Geopolitical and Technical Dimensions of Internet Fragmentation[⋆]

Vladimer Svanadze[1,†], Maksim Iavich[1,*,†] and Viktoriia Lukashenko[2,†]

[1] *Caucasus University, 1 Paata Saakadze str., 0102 Tbilisi, Georgia*
[2] *National Aviation University,1 Liubomyra Huzara ave, 03058 Kyiv, Ukraine*

Abstract

Internet fragmentation, driven by both technical and geopolitical factors, threatens the unity, security, and stability of global cyberspace. This paper examines the key dimensions of fragmentation, focusing on technical parameters such as network congestion, routing inefficiencies, security measures, and geographical disparities in infrastructure. These factors, combined with the challenges arising from the slow adoption of IPv6 and the geopolitical implications of cyber warfare, contribute to the division of the global Internet. In particular, regional conflicts, such as the Russia-Ukraine war, highlight how military tensions can disrupt critical infrastructure, further isolating networks and exacerbating fragmentation. The paper also discusses potential mitigation strategies, including the adoption of improved routing protocols, acceleration of IPv6 deployment, and increased international cooperation to enhance network infrastructure. The analysis concludes by emphasizing the need for coordinated international efforts to address both the technical and geopolitical dimensions of Internet fragmentation to preserve a secure, open, and interconnected global digital ecosystem.

Keywords

Internet fragmentation, unity, sustainability, security, stability, development, political, technical, commercial, governmental, policy, Internet Governance Forum, IGF, World Economic Forum, WEF, International Security, NATO

1. Introduction

The Internet is a symbol of global stability, security, openness, and unity, facilitating the free flow of information across borders. However, the phenomenon of Internet fragmentation is emerging as a significant and alarming concern, potentially undermining these fundamental principles. While there remains some skepticism about the extent and inevitability of this fragmentation, discussions around the issue have gained prominence at various international forums, including high-level meetings.

One such event, the keynote session on the “Policy Network on Internet Fragmentation” held at the 2024 Internet Governance Forum (IGF) in Riyadh, Saudi Arabia, focused on addressing the fragmentation of the Internet. This session was dedicated to the implementation of Article 29C of the Global Digital Compact (GDC), which emphasizes the importance of international cooperation in preventing the fragmentation of the Internet. Specifically, Article 29C states: “Promote international cooperation among all stakeholders to prevent, identify and address risks of fragmentation of the Internet in a timely manner (SDG 16)” [1].

The panel discussion brought together a wide array of stakeholders, including government officials, technical experts, civil society members, and academic representatives. Their conversations underscored the multifaceted nature of Internet fragmentation, highlighting both its technical and geopolitical dimensions. As Anriette Esterhuysen aptly put it, “Addressing Internet fragmentation requires a concerted effort to view the digital landscape through diverse lenses”. The

[⋆] *CPITS 2025: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2025, Kyiv, Ukraine*
[*] Corresponding author.
[†] These authors contributed equally.

vsvanadze@cu.edu.ge (V. Svanadze); miavich@cu.edu.ge (M. Iavich); viktoriia.lukashenko@kai.edu.ua (V. Lukashenko)
0009-0008-3283-7872 (V. Svanadze); 0000-0002-3109-7971 (M. Iavich); 0009-0009-0458-2590 (V. Lukashenko)

session reinforced that preventing fragmentation is not merely a technical challenge but a deeply human one, necessitating collaboration, research, and ongoing dialogue.

Moreover, Amitabh Singhal highlighted the IGF's unique role in bridging the technical and policy divides, stressing that the renewal of the IGF's mandate would be pivotal in continuing these critical discussions. Given this context, the fragmentation of the Internet demands urgent attention and a multi-dimensional approach to ensure its stability, openness, and global interconnectedness.

*This paper aim*s to examine the causes and consequences of Internet fragmentation, particularly through a dual lens of technical and geopolitical perspectives. The main objectives of this study are:

- To analyze the technical, political, and commercial factors that contribute to the fragmentation of the global Internet.
- To explore the geopolitical implications of Internet fragmentation, particularly the role of regional conflicts and national policies.
- To frame Internet fragmentation within the context of international security and emphasize the need for collaborative, research-driven efforts to mitigate the risks involved.
- To propose practical strategies to preserve the unity of the Internet, including improving infrastructure, enhancing international cooperation, and addressing security challenges.

By addressing these goals, this paper seeks to offer a comprehensive understanding of Internet fragmentation and contribute to the ongoing global discourse on maintaining the Internet as a unified, open, and secure platform.

2. Definition of internet fragmentation and existing challenges

What is Internet fragmentation and how can it be defined? A question that is the subject of discussion among experts is the difference of opinion regarding the division of the Internet into fragments. However, it should be noted that from the rostrum of high-level meetings, we increasingly hear about the threats that are caused precisely by the process of Internet fragmentation and which directly threaten the unity of the global Internet, its stable and secure development, as well as the openness, transparency, and accessibility of the Internet.

An interesting definition of Internet fragmentation is offered by the Internet Society (ISOC), a fairly authoritative Internet organization. Specifically, on the organization's website, we read that "Internet fragmentation is the division or splintering of the unified, open, global Internet into smaller, isolated networks subject to different rules, regulations, and technical standards—which may not be able to interconnect or interoperate seamlessly".

There is also an interesting note there, which leads us to a better understanding of the definition of Internet fragmentation, namely: "The Internet works well because no single person or entity controls it. Anyone can choose to connect to it, and the network grows and adapts to fit our needs. When all this works correctly, our experience of the Internet should be the same no matter who or where we are, because we are all connecting to the same unified, global, seamless Internet". Otherwise, we will be limiting free access to the Internet, violating its unity, which in turn threatens its openness and transparency. All of this will contribute to the process of the Internet breaking up into fragmented parts.

And yet, to better understand the fragmentation of the Internet, the Internet Society (ISOC) provides the following explanation:

- Internet fragmentation is not an event, it is not something that will happen overnight. Instead, it is a process that is in motion in different regions of the world, and being brought about by a variety of policy and business decisions.
- Multiple types of fragmentation will break the Internet. From a user's perspective, people will experience the Internet very differently depending on who and where they are.

- Fragmentation will change the way we experience the Internet. It will disrupt international trade and business, as well as global supply chains. It will disproportionately impact smaller businesses. It will limit people's ability to communicate with friends and family.
- Some policies that may sound reasonable, such as regional DNS resolvers or cost-sharing, actually threaten to fragment the Internet, and it is important to analyze the impact they might have on the Internet and people.

When discussing the definition of Internet fragmentation and its impact on the integrity, stability, and security of the global Internet, we cannot ignore a report commissioned by the World Economic Forum (WEF) in 2016, which identifies the scope of fragmentation according to three categories, reflecting our broad understanding of the global Internet, namely [2]:

- Technical fragmentation—"The 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 end points".
- Governmental fragmentation—"Policies and actions that constrain or prevent certain uses of the Internet to create, distribute or access information resources".
- Commercial fragmentation—"Business practices that constrain or prevent certain uses of the Internet to create, distribute or access information resources".

3. The geopolitical dimension of Internet fragmentation

In general, it can be said that the Internet has its characteristics, which are used to measure the performance of the Internet, its quality, security, stability, etc. Any interference or encroachment on the dimensions of the Internet that make the Internet global, accessible, open, and unified will lead to the fragmentation of the Internet. In particular, we are talking about the technical characteristics of the global Internet and the threats that can lead to the fragmentation of the global Internet.

This process is well described by Konstantinos Komaitis in his focused study "Internet Fragmentation: Why It Matters for Europe". Here I would like to mention just a few of the technical dimensions proposed by Konstantinos Komaitis and the dangers that accompany them. Specifically, according to the author [3]:

- The threat to the Domain Name System (DNS)
  The DNS is the glue that holds the global internet together and is responsible for translating internet protocol (IP) addresses to user-friendly alphanumeric domain names. Management and coordination functions of the DNS are performed by the Internet Corporation for Assigned Names and Numbers (ICANN). Any attempt by any actor to set up alternative root serves apart from ICANN will cause fragmentation; users, where such alternative root servers exist, will be severed from the global internet.
- The slow transition from IPv4 to IPv6 addresses
  The IPv4 address space has been exhausted for quite some time now. If countries do not promote, and businesses do not proceed to, IPv6 deployment, there is a chance that users will not be able to access some new services and apps. We could have an 'IPv6 internet' that is fragmented from the legacy 'IPv4 internet'.
- Internet content blocking and/or filtering
  In the simplest case, some amount of internet fragmentation results from countries' inconsistent filtering of content based on their definition of what constitutes permissible speech. Governments are deploying a variety of technical and legal tools to block websites and platforms and to remove online content. Using tools such as DNS filtering, IP blocking, distributed denial of service (DDoS) attacks, and search result removals, governments are changing the way users connect to and participate in the global internet.

In general, it is difficult to show the exact dimensions and threats of Internet fragmentation. It can be said that this is directly related to the active steps taken by some states that lead to a shift towards globalization, which is directly related to the unity, openness, security, and stability of the global Internet. All this contributes to the development of an ecosystem of Internet fragmentation.

And yet, the question arises whether the fragmentation of the Internet described above, in parallel with its technical dimensions, can also be considered in a geopolitical context as a subject of international security research.

This is a hypothetical question and requires in-depth research. However, it can also be said that the Internet, considered in a national, regional, and global context, is one of the components of international security and this is related to the processes existing in the Internet space, which directly threaten the unity and sustainability of the global Internet space, its security and stability, openness and transparency, as well as the cyber resilience of individual countries and regions. Therefore, when we talk about the threats existing in the Internet space, the process must also be considered in the context of international security. Especially considering that the Internet space has become a serious tool for some states to achieve their goals.

It is also worth noting the recognition made by the North Atlantic Alliance regarding cyberspace, according to which international law also applies to cyberspace and that cyber defense is part of the Alliance's core collective defense task, i.e. the Alliance considers cyberspace as a "domain of operations". In particular, according to paragraph 72 of the Wales Summit Declaration [4, 5]:

- As the Alliance looks to the future, cyber threats and attacks will continue to become more common, sophisticated, and potentially damaging. To face this evolving challenge, we have endorsed an Enhanced Cyber Defence Policy, contributing to the fulfillment of the Alliance's core tasks. The policy reaffirms the principles of the indivisibility of Allied security and prevention, detection, resilience, recovery, and defense. It recalls that the fundamental cyber defense responsibility of NATO is to defend its networks, and that assistance to Allies should be addressed by the spirit of solidarity, emphasizing the responsibility of Allies to develop the relevant capabilities for the protection of national networks.
- Our policy also recognizes that international law, including international humanitarian law and the UN Charter, applies in cyberspace. Cyber attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm therefore that cyber defense is part of NATO's core task of collective defense. A decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis.

The threats and protection of cyberspace, the Internet, are recognized by the Alliance, which includes 32 member states (30 from Europe, most of which are also EU member states, and two from North America). These are the countries that also play a major role in the development and implementation of global Internet policies. In fact, by including this provision in the Alliance's declaration, cyberspace, the Internet, has been recognized as a component of international, regional, and national security.

Here we hear a second hypothetical question, namely, if the global Internet, cyberspace, is one of the components of international security, then the fragmentation of the Internet and the threats that accompany this process should also be considered in the context of international security, and in parallel with the technical dimensions, the geopolitical dimension of fragmentation should be recognized and studied.

When we talk about the geopolitical dimension of Internet fragmentation and consider it in the context of international security, along with other influencing factors, it is necessary to mention the ongoing military conflicts in the world, which cause great damage, first of all, to the national

Internet, and then, consequently, to the unity, security, and stability of the regional and global Internet, which in turn depends on the full functioning of the national Internet [6–9].

Among the ongoing military conflicts, the Russia-Ukraine war should be highlighted, which also covers the Black Sea region and poses a threat to the cyber resilience of the countries of the region. This conflict also causes great damage to the routes of optical fiber cables in the Black Sea, to the domain name systems, and to the full functioning of IP addresses. In addition, there are threats resulting from the Internet policies of individual country governments, such as geographical restrictions on data transfer and access, user blocking, hybrid challenges, and an increasing number of cyberattacks [9–11].

4. Technical dimensions of Internet fragmentation

In addition to the political, commercial, and governmental dimensions of Internet fragmentation, several technical parameters contribute to the division and segmentation of the global Internet. These technical factors encompass network performance, data routing inefficiencies, infrastructure limitations, and security measures, all of which impact the seamless flow of data across global networks and thus contribute to fragmentation. This section outlines the key technical parameters that influence Internet fragmentation [12–15].

4.1. Bottlenecks and congestion in network infrastructure

Bottlenecks occur when data flows exceed the capacity of a network segment, leading to delays, packet loss, and inefficient routing. Such congestion points are often found at key transit points, such as international exchange points, undersea cables, and cross-border routing [16]. The following factors contribute to bottlenecks:

- Bandwidth limitations: Limited bandwidth at key network nodes can cause congestion, leading to slower data transmission speeds and packet loss, which results in fragmentation.
- Overloaded peering points: At network interconnection points, where large-scale traffic is exchanged between networks, congestion can result from unbalanced data flows.
- Capacity mismatches: Disparities in network infrastructure capabilities between regions or service providers can lead to asymmetric data flows and interruptions.

Identifying and managing these bottlenecks is crucial for preventing fragmentation, and this often involves the use of technologies such as traffic engineering, load balancing, and traffic prioritization.

4.2. Routing inefficiencies and path divergence

The current global Internet routing model, primarily based on the Border Gateway Protocol (BGP), is susceptible to inefficiencies and inconsistencies in routing tables [17]. This results in data being sent through suboptimal or longer paths, exacerbating fragmentation. The following issues contribute to routing inefficiencies:

- BGP route hijacking and misconfiguration: Malicious actors or misconfigured routers can cause data to be routed through unintended paths, potentially isolating regions or countries.
- AS path fragmentation: The global Internet relies on Autonomous Systems (AS) to manage routing. Over time, the proliferation of AS numbers and the complexity of inter-AS agreements can cause fragmentation in the routing space.
- IPv4 and IPv6 transition challenges: The ongoing transition from IPv4 to IPv6 can cause compatibility issues, especially in regions where IPv6 adoption is slow. As a result, some areas may be isolated from parts of the global Internet.

These routing inefficiencies not only slow down data transfer but can lead to entire regions being isolated from the global network, contributing to the overall fragmentation of the Internet.

4.3. Impact of network security measures on fragmentation

Security measures, while essential for protecting the Internet, can also inadvertently contribute to fragmentation. Various security-related practices can impose restrictions on data flow, leading to segmented networks:

- Firewall policies: Firewalls designed to block malicious traffic can sometimes inadvertently block legitimate cross-border data traffic, creating isolated network segments.
- DNS filtering and IP blocking: Governments and corporations often use DNS filtering and IP blocking to limit access to certain websites and services, which can fragment the Internet by restricting connectivity between regions.
- Content filtering and censorship: Countries with strict censorship policies often employ mechanisms like DNS poisoning or Deep Packet Inspection (DPI), which can prevent users in certain regions from accessing global content. This leads to the creation of walled-off segments of the Internet.

While these security measures are essential to protect national interests, they can also lead to a breakdown in the interoperability of networks, thereby contributing to fragmentation.

4.4. Infrastructure and geographical disparities

The global Internet's infrastructure is unevenly distributed, with certain regions having more advanced networks and better connectivity than others. These geographical disparities can create isolated networks:

- Undersea cable routes: Damage to or interference with undersea cables can disrupt global connectivity, isolating regions and countries from one another. The Russia-Ukraine war, for example, has threatened key fiber-optic cable routes in the Black Sea, leading to potential fragmentation of regional Internet traffic.
- Peering agreements: Regional ISPs (Internet Service Providers) and national governments may choose to establish peering agreements that prioritize local or regional data exchanges, limiting the international flow of data.
- Access to modern infrastructure: In many developing countries, access to modern Internet infrastructure, including high-speed fiber-optic networks, is limited. This creates a situation where these countries may have slower or isolated connections to the global Internet, exacerbating fragmentation.

4.5. Latency and throughput constraints

High latency and low throughput can lead to inconsistent access to the Internet, especially across different regions or during peak usage periods [18–21]. These performance issues create the potential for data to be delayed or dropped, further contributing to the fragmentation process.

- Latency: Long delay times between sending and receiving data (often due to long-distance routing or bottlenecks) can degrade the user experience, especially in real-time communications like video calls, gaming, or financial transactions.
- Throughput issues: Areas with limited bandwidth or higher congestion levels often experience lower throughput, which can prevent effective cross-border communication and information exchange.

4.6. Mitigation strategies and future developments

To prevent the technical fragmentation of the Internet, several strategies can be implemented [22–25]:

- Improved routing protocols: Developing and implementing more robust routing protocols, such as Segment Routing (SR) or Multiprotocol Label Switching (MPLS), could help mitigate path divergence and improve network performance.
- IPv6 adoption: Accelerating the global transition to IPv6 would help ensure compatibility across all regions and prevent the creation of isolated "IPv4 islands".
- Cross-border collaboration: Encouraging international cooperation between governments and private entities to upgrade network infrastructure and resolve routing inefficiencies is critical to avoiding fragmentation.

Conclusions

In conclusion, the process of Internet fragmentation poses a significant threat to the unity of the global Internet, its safe and stable development, openness, transparency, and free access. As highlighted in the paper, the declaration adopted by the North Atlantic Alliance at the Wales Summit, particularly paragraph 72, underscores the recognition of cyberspace as an "operational domain". This acknowledgment not only reflects the increasing frequency and sophistication of cyberattacks but also emphasizes the critical importance of safeguarding cyberspace to ensure international security. Cyberattacks, alongside other technical dimensions of fragmentation, contribute to the broader trend of dividing the Internet into isolated fragments, with serious consequences for global connectivity [26–28].

The paper raises two important hypothetical questions that warrant further investigation:

- Can the fragmentation of the Internet, alongside its technical dimensions, be considered a subject of international security research within a geopolitical context?
- If cyberspace, as part of the global Internet, is integral to international security, should the fragmentation of the Internet and its associated risks be framed within this context, recognizing and studying both the technical and geopolitical dimensions of this fragmentation?

Furthermore, when evaluating the threats in the Internet space that amplify the fragmentation process, it is crucial to address the issue within both technical and geopolitical frameworks, particularly at the regional level. Military conflicts and political tensions continue to inflict significant damage on the Internet infrastructure, which, in turn, undermines the security and stability of global and regional networks.

In this context, the Black Sea region serves as a notable example, where the ongoing Russia-Ukraine conflict exacerbates the cyber resilience of the surrounding nations. This conflict not only disrupts critical infrastructure such as fiber-optic cables, DNS routes, and IP address allocation but also poses significant challenges to the seamless global operation of the Internet. The technical fragmentation arising from the blocking or filtering of content, variations in network standards (e.g., the slow adoption of IPv6), and localized DNS management are contributing to a fragmented cyberspace that risks isolating regions and further destabilizing global connectivity [29, 30]. Additionally, government policies that enforce geographical restrictions on data transmission, implement user blocking, and increase cyberattacks create further vulnerabilities.

As such, the dual threat of geopolitical instability and technical fragmentation warrants urgent attention. Efforts to mitigate these threats must address not only the underlying geopolitical tensions but also the technical barriers that hinder the global Internet's operation. Without coordinated international action, these issues will continue to erode the security, stability, and openness of the global digital ecosystem.

Acknowledgment

This work was supported by the Shota Rustaveli National Foundation of Georgia (SRNSFG) (NFR-22-14060).

Declaration on Generative AI

While preparing this work, the authors used the AI programs Grammarly Pro to correct text grammar and Strike Plagiarism to search for possible plagiarism. After using this tool, the authors reviewed and edited the content as needed and took full responsibility for the publication's content.

References

[1] UNGA, The pact for the future A/79/L.2 (Annex I. Global digital compact), 2024. URL: https://documents.un.org/doc/undoc/ltd/n24/252/89/pdf/n2425289.pdf

[2] W. J. Drake, V. G. Cerf, W. Kleinwächter, Internet fragmentation: An overview, in: World Economic Forum, 2016. URL: https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf

[3] K. Komaitis, Research in focus Internet fragmentation: Why it matters for Europe, 2023. URL: file:///C:/Users/lsvan/Desktop/%E1%83%A1%E1%83%A2%E1%83%90%E1%83%A2%E1%83%98%E1%83%90_1/internet-fragmentation-why-it-matters-for-europe.pdf/

[4] T. Minárik, NATO recognises cyberspace as a "Domain of operations" at Warsaw summit. URL: https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/

[5] Wales summit declaration, Paragraph 72. URL: http://www.nato.int/cps/en/natohq/official_texts_112964.htm

[6] V. Svanadze, Internet fragmentation as a new challenge for the unified, security and stability of Internet, Sci. Practical Cyber Secur. J. (SPCSJ) 8(4) (2024).

[7] V. Svanadze, M. Iavich, Impact of Internet fragmentation on the unity, security, and stability of global Internet, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3654, 2024, 520–525.

[8] V. Svanadze, Challenges of Internet fragmentation and global cyberspace, Sci. Practical Cyber Secur. J. 4(07) (2023).

[9] The Internet way of networking: Defining the critical properties of the Internet, Internet Society, 2020. URL: https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/critical-properties-of-the-internet/

[10] M. Mueller, Will the Internet fragment? Sovereignty, globalization and cyberspace, Cambridge: Polity Press, 2017.

[11] ICANN org comments on the Proposal for a Directive of the European Parliament and of the Council on Measures for a High Common Level of Cybersecurity Across the EU, repealing Directive (EU) 2016/1148 (NIS 2 Directive). URL: https://www.icann.org/en/system/files/files/icann-org-comments-proposed-nis2-directive-19mar21-en.pdf

[12] APNIC, "IPv4 exhaustion details". URL: https://www.apnic.net/community/ipv4-exhaustion/ipv4-exhaustion-details/

[13] RIPE NCC, The RIPE NCC has run out of IPv4 addresses. URL: https://www.ripe.net/publications/news/about-ripe-nccand-ripe/the-ripe-ncc-has-run-out-of-ipv4-addresses

[14] European Commission, Europe's digital decade: Digital targets for 2030. URL: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets2030_en

[15] Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union (Text with EEA relevance). URL: https://eurlex.europa.eu/legalcontent/EN/TXT/?toc=OJ%3AL%3A2015%3A310%3ATOC&uri=uriserv%3AOJ.L_.2015.310.01.0001.01.ENG

[16] D. Lei, et al., Identifying service bottlenecks in public bikesharing flow networks, J. Trans. Geogr. 116 (2024) 103830. doi:10.1016/j.jtrangeo.2024.103830

[17] B. A. Scott, M. N. Johnstone, P. Szewczyk. A survey of advanced border gateway protocol attack detection techniques, Sensors 24(19) (2024) 6414.

[18] M. Iorio, F. Risso, C. Casetti, When latency matters: measurements and lessons learned, ACM SIGCOMM Comput. Commun. Rev. 51(4) (2021) 2–13.

[19] F. Han, et al., Future data center networking: From low latency to deterministic latency, in: IEEE Network 36(1) (2022) 52–58.

[20] L. M. Akimova, et al., The negative impact of corruption on the economic security of state, Int. J. Manag. 11(5) (2020) 1058–1071.

[21] R. Kostyrko, et al., Ukrainian market of electrical energy: Reforming, financing, innovative investment, efficiency analysis, and audit, Energies, 14(16) (2021) 5080.

[22] O. Solomentsev, et al., Efficiency of operational data processing for radio electronic equipment, Aviation, 23(3) (2020) 71–77.

[23] J. S. Al-Azzeh, et al., Analysis of self-similar traffic models in computer networks, Int. Rev. Modelling Simul. 10(5) (2017) 328–336.

[24] I. Ostroumov, N. Kuzmenko, Configuration analysis of European navigational aids network, in: 2021 Integrated Communications Navigation and Surveillance Conference (ICNS), 2021, 1–9. doi:10.1109/ICNS52807.2021.9441576

[25] Y. Averyanova, et al., Turbulence detection and classification algorithm using data from AWR, in: 2022 IEEE 2nd Ukrainian Microwave Week (UkrMW), 2022, 518–522. doi:10.1109/UkrMW58013.2022.10037172

[26] V. Sydorenko, et al., Experimental FMECA-based assessing of the critical information infrastructure importance in aviation, in: ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer, vol. 2732, 2020, 136–156.

[27] A. Imanbayev, et al., Research of machine learning algorithms for the development of intrusion detection systems in 5G mobile networks and beyond, Sensors, 22(24) (2022) 9957.

[28] Z. Avkurova, et al., Targeted attacks detection and security intruders identification in the cyber space, Int. J. Comput. Netw. Inf. Secur. 16(4) (2024) 144–153.

[29] Y. Kostiuk, et al., A system for assessing the interdependencies of information system agents in information security risk management using cognitive maps, in: 3rd International Conference on Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN), Kyiv, Ukraine, vol. 3925, 2025, 249–264.

[30] Y. Kostiuk, et al., Models and Algorithms for analyzing information risks during the security audit of personal data information system, in: 3rd International Conference on Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN), Kyiv, Ukraine, vol. 3925, 2025, 155–171.