscape and the responses of nations over time.

Keywords

Internet fragmentation, unity, sustainability, robustness, security, stability, development, political, technical, commercial, governmental, policy.

1. Introduction

The positive process of rapid development of the Internet and Internet technologies is accompanied by certain risks, which threaten the unity and security of the global Internet network, its stability, and stable development [1–3].

When we talk about the unity, security, and stability of the global Internet network, we must mention the Internet Governance Forum, convened by the Secretary General of the United Nations, whose work involves all interested parties—public and private sectors, civil society, and representatives of academic circles [4]. It is the best platform where the exchange of ideas, discussion, and sharing of experiences about the processes taking place in the Internet space takes place among interested parties at the global, national, and regional levels [5, 6]. The convening of the Internet Governance Forum by the United Nations was preceded by the adoption of the

CPITS-2024: Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2024, Kyiv, Ukraine
EMAIL: svanadze@gmail.com (V. Svanadze); miavich@cu.edu.ge (M. Iavich)
ORCID: 0000-0001-4122-2536 (V. Svanadze); 0000-0002-3109-7971 (M. Iavich)

Tunisian Agenda for the Information Society in 2005. This included defining the term Internet governance and recognizing that the Internet governance process involves the involvement of stakeholders in different roles [7, 8].

In particular, in the Tunisian agenda for the information society, we read that Internet governance is the development and application by governments, the private sector, and civil society, in their respective roles, of shared 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 Tunisian agenda establishes the mandate of the Internet Governance Forum, the first paragraph of which is formulated as follows:

a) "Discuss public policy issues related to key elements of Internet governance to foster the sustainability, robustness, security, stability, and development of the Internet………."

The United Nations General Assembly recognizes the importance of the Forum in promoting the sustainability of the Internet, its unity, resilience, security, stability, and development. The purpose of the study is to discuss the newly recognized fourth political form of fragmentation, which is related to the Internet policies of individual countries, current military operations, and, in general, the current unstable global and regional situation, which harms the global Internet, its unity, security, and stability. Research shows that the political aspect of Internet fragmentation is a determinant of other forms of fragmentation and is the main form of fragmentation.

The goal of the paper is also to offer the mathematical model of internet fragmentation, which can be modified based on the geopolitical landscape and the responses of nations over time.

2. Forms and Characteristics of Internet Fragmentation

It is the active use of the Internet and Internet technologies that has further increased its importance and dependence on it. In addition, the Internet and cyberspace in general have faced new threats related to the imposition of total control over it by individual autocratic governments, global ethno-conflicts and hostilities, and increased cybercrimes. All this violates the unity and stability of the Internet and threatens its stable and safe development process. This process also contradicts the Tunisian agenda adopted by the United Nations Assembly at the time [9–11].

In recent years, there has been growing concern that the Internet is in danger of disintegrating into loosely connected fragments. Several worrying trends are related to technological development, internet policies, and commercial activities of states, as well as the current international situation. This process extends to the Internet network, and its separate layers, and affects the process, and this is called Internet fragmentation. However, it should be noted that there is still no widespread understanding of what "fragmentation" is and is not, or what risks it poses to the integrity, stability, and security of the Internet, aka cyberspace [12].

This begs the question of what is "Internet fragmentation" and how can this term or practice be defined.

Internet fragmentation, also known as Splinternet, is the opposite of the Internet and means that the open, secure, and stable globally unified Internet that we enjoy is divided into separate, isolated networks controlled by governments and corporations. In addition, to the similar definition of "internet fragmentation", taking into account the recent global events, we can also add hostilities and ethno-conflicts, which already physically damage the unity of cyberspace.

There are the following three 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 of the Internet to function consistently at all endpoints.
2. **Governmental Fragmentation:** Government policies and actions that constrain or prevent certain uses of the Internet to create, distribute, or access information resources.
3. **Commercial Fragmentation:** Business practices that constrain or prevent certain uses of the Internet to create,

distribute, or access information resources.

Each type of Internet fragmentation can be very different along several dimensions [13, 14]. In this case, four main characteristics are distinguished, namely:

- **Occurrence:** whether a type of fragmentation exists or is a potential.
- **Intentionality:** whether fragmentation is the result of deliberate action or an unintended consequence.
- **Impact:** whether fragmentation is deep, structural, and configurative of large swaths of activity or even the Internet as a whole, or rather more shallow, malleable, and applicable to a narrowly bounded set of processes, transactions, and actors.
- **Character:** whether fragmentation is generally positive, negative, or neutral.

Here, as a fourth type of Internet fragmentation, we can add—Internet fragmentation, which we got as a result of the internal and external Internet policies of one or another government, the current hostilities, and in general, the unstable situation globally or regionally, which harms the unity, security, and stability of the global Internet.

This fourth type is called Political Fragmentation, which some refer to as Governmental Fragmentation.

3. Impact of the War in Ukraine on the Political Fragmentation

While discussing each form of Internet fragmentation, different types of problematic categories and types of fragmentation arising from them are considered, however, in this paper, the fourth alleged form of Internet fragmentation, which is related to national or global security, and shows the influence of domestic and foreign Internet policies carried out by individual governments, is discussed more broadly. Consequences for the unity, stability, security, and stability of the Internet itself, cyberspace.

When we talk about this kind of fragmentation, the discussion starts with the Ukraine-Russia war, which has a great impact on cyberspace. There was a threat that Russia would be isolated from the global Internet, which has not happened, but we may be witnessing the beginning of a more fundamental fragmentation of the global Internet [15, 16].

The government of the Russian Federation has ordered Russian website operators to become independent from the global network by March 11, 2022. After Russia has indeed taken effective steps. In particular, the Russian authorities blocked many news sites, banned popular Western Internet services and social platforms, including Facebook, Instagram, and Twitter, and introduced a new law e.g. year "fake news" and disinformation—about spreading propaganda [17].

Despite such repressive actions, Russia has not cut off its connection to the global Internet, although Russia's 2019 law on "Internet Sovereignty" has given all this a peculiar legal basis. This law requires Internet service providers to route traffic through exchange points approved by the federal agency Roskomnadzor. In addition, the law gives Roskomnadzor the right to force Internet service providers to route traffic through special blocking systems, which the authorities can use to filter traffic and route it the way they want. Moreover, from 2021, Russian Internet service companies should be able to process requests to domain name systems, and servers located inside the country, and in case of disconnection from the global Internet network, it will be possible to use Internet resources [18–21].

It is difficult to say how these systems will work in a real situation, although the fact is that an autonomous segment that replicates a large part of the functions of the global Internet is more difficult to realize from a technical point of view than from a political point of view. In any case, Russia's ability to stop data transmission is not an impossible process, and it will not lead to a deterioration in the quality of service. Therefore, such a radical step is unlikely unless the Kremlin deems it necessary to regain control over information or to prevent cyber incidents [22].

Ukraine has attempted to cut off Russia's connections to the global Internet and limited its ability to address domestic demands. To this end, Ukraine sent a letter to ICANN, which coordinates domain name systems, and requested to cancel the top-level domains issued in the Russian Federation (eg, ".ru", ".рф" and ".su") and to withdraw from Russia

Located DNS root servers. Ukrainian authorities also asked RIPE NCC, the regional Internet registry for parts of Europe, the Middle East, and Central Asia, to cancel Russian IP addresses. However, both organizations, ICANN and RIPE NCC, rejected Ukraine's request and, to maintain a global and compatible Internet, emphasized the importance of their neutrality in the technical management of the Internet [23–26].

Ukraine's request would set a precedent for the fusion of foreign policy and technical administration, which in turn undermines the role of these institutions as universally legitimate governing bodies. If the global consensus on the technical governance of the Internet disappears, the emergence of competing institutions will be a new challenge and a serious risk to the unity of the Internet.

Although governing institutions have resisted political orders, increasing control over digital infrastructure will further intensify the process of internet fragmentation. On the other hand, the current process in Ukraine may give a greater impetus to the fundamental fragmentation of the global digital connection, one of the main aspects of which is the politicization of the technical management of the Internet.

A year after the beginning of the war, the country has yet to be disconnected from the global Internet. However, it should be noted that the war highlights the great temptation for states to use their technical control over the Internet and the entire Internet infrastructure as a weapon. Although there were attempts to use total control of cyberspace as a weapon, these attempts were foiled in time. The broader geopolitical controversy surrounding the war is exacerbating the deep fragmentation of global digital connectivity and making it more fundamental [27].

4. Mathematical Model for Internet Fragmentation in Geopolitical Conflicts

Let $I(t)$ represent the Internet Fragmentation Index at time t.

$$I(t)=f(TC(t),LM(t),GC(t),CP(t),P(t)) \quad (1)$$

$TC(t)$ represents the technical control exerted by a government at time t. Considering the factors such as autonomous systems, domain control, and filtering mechanisms.

$LM(t)$ represents the legal measures in place at time t, including parameters for content censorship, information control laws, and legal restrictions.

$GC(t)$ denotes the level of global cooperation at time t. It gives the opportunity to measure adherence to international standards, cooperation in Internet governance, and participation in global initiatives.

$CP(t)$ reflects the cybersecurity practices implemented at time t, considering parameters such as the robustness of cybersecurity infrastructure and the effectiveness of measures against cyber threats.

$P(t)$ captures the geopolitical context at time t, Including indicators for ongoing conflicts, diplomatic tensions, and geopolitical events.

The factors can be combined using weighted coefficients:

$$I(t)=w_{TC}TC(t)+w_{LM}LM(t)+w_{GC}GC(t)+ \\ +w_{CP}CP(t)+w_{P}P(t) \quad (2)$$

We must ensure that the weights satisfy the following formula for the normalization:

$$w_{TC}+w_{LM}+w_{GC}+w_{CP}+w_{P}=1 \quad (3)$$

It is also very important to consider the model incorporating dynamics over time:

$$I(t+1)=\alpha I(t)+\beta \Delta I(t) \quad (4)$$

Where α represents a decay factor, and β represents the impact of recent changes $(\Delta I(t))$ on the overall index.

This dynamic model allows for an evolving representation of Internet fragmentation. The changes must be considered based on the geopolitical landscape and the responses of nations over time [28–30].

5. Conclusions

On the example of the Ukraine-Russia war and the Internet policy of Russia, the paper discussed the political aspect of Internet fragmentation, which is one of the main forms of fragmentation, which, determines other forms of fragmentation [31, 32].

Taking into account the current reality, which is related to the Internet policies and approaches of individual countries, it can be assumed that Internet fragmentation is an irreversible process. However, at the same time, it should be noted the need for the efforts of the global community, which is related to the public welfare, the unity, security, and stability of the Internet.

As part of the work on the Global Digital Treaty, which should be agreed upon in September 2024, the global and inclusive process of developing common principles for the digital space continues. This is an opportunity to recognize the global Internet as an important tool for solving common problems. In general, it should be noted that stopping the process of fragmentation of the Internet is a difficult task, but it can be done through high-level meetings between states, focused dialogues and efforts on the main fragmenting factors, such as cyber espionage, attempts to impose control over Internet infrastructure, and the use of the Internet and Internet technologies as weapons against countries and people.

Finally, according to ICANN president Sally Costerton, "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." This warning was directed at the United Nations. It was at the initiative of this organization that the Internet Governance Forum, created at the time, laid the foundation for the sustainability of the Internet, its unity, durability, security, stability, and development.

References

[1] P. Anakhov, et al., Increasing the Functional Network Stability in the Depression Zone of the Hydroelectric Power Station Reservoir, in: Workshop on Emerging Technology Trends on the Smart Industry and the Internet of Things, vol. 3149 (2022) 169–176.

[2] K. Khorolska, et al., Application of a Convolutional Neural Network with a Module of Elementary Graphic Primitive Classifiers in the Problems of Recognition of Drawing Documentation and Transformation of 2D to 3D Models, J. Theor. Appl. Inf. Technol. 100(24) (2022) 7426–7437.

[3] Y. Sadykov, et al., Technology of Location Hiding by Spoofing the Mobile Operator IP Address, in: IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (2021) 22–25. doi: 10.1109/UkrMiCo52950.2021.9716700.

[4] Z. Brzhevska, et al., Analysis of the Process of Information Transfer from the Source-to-User in Terms of Information Impact, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3188 (2021) 257–264.

[5] P. Anakhov, et al., Evaluation Method of the Physical Compatibility of Equipment in a Hybrid Information Transmission Network, J. Theor. Appl. Inf. Technol. 100(22) (2022) 6635–6644.

[6] M. TajDini, V. Sokolov, P. Skladannyi, Performing Sniffing and Spoofing Attack Against ADS-B and Mode S using Software Define Radio, in: IEEE Int. Conf. on Information and Telecommunication Technologies and Radio Electronics (2021) 7–11. doi: 10.1109/ UkrMiCo52950.2021.9716665.

[7] V. Svanadze, Doctoral Thesis "Cyber-security Policy and Strategy of Management", Georgian Technical University (2023).

[8] V. Svanadze, Near Future of Cyber Security and New Trends in Cyberspace, Global Foundation for Cyber Studies and Research (2020).

[9] R. Jeyaraj, et al., Resource Management in Cloud and Cloud-Influenced Technologies for Internet of Things Applications, ACM Computing Surveys 55(12) (2023) 1–37.

[10] H. Ma, J. Li, An Innovative Method for Digital Media Education Based on Mobile Internet Technology, Int. J. Emerging Technol. Learn. 16(13) (2021) 68–81.

[11] Z. Al-Qudah, et al., On the Stability and Diversity of Internet Routes in the MPLS Era, Performance Evaluation 138 (2020). doi: 10.1016/j.peva.2020.102084.

[12] H. Stacie, D. Lazanski, E. Taylor. Standardising the Splinternet: How China's Technical Standards Could Fragment the Internet, J. Cyber Policy 5(2) (2020) 239–264.

[13] K. Kamaitis, Internet Fragmentation: Why It Matters for Europe (2023).

[14] W. Drake, V. Cerf, W. Kleinwachter, Internet Fragmentation: An Overwiev (2016).

[15] C. Stokel-Wallker, Russia Inches Toward Its Splinternet (2022).

[16] A. Sullivan, Misguided Policies the World Over Are Slowly Killing the Open Internet, Internet Society (2023).

[17] S. Gnatyuk, et al., High-Performance Reliable Block Encryption Algorithms Secured against Linear and Differential Cryptanalytic Attacks, CEUR Workshop Proceedings Vol. 2104 (2018) 657–668.

[18] P. Yu, et al., Design of Security Protection Based on Industrial Internet of Things Technology, International Conference on Measuring Technology and Mechatronics Automation (2022) 515–518. doi: 10.1109/ICMTMA54903.2022.00109.

[19] M. Hadidi, et al., ZigBee, Bluetooth and Wi-Fi Complex Wireless Networks Performance Increasing, Int. J. Commun. Antenna Propagation 7(1) (2017) 48–56.

[20] R. Goswami, et al., Analysing the Functions of Smart Security Using the Internet of Things, 6th International Conference on Contemporary Computing and Informatics (2023) 71–76.

[21] S. Gnatyuk, et al., Method of Algorithm Building for Modular Reducing by Irreducible Polynomial, 16th International Conference on Control, Automation and Systems (2016) 1476–1479.

[22] M. El.zuway, H. Farkash, Internet of Things Security: Requirements, Attacks on SH-IoT Platform, 21st international Ccnference on Sciences and Techniques of Automatic Control and Computer Engineering (2022) 742–747.

[23] M. Iavich, et al., The Novel System of Attacks Detection in 5G, Adv. Inf. Netw. Appl. LNNS 226 (2021) 580–591. doi: 10.1007/978-3-030-75075-6_47.

[24] M. Abdu, A. Murshed, A. Alhammadi, The Principles of Information Security and the Challenges Facing the Internet of Things in Developing Countries, 3rd International Conference on Emerging Smart Technologies and Applications (2023) 1–5. doi: 10.1109/eSmarTA59 349.2023.10293280.

[25] R. Odarchenko et al., Traffic Offload Improved Method for 4G/5G Mobile Network Operator, 14th International Conference on Advanced Trends in Radio-electronics, Telecommunications and Computer Engineering (2018) 1051–1054.

[26] D. Liu et al., Research on Key Technology of Terminal Equipment Security Protection for Energy Internet, IEEE 12th International Conference on Electronics Information and Emergency Communication (2022) 163–167.

[27] M. Iavich, et al., Hybrid Encryption Model of AES and ElGamal Cryptosystems for Flight Control Systems, IEEE 5th International Conference on Methods and Systems of Navigation and Motion Control (2018) 229–233.

[28] J. Brown, Executive’s Cybersecurity Program Handbook: A Comprehensive Guide to Building and Operationalizing a Complete Cybersecurity Program, Packt Publishing (2023).

[29] A. Peleschyshyn, T. Klynina, S. Gnatyuk, Legal Mechanism of Counteracting Information Aggression in Social Networks: from Theory to Practice, CEUR Workshop Proceedings Vol. 2392 (2019) 111–121.

[30] K. Naidu, et al., Analyzing the Function of Smart Security in the Context of the Internet of Things, 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (2023) 423–426.

[31] J. Al-Azzeh, et al., Analysis of Self-Similar Traffic Models in Computer Networks, Int. Rev. Model. Simulations 10(5) (2017) 328–336.

[32] H. Qin, et al., TriBoDeS: A Tri-Blockchain-Based Detection and Sharing Scheme for Dangerous Road Condition Information in Internet of Vehicles, IEEE Internet of Things Journal 11(2) (2024) 3563–3577.