

The State of the Internet and Digital Rights in Ukraine (2019–2025)

The Internet in Ukraine, having withstood the test of a full-scale war, demonstrates a unique model of resilience and adaptation. Despite unprecedented destruction of infrastructure, the country’s digital space has not only survived but continues to develop, showing growth in some segments and transformation in others. This report examines in detail how the Ukrainian network is coping with the challenges of wartime — from restoring destroyed networks to countering cyberattacks and maintaining connectivity in occupied territories.

This study goes beyond a simple statistical overview. We delve into the key trends shaping the future of the Ukrainian Internet: from the real (rather than inflated) pace of IPv6 adoption to the paradoxical increase in the number of Internet providers amid active hostilities. Particular attention is paid to the mobile communications market, which has faced subscriber outflow and network destruction, and to the role of satellite Internet, which has become a critically important element for maintaining connectivity.

This document offers a comprehensive view of the complex interplay between technology, legislation, and human rights under extreme conditions. You will learn about new regulatory initiatives aimed at protecting digital sovereignty, the methods of blocking and censorship applied in occupied territories, and how VPN services have evolved from a niche tool into an essential means for accessing free information. We invite you to explore a detailed analysis of Ukraine’s digital front.

Disclaimer: This document was partially generated using several large language models (LLM). The information presented in it is based on the analysis and generalization of data from the specified sources, however, the process of its structuring, generalization, and presentation was performed using artificial intelligence technologies. It is recommended to use this text as a starting point for further research and to verify critically important data from primary sources.

The State of the Internet and Digital Rights in Ukraine (2019–2025)	1
1. General Information	3
1.1. Geographical Location	3
1.2. Population	3
1.3. Gross Domestic Product	4
1.4. Main Economic Characteristics	6
1.5. General Political Situation	6

2. Internet	8
2.1. National domain	8
2.2. Number of users	9
2.2.1 Fixed-line Internet	9
2.2.2 Mobile Internet	12
2.3. Internet access speed and service quality	14
2.4. Development of providers and Autonomous Systems	15
2.5. IPv6 adoption	19
2.6. Connectivity Index	21
3. Legislation on the Internet	24
3.1. Principles of Internet governance	24
3.1.1. Regulation	24
3.1.2. Regulatory bodies and responsible persons	25
3.2. Market monopolization	26
3.3. Internet shutdowns by government order	28
3.4. Legislation on “words on the Internet”	29
3.5. Legislation on Internet blocking	30
3.5.1. Legislation	31
3.5.2. Blocking procedures	32
3.5.3. Registries of blocked Internet resources	33
3.5.4. Development of Blocking	35
4. Human Rights Violations on the Internet	37
4.1. Internet Shutdown by Government Order	37
4.2. Criminalization of Statements on the Internet	38
4.3. Persecution of Media and NGOs	40
5. Civil Society in the Field of Internet Governance	42
5.1. Organizations	42
5.2. VPN and Means of Bypassing Blocks	44
5.2.1. Status of VPN Services	44
5.2.2. Number of VPN Users	45
5.2.3. Cases of Persecution for Using VPN	47
5.2.4. Monitoring of Blocks	48
6. Conclusion	50
Sources	51

1. General Information

1.1. Geographical Location

Ukraine is a state located in Eastern Europe. The vast majority of the country's territory lies within the East European Plain (95% of the area); the north is dominated by the Polissia Lowland, the center by the Dnipro Lowland, and the south by the Black Sea Lowland. In the west are the Volyn, Podillia, and Dnipro Uplands and the Tovtry ridge; in the north — the Slovechansko-Ovruch ridge. A small part (about 3%) is occupied by mountains: the Ukrainian Carpathians in the west (highest point — Hoverla, 2061 m) and the Crimean Mountains in the south (up to 1545 m).¹ The total area within internationally recognized borders is 603,549 km². Ukraine borders Romania and Moldova in the southwest, Hungary, Slovakia, and Poland in the west, Belarus in the north, and Russia in the east, northeast, and southeast.¹

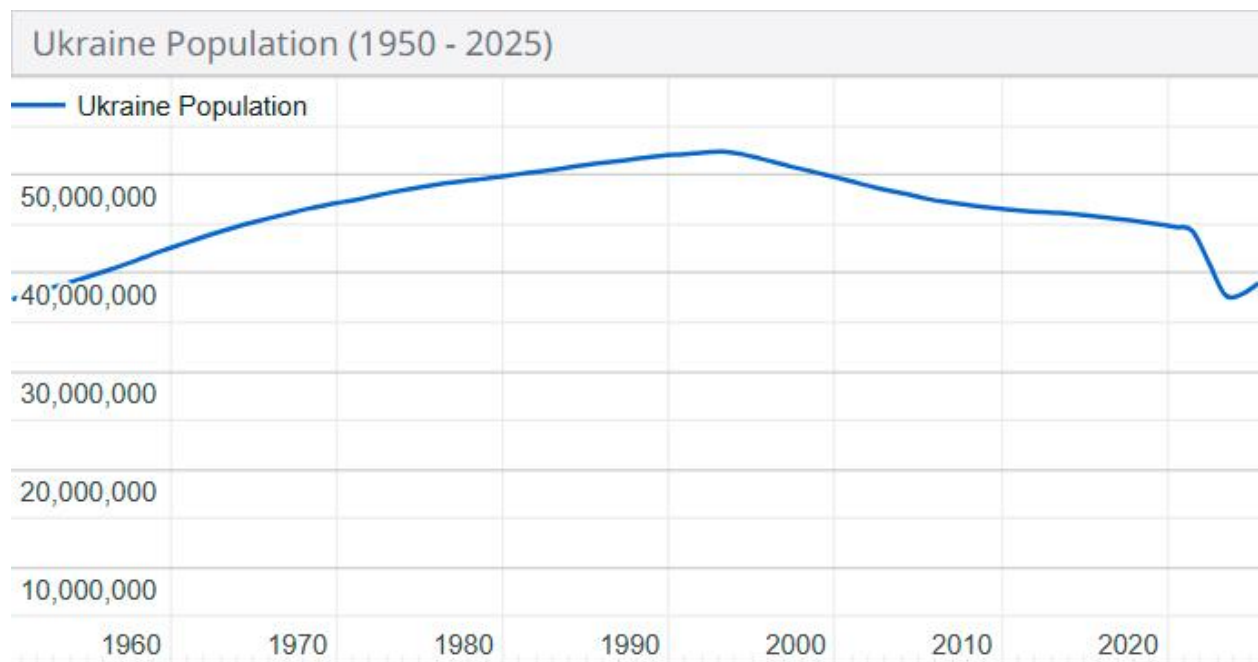
This geographical position, especially the long border with Russia and Belarus and access to the Black and Azov Seas, is of critical importance in the context of the ongoing armed conflict that began in 2014 and escalated into a full-scale phase in February 2022. This conflict directly affects the state and security of digital infrastructure as well as cross-border data flows. The predominantly flat terrain, on the one hand, facilitates the laying of communications, but on the other hand makes them more vulnerable to physical damage during hostilities compared to mountainous areas where infrastructure can be better protected by the natural landscape.

1.2. Population

Ukraine's population has shown a steady downward trend over recent decades. This process worsened significantly after 2014 and especially catastrophically after the start of Russia's full-scale invasion in February 2022. The main factors of the current demographic crisis are direct military losses, significant forced emigration of citizens (primarily women and children), internal displacement, and the inability to accurately count the population in temporarily occupied territories.³ Urban population has traditionally predominated in the population structure. The age structure is also undergoing negative changes characterized by population aging and declining birth rates, creating additional long-term challenges for the country's socio-economic development.

Data on Ukraine's population from 2019 to 2025 vary considerably depending on the source and counting methodology, which has become particularly noticeable after February 2022 due to the difficulty of collecting accurate information amid war and mass migration. The sharp population decline, especially of working age in particular, and large-scale migration create long-term challenges for Ukraine's digital economy. These include a potential shortage of qualified IT personnel and related industries, as well as a narrowing of the domestic market for digital products and services. Some international forecasts indicating possible population growth in 2024–2025⁴ should be interpreted with caution, as they may be based on assumptions about the mass return of refugees or changes in counting methodology, which under continuing conflict appear overly optimistic and contrast with earlier forecasts of gradual decline.⁶

Graph 1: Ukraine Population Dynamics (1950–2025)



Source: worldometers.info

This table clearly demonstrates the scale of demographic changes. The population decline directly affects the number of potential Internet users, although Internet penetration among the remaining population may increase due to its growing importance. Demographic shifts also put pressure on the labor market, including the IT sector, which is an important driver of Internet and digital economy development in the country. Differences in estimates highlight the difficulty of collecting accurate data amid ongoing conflict and occupation of part of the territory.

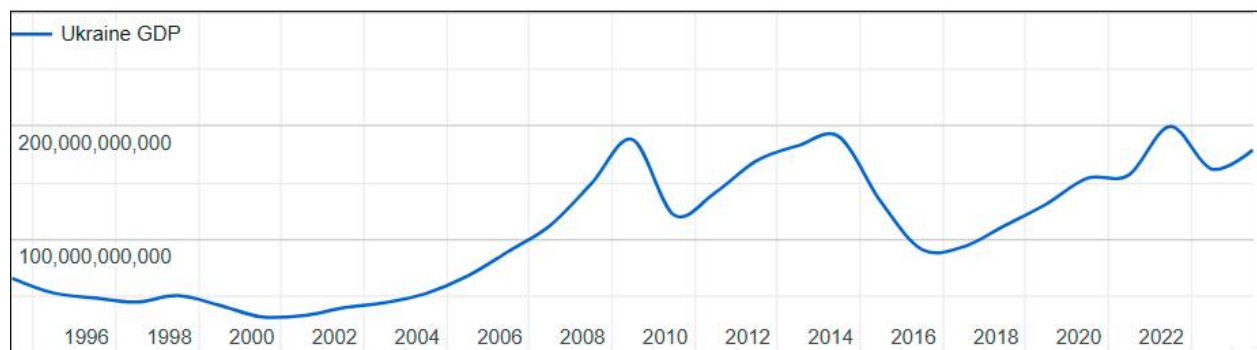
1.3. Gross Domestic Product

Ukraine's economy experienced an unprecedented shock in 2022 due to Russia's full-scale invasion, resulting in a GDP drop of approximately 29–30%.⁷ In 2023, partial recovery of economic activity was observed, with GDP growth of about 5.3%.⁸ However, forecasts for 2024–2025 indicate a slowdown: the State Statistics Service of Ukraine reported 2.9% growth in 2024¹⁰, the European Bank for Reconstruction and Development (EBRD) forecasts 3.3% growth in 2025¹¹, and the National Bank of Ukraine (NBU) expects 3.1% growth in 2025.¹² The country's economy remains heavily dependent on international financial assistance and the further development of the situation at the front.

Ukraine's pre-war GDP in 2019 was approximately USD 153.88 billion.¹³ In subsequent years the dynamics were as follows: 2020 — USD 156.62 billion¹³, 2021 — USD 199.77 billion.¹³ After the start of the full-scale war, GDP fell sharply: in 2022 to USD 161.99 billion.¹³ In 2023, GDP was estimated at USD 178.76 billion, showing some recovery.¹³ Forecasts for 2025 from various institutions vary: the IMF (via Wikipedia⁷) indicated nominal GDP of USD 195.23 billion, the EBRD forecasts 3.3% growth¹¹, and the NBU — 3.1%.¹² Data in national currency (hryvnia) also reflect these trends but are subject to significant inflation and exchange-rate fluctuations.¹⁴ Despite partial GDP recovery in 2023–2024, its level remains significantly below pre-war levels.⁹ The slowdown in growth in 2024 compared to 2023¹⁰ indicates persistent structural problems and the continuing negative impact of the war, especially on energy infrastructure and the agricultural sector. This casts doubt on the sustainability of long-term recovery without an end to hostilities and sustained large-scale international support.

Graph 2: Dynamics of Ukraine's Nominal GDP (1993–2023)

Ukraine GDP (Nominal, \$USD) 1993-2023



Source: worldometers.info

The state of GDP directly correlates with the ability of the state and private sector to invest in the development and maintenance of Internet infrastructure. Population solvency, closely

linked to per capita GDP, affects demand for Internet services and their quality. Forecasts for 2024–2025 are important for assessing the prospects for digital sphere development, but they carry significant uncertainty due to the ongoing war.

1.4. Main Economic Characteristics

Ukraine's economy in the period under review (2019–2025) is undergoing a period of profound shocks and transformations caused first by the consequences of the COVID-19 pandemic and then, to a much greater extent, by Russia's full-scale invasion in February 2022. After a sharp recession in 2022, when GDP contracted by 29.1%⁷, slow and uneven recovery is observed.⁸ The key sectors of the Ukrainian economy have traditionally been agriculture (especially grain and oilseed exports), heavy industry (including the mining and metallurgical complex and mechanical engineering), and the dynamically developing services sector, including IT.⁷ During the war, the role of the defense-industrial complex and sectors ensuring the country's vital functions has increased significantly.

Structural problems of the Ukrainian economy that existed before 2022 have worsened considerably. These include: colossal damage to physical infrastructure (energy, transport, industrial) and production facilities as a result of hostilities; disruption of logistics chains, especially export routes through the Black Sea; loss of control over part of the territories with their economic potential and production assets; acute labor shortage caused by mass emigration, internal migration, and mobilization.¹⁵ The economy is critically dependent on international financial assistance to cover the budget deficit and finance recovery.¹¹ Problems with high levels of corruption and the need to continue structural reforms begun after the collapse of the USSR remain.¹⁷ According to 2024 estimates, annual GDP growth slowed to 2.9%, inflation was about 5.8%, unemployment remained high (14.2%), and public debt continued to rise, reaching 95.6% of GDP.⁹ So-called "war Keynesianism" — economic growth stimulated by military orders and spending¹⁵ — may temporarily support some indicators but does not solve fundamental structural problems and is not a sustainable long-term development model, carrying inflationary risks.

Solving these structural problems, including the restoration of critical infrastructure (especially energy, which is vital for the functioning of the Internet and digital services) and effective fight against corruption, will be key to post-war recovery and further development of the digital economy.

1.5. General Political Situation

Ukraine is a unitary republic with a mixed (semi-presidential) form of government, where the president is the head of state and the prime minister is the head of government.¹⁸ The

country's political system is characterized by multi-party politics. As of the preparation of this report, the incumbent President of Ukraine is Volodymyr Zelenskyy. Executive power is headed by the Cabinet of Ministers of Ukraine, formed by a coalition of parliamentary factions in the Verkhovna Rada. Legislative power belongs to the unicameral parliament — the Verkhovna Rada of Ukraine.

Since 24 February 2022, due to the full-scale invasion by the Russian Federation, martial law has been in effect throughout Ukraine. This legal regime has led to certain restrictions on some constitutional rights and freedoms of citizens, including freedom of movement and assembly, and has also affected political processes. In particular, the next parliamentary elections scheduled for autumn 2023 and presidential elections scheduled for spring 2024 were postponed.¹⁹ This decision, although it has drawn some criticism from certain political forces and experts, is generally supported by the majority of the population under conditions of continuing war, as confirmed by sociological surveys.¹⁹

In May 2022, President Volodymyr Zelenskyy signed a law banning the activities of political parties that justify, recognize as lawful, or deny the armed aggression of Russia against Ukraine. Subsequently, more than a dozen political parties were declared “pro-Russian” and banned by court order, including the then-largest opposition party, Opposition Platform — For Life (OPFL).¹⁹ A certain consolidation of the information space is also observed: the main national news TV channels operate in the format of a single information marathon “United News,” broadcasting predominantly government-approved content and giving airtime mainly to representatives of the ruling party, which limits the ability of opposition parties to convey their position to a wide audience.¹⁹ These measures, explained by the needs of national security and information confrontation in wartime, spark discussions about their impact on political pluralism and freedom of speech.

Ukraine's administrative-territorial structure underwent a major decentralization reform. As of 17 July 2020, regions (oblasts, the Autonomous Republic of Crimea, and the cities of Kyiv and Sevastopol with special status) are divided into 136 enlarged districts (instead of the previous 490). Districts, in turn, consist of territorial communities (hromadas) — urban, settlement, and rural.²¹ This reform aims to transfer greater powers and financial resources to the local level and strengthen local self-government. The concentration of power and restriction of political pluralism observed under martial law, although explainable by objective national security challenges, create potential risks for the country's long-term democratic development. This may also indirectly affect freedom of speech and information on the Internet, as increased state control over the media sphere and the banning of certain political forces may lead to a narrowing of space for independent voices and opposition opinions, including online.

2. Internet

2.1. National domain

The national top-level domain (ccTLD) for Ukraine is **.UA**.²³ It was officially delegated by the Internet Assigned Numbers Authority (IANA) on December 1, 1992, to representatives of the Ukrainian Internet community Oleh Voloshchuk and Ihor Svyrydov.²³ Since 2001, the administration and technical maintenance of the **.UA** domain, as well as public second-level domains within it, have been carried out by **Hostmaster Ltd.**²⁵ Hostmaster ensures stable and secure operation of the domain zone, supports international standards such as **DNSSEC** (Domain Name System Security Extensions, signed in 2012²³), **IDN** (internationalized domain names), and **RDAP** (Registration Data Access Protocol), and cooperates with domain name registrars in Ukraine and worldwide.²⁵

The history of the **.UA** domain development includes several key stages. In 1995, the first targeted public second-level domains were delegated: **COM.UA** (for commercial organizations), **GOV.UA** (for state institutions), and **NET.UA** (for network organizations).²³ In 1996, “short” (two-letter) geographical synonym domains appeared (e.g., **km.ua** for Khmelnytskyi Oblast).²³ Later, **EDU.UA** (for educational institutions, 1998) and **ORG.UA** (for public organizations, 1999) were delegated.²³

The first private second-level domain (not public, but directly under **.UA**, e.g., **example.ua**) — **BUSINESS.UA** — was delegated on October 23, 2001.²³ By 2000, a layer of registrar companies had already formed in Ukraine, and all rules and principles of operation were regulated exclusively by the internal rules of the **.UA** domain.²⁴ A significant event was the implementation of IPv6 protocol support in 2010, when the number of sites in the **.UA** zone exceeded 500,000.²⁴ In 2009, an application was submitted to ICANN for the registration of the Cyrillic domain **.YKP**, which was delegated later (the process was completed by March 2013²³).

A key characteristic and the main condition for registering a private second-level domain name directly in the **.UA** zone (e.g., **company.ua**) is the mandatory presence of a valid Ukrainian certificate for a sign for goods and services (trademark) issued by the authorized state body (State Patent Office, now UkrNOIV), or an international trademark registration that extends to the territory of Ukraine.²⁷ The domain name must exactly match the verbal part of

the trademark. This rule is aimed at protecting intellectual property rights and preventing cybersquatting. For registration of domains in public second-level domains (such as **com.ua**, **org.ua**, **kiev.ua**, etc.), the requirement for a trademark is absent, making them more accessible to a wide range of users.²⁴ Such a strict rule for second-level **.UA** domains, on the one hand, is a significant barrier for many potential registrants, especially small businesses or individuals who do not have registered trademarks. On the other hand, it increases the level of trust in such domains, as they are associated with officially registered brands, and significantly reduces the number of disputes related to bad-faith domain registrations. This policy distinguishes **.UA** from many other national domains where registration rules are more liberal.

2.2. Number of users

According to Datareportal research, as of early 2025, Ukraine had **31.5 million** active Internet users, which accounted for **82.4%** of the country's total population.²⁹ The International Telecommunication Union (ITU) also confirms an Internet penetration level of **82.4%** as of 2023.³² Other sources provide similar figures for previous years: Wikipedia, citing various data, indicates **31.1 million** users in 2022³³, while The World Bank, through TheGlobalEconomy.com, reported **79.22%** penetration in 2021.³⁴ Freedom House, relying on ITU data, noted a **75%** penetration level in 2020.³⁵

Despite the ongoing armed conflict and the associated population decline, the Internet penetration level in Ukraine not only remains high but, according to some estimates, shows a certain growth. Kepios analysis cited in the Datareportal report indicates an increase in the number of Internet users by **690 thousand** (+2.2%) between January 2024 and January 2025.²⁹ This underscores the critical importance of the Internet for the population amid the crisis — as the primary means of communication, access to vital information, state and financial services, as well as education and work. The remaining **17.6%** of the population not using the Internet as of early 2025²⁹ likely includes elderly people, residents of remote rural areas with limited coverage or insufficient connection quality, as well as persons living in temporarily occupied territories where access to the Ukrainian Internet segment may be restricted or blocked.

A high penetration level means that any disruptions in network access, censorship, or cyberattacks will have broad and immediate consequences for a significant part of society.

2.2.1 Fixed-line Internet

Fixed broadband access (BBA) in Ukraine has historically been characterized by a high level of competition among providers and gradual technological upgrading of networks. In recent years, especially amid frequent power outages due to Russian attacks on energy infrastructure, there has been an active transition to more energy-independent technologies such as **xPON** (passive optical networks). The fixed BBA market remains highly fragmented, with a large number of small and medium-sized operators alongside several major national players. Military actions have caused significant damage to fixed-line infrastructure, but operators are making considerable efforts to restore and modernize it.³⁵

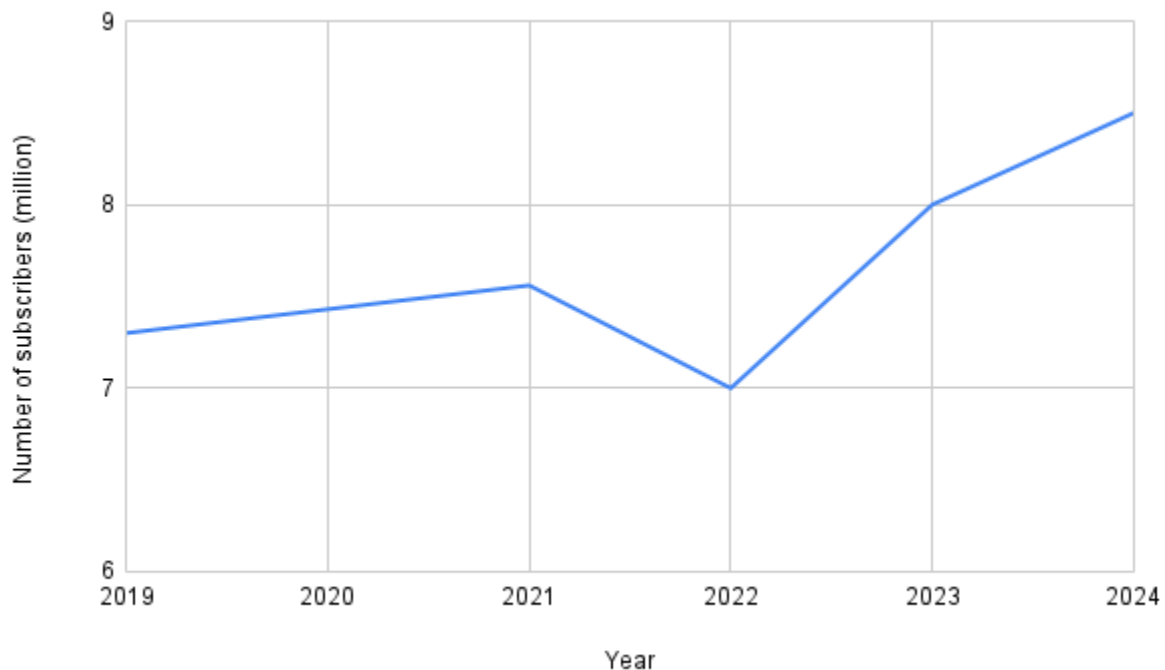
According to the analytical report of the Office for Effective Regulation BRDO, as of the end of 2024, approximately **8.5 million** subscribers (including households and legal entities) used fixed-line Internet access services. This figure indicates a recovery of the subscriber base to the 2021 level after a significant decline in the first months of the full-scale invasion. Notably, **27%** of all fixed BBA subscribers are located in rural areas, indicating a gradual bridging of the digital divide between urban and rural areas.³⁷ According to the National Commission for the State Regulation of Electronic Communications (NCEC) data cited by Mind.ua, in 2024 Ukraine had **8.2 million** fixed-line access subscribers, a **1.2%** increase compared to the previous year. Of these, **3.98 million** subscribers (almost **48.5%**) were already using **xPON** technology.³⁸

Largest home Internet providers (according to various estimates and indicators):

- **JSC “Ukrtelecom”**: Traditionally one of the largest players, although its market share may have gradually declined in recent years due to competition. According to Tadviseer (period not specified, likely pre-2023), the company’s revenue from Internet services (including the business segment) was **0.83 billion UAH**.³⁹ Total revenue of JSC “Ukrtelecom” in 2024 amounted to **5.9 billion UAH**, with a net profit of **389 million UAH**.⁴⁰ Website: <https://ukrtelecom.ua/>
- **PrJSC “Kyivstar”**: The largest mobile operator, also actively providing fixed BBA services under the “Home Internet” brand. Revenue from Internet services, according to Tadviseer, was **0.69 billion UAH**.³⁹ Total revenue of PrJSC “Kyivstar” in 2024 — **39.2 billion UAH**.⁴⁰ Website: <https://kyivstar.ua/>
- **Datagroup-Volia** (formerly LLC “Volia-Cable” and PrJSC “Datagroup”): Formed as a result of the merger of two major players, becoming one of the market leaders.⁴² Revenue of “Volia-Cable” (before full merger) was **0.44 billion UAH**³⁹, total revenue of LLC “Volia-Cable” in 2024 — **1.6 billion UAH**.⁴⁰ Revenue of “Datagroup” (before merger) — **0.34 billion UAH**³⁹, total revenue of PrJSC “Datagroup” in 2024 — **3.5 billion UAH**.⁴⁰ Websites: <https://volia.com/>, <https://www.datagrup.ua/>
- Other notable providers: Triolan, Lanet, Freenet (“OGO!Port”, “FREENET”), TENET, Maxnet. These providers often lead in speed according to independent tests, for example, for Steam service users.⁴³

Market shares (approximate estimates): According to BRDO data for the first half of 2024, the top-10 largest fixed-line access companies served about **33%** of all Ukrainian subscribers (approximately **2.8 million** users), generating **28%** of the industry’s total revenue. Notably, the market share of the largest operators, both in revenue and subscriber numbers, tends to decrease annually.³⁷ This indicates growing competition from smaller players, particularly sole proprietors actively developing their networks, especially in regions.

Graph 3: Dynamics of fixed BBA subscribers in Ukraine (2019–2023)



The fixed-line Internet market in Ukraine demonstrates significant resilience and adaptability under extremely difficult military conditions, having managed to restore the subscriber base to pre-war levels by the end of 2024.³⁷ Active implementation of **xPON** technology³⁸ is an important factor in improving connection reliability amid the energy crisis caused by Russian attacks. At the same time, the role of small and medium-sized providers, operating as sole proprietors, is strengthening.

This indicates a high level of competition and market decentralization, which is generally a positive factor. However, such fragmentation can also create challenges related to ensuring proper service quality, investments in modernization and network security by smaller players, as well as their vulnerability to possible pressure from larger companies or changes in regulator’s technological requirements.³⁷

2.2.2 Mobile Internet

Mobile Internet plays a key role in providing communication and information access for most Ukrainians, especially when fixed infrastructure may be damaged or unavailable.³⁵ According to GSMA Intelligence, as of early 2025, **94.1%** of all mobile connections in Ukraine were classified as broadband, i.e., carried out via 3G, 4G, or 5G networks.²⁹ The total number of active mobile connections (including those that may be used only for voice and SMS and do not necessarily have Internet access) on the same date was **56.4 million**. This figure, equivalent to **147%** of the total population,²⁹ indicates the widespread practice of using multiple SIM cards by one subscriber or the presence of inactive but registered cards.

According to NCEC data (via Mind.ua), the number of subscribers using 4G technology reached **30.5 million** by the end of 2024, a **2.5%** increase compared to the previous year. Thus, **62.5%** of all active SIM cards in the country had access to fourth-generation communication.³⁸ In 2022, despite the start of the full-scale war, the total revenue of mobile operators grew by **5.1%**. This growth, though lower than previous average annual rates (about 14%), was driven mainly by increased data service consumption and international roaming due to the mass migration of Ukrainians abroad and heightened communication needs.⁴⁵

Largest mobile Internet providers:

The mobile communications and mobile Internet market in Ukraine is highly concentrated and represented by three main players:

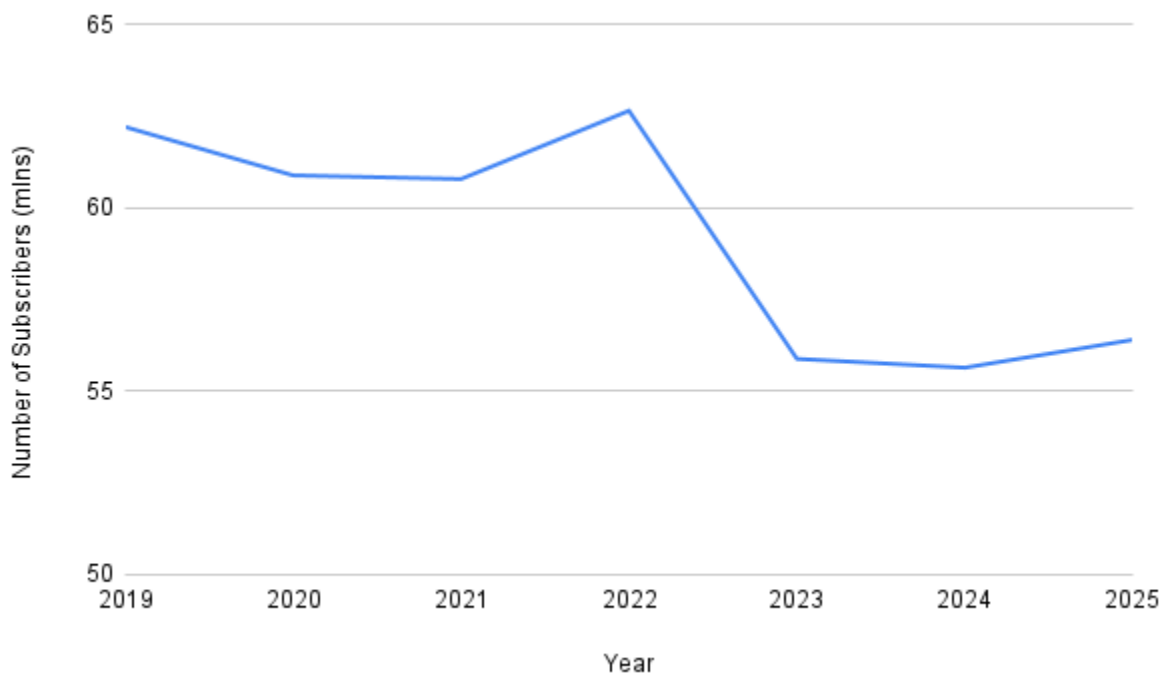
- **PrJSC “Kyivstar”**: The largest mobile operator in the country. As of the end of 2023, the operator’s subscriber base was **23.9 million** users.⁴⁶ According to data for the first 9 months of 2024, the number of subscribers slightly decreased to **23.3 million**, but the 4G user base grew to **15.3 million**, accounting for **65.4%** of the total subscriber base.⁴⁷ The company’s revenue for the first 9 months of 2024 was **26.86 billion UAH**.⁴⁷ According to other data, the total revenue of PrJSC “Kyivstar” for 2024 is estimated at **39.2 billion UAH**.⁴⁰ Website: <https://kyivstar.ua/>
- **PrJSC “VF Ukraine”** (operating under the Vodafone brand): The second-largest mobile operator. As of the end of 2023, its subscriber base was **15.9 million** users.⁴⁶ The company’s total revenue for 2024 is estimated at **23 billion UAH**.⁴⁰ Website: <https://www.vodafone.ua/>

- **LLC “lifecell”**: The third major player. As of the end of 2023, the operator served **11.7 million** registered subscribers, of which **9.9 million** were active (performed a paid operation within the last three months).⁴⁶ The company’s total revenue for 2024 was **14 billion UAH**.⁴⁰ Website: <https://www.lifecell.ua/uk/>

Market shares (approximate, based on active subscriber data as of the end of 2023⁴⁶, total active base of the three operators ~49.7 million taking into account lifecell’s active subscribers):

Kyivstar ~48.1%, Vodafone ~32.0%, lifecell ~19.9%.

Graph 4: Dynamics of mobile BBA subscribers in Ukraine (2019–2025)



The mobile communications market in Ukraine, despite a slight decline in the overall subscriber base of individual operators (e.g., Kyivstar⁴⁷), demonstrates qualitative growth. This is reflected in the increasing share of 4G Internet users and growth in mobile data consumption.³⁸ Such dynamics indicate continued network modernization by operators and user adaptation to services requiring higher speed and traffic volume. Competition among the three main players (“the big three”) remains high, encouraging investment in infrastructure development and service quality improvement. The significant excess of active mobile connections over the country’s total population²⁹ indicates high market saturation and the

widespread practice among Ukrainians of using multiple SIM cards simultaneously, which may be due to the search for better tariffs or coverage in different locations.

2.3. Internet access speed and service quality

The quality and speed of Internet access in Ukraine present a mixed picture with positive dynamics in recent years, despite serious challenges related to the war. According to Ookla (Speedtest.net) data for January 2025, cited by Datareportal and ITC.ua, the median download speed for mobile Internet in Ukraine was **31.23 Mbit/s**. This is a significant increase of **25.8%** compared to the previous year. For fixed broadband access, the median download speed reached **83.81 Mbit/s**, increasing by **13.7%** over the year.²⁹

In the Speedtest Global Index global ranking, Ukraine's position in mobile Internet speed is subject to fluctuations. In February 2025 (publication date of the article, the ranking itself may have been compiled slightly earlier), Ukraine ranked **71st** in the world.⁴⁹ Speedtest data for earlier periods also indicated that the median mobile download speed in Ukraine was below global averages: **22.3 Mbit/s** in May 2022³⁵ and **24.74 Mbit/s** in May 2023.³⁶ This suggests that, despite growth, there remains potential for improving mobile Internet speed characteristics.

Interesting data is provided by the statistics of the digital game distribution service Steam, which reflects the experience of users demanding high connection quality. According to 2024 data, average download speeds from various Ukrainian Internet providers ranged widely: from **42 Mb/s** for "Ukrtelecom" to **120.5 Mb/s** for "Lanet Network".⁴³ Other providers such as Maxnet, Triolan, TENET, Freenet, Volia, and Kyivstar showed speeds in the **53–85 Mb/s** range.⁴³ These figures are generally higher than the national median speeds, which may be due to the specificity of the sample (gamers often choose higher-speed tariffs and providers with better infrastructure) or Steam's measurement methodology.

The Internet Society report analyzing Internet resilience in Ukraine in 2022 indicated some performance degradation (bandwidth and latency) compared to 2021, which is a direct consequence of the war. However, the same report emphasized the significant resilience of the core routing of the Ukrainian Internet segment.⁵⁰ This suggests that the country's backbone infrastructure was able to withstand significant loads and damage. The observed positive dynamics in both mobile and fixed Internet speeds, despite military actions,²⁹ is an important achievement. Nevertheless, especially in the mobile segment, speeds may still lag behind those of the most developed countries.³⁵ Service quality strongly depends on the

specific provider, region, and the current security and power supply situation, which remains tense due to ongoing attacks on energy infrastructure.

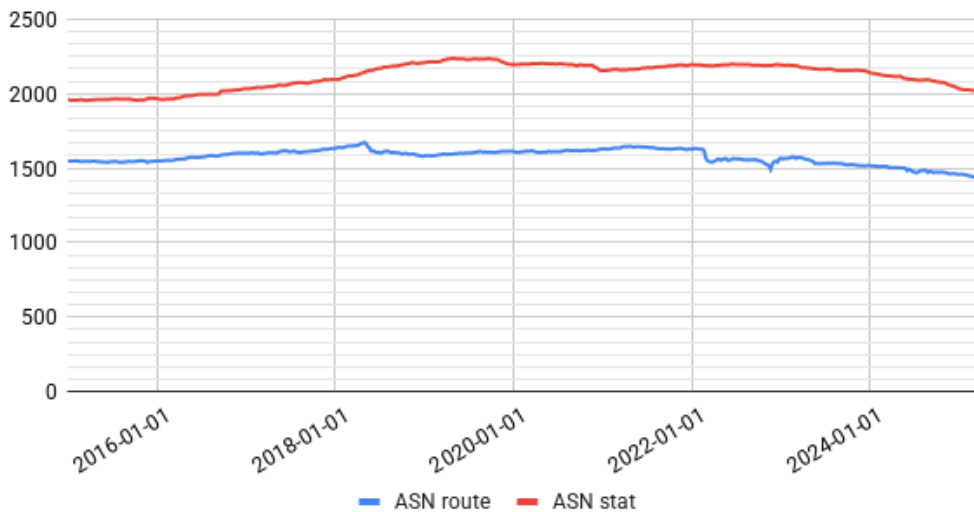
2.4. Development of providers and Autonomous Systems

The number of autonomous systems (AS) in Ukraine, according to RIPE NCC (Regional Internet Registry for Europe, the Middle East, and parts of Central Asia), experienced a noticeable decline after the start of the full-scale Russian invasion in February 2022. If on January 1, 2022, Ukraine had **1,781** active AS, by April 1, 2023, their number decreased to **1,677**, which is **110 AS** (or **6.2%**) fewer.⁵¹ The Internet Society report also indicated **1,793** used AS at the beginning of 2023, which is also less than **1,822** AS a year earlier.⁵⁰

This reduction is apparently a direct consequence of military actions and the occupation of part of Ukrainian territories. Providers operating in these regions may have ceased operations, been disconnected from the Ukrainian network, or forcibly switched to Russian infrastructure. Despite this decrease, the Ukrainian Internet segment retains a high degree of decentralization at several levels, which is confirmed by the presence of a significant number of Internet exchange points (IXP) throughout the country. It was precisely this decentralization, formed before the war, that largely contributed to the overall resilience of the Ukrainian Internet in the face of external threats.⁵¹ The number of foreign upstream AS providing transit to Ukrainian networks also slightly decreased during this period.⁵¹ An important change in the structure of international connectivity was a significant reduction in the role of Russian AS as upstream providers for Ukrainian networks and a reorientation to European and other international providers.⁵¹

Graph 5: Dynamics of Autonomous Systems in Ukraine (2015–2025)

ASN Stat



The graph clearly demonstrates several key stages in the development of the Ukrainian Internet segment:

1. Growth period (2016–2020): Until early 2020, there was steady growth in both the total number of registered autonomous systems (ASN stat) and the number of systems announcing routes (ASN route). This indicates the development of the Internet access market, the emergence of new providers, and decentralization of Internet infrastructure.
2. Peak and stagnation (2020–2022): Around 2020, the total number of AS reached its peak (about 2,250) and began to slowly decline. The number of routable systems also stabilized and peaked at the beginning of 2022.
3. Decline period (since 2022): The most noticeable drop, especially in the number of routable AS, began in 2022. This trend is most likely directly related to the full-scale invasion, which led to the destruction of infrastructure in occupied territories, relocation or closure of businesses.

As of the time of writing the report, there are **2,012** autonomous systems in Ukraine, of which **1,430** are in active routing. This means that about **29%** of registered AS do not announce their networks in the global routing table.

AS density (number of systems per 1 million residents) is an important indicator of market maturity and fragmentation of Internet services. A higher value often indicates a more competitive market with a larger number of small and medium-sized providers.

For Ukraine, with a population of about 39 million and 2,012 autonomous systems, the density is approximately **51.6 AS per 1 million residents**.

This indicator, although high, is somewhat lower than in neighboring countries in the region. For example, Poland, with a comparable population (~37.7 million), has about **2,600** autonomous systems, giving a density of **~69 AS per million residents**. Very similar high figures are shown by the Czech Republic with a density of **~68.8** (750 AS for 10.9 million residents) and Romania with a density of **~63.4** (1,250 AS for 19.7 million residents).

Conclusions:

High level of development: Despite the current decline, Ukraine has historically had and continues to have a very developed and fragmented Internet provider market. The AS density indicator, even being lower than that of neighbors, indicates a high degree of decentralization of Internet infrastructure.

Regional context: Comparison shows that the Ukrainian market may have begun consolidating (enlargement of players) even before 2022. Military actions, in turn, accelerated this process, which is reflected in the gap in density indicators with countries such as Poland and the Czech Republic.

Impact of the war: The obvious decline since 2022 is a direct consequence of the war. Companies in occupied territories ceased to exist, part of the infrastructure was destroyed, and some providers may have been absorbed by larger players in the process of business migration and adaptation.

Overall, the Ukrainian Internet segment demonstrates a high degree of maturity but is undergoing a difficult period of transformation and consolidation, exacerbated by external factors.

Table 1: Top 10 largest Autonomous Systems in Ukraine

#	Number of AS	Name	Web Site	Foreign neighbour count	Local neighbour count	Total neighbour count	Foreign neighbours share
1	48919	Uacity LLC	https://uacity.net	1806	34	1840	98%
2	35320	Eurotranstelec om	https://ett.ua	500	274	774	65%
3	3326	Datagroup PJSC	https://www.datagroup.ua/	168	472	640	26%

4	35297	Dataline Net	https://dataline.ua	194	308	502	39%
5	3255	Uar .net	http://www.uar.net	62	352	414	15%
6	8772	NetAssist LLC	http://www.netassist.ua/	272	128	400	68%
7	199995	Omega Telecom	http://omegatelcom.ua/	154	222	376	41%
8	15895	Kyivstar	https://kyivstar.ua	142	152	294	48%
9	21497	Vodafone Ukraine	https://www.vodafone.ua/	136	146	282	48%
10	44600	LLC "Gigatrans Ukraine"	http://www.gigatrans.ua/	124	136	260	48%

Based on the table of the top-10 largest autonomous systems, the following conclusions can be drawn about the structure of the core of the Ukrainian Internet:

1. Clear division of roles The list of leaders clearly shows companies with different business models and network policies:
 - International gateways (Transit Providers): Companies **Uacity LLC (AS48919)**, **NetAssist (AS8772)**, and **Eurotranstelecom (AS35320)** stand out with a huge share of foreign connections (98%, 68%, and 65% respectively). Their main function is not providing Internet to end users but selling traffic transit to and from Ukraine. Uacity, ranking first in total connections, has only 34 local connections, confirming its status as an almost pure transit operator.
 - National operators and exchange points: On the opposite end are **Datagroup (AS3326)** and **Uar.net (AS3255)**. They, on the contrary, have predominantly local connections (472 and 352 respectively) with a minimal share of foreign ones (26% and 15%). These form the core of the internal Ukrainian Internet. They connect hundreds of other Ukrainian operators, ensuring fast internal traffic exchange.
 - Large retail and mobile operators: **Kyivstar (AS15895)** and **Vodafone (AS21497)**, as well as other providers like Dataline and Omega Telecom, demonstrate a balanced policy. The share of their foreign connections is 40–50%. This is logical for their business model: they need both high-quality access to global resources for their subscribers and developed peering connections within Ukraine for fast content delivery and latency reduction.

2. Dependence on external channels The high positions of operators specializing in international transit underline the importance of external channels for the Ukrainian Internet. A significant portion of traffic does not stay within the country but requires access to global networks.
3. Mature internal ecosystem The large number of local connections at Datagroup and Uar.net indicates a developed internal peering. This allows keeping local traffic within Ukraine, which is critically important for speed of access to Ukrainian resources and overall network resilience.

The table shows that the core of the Ukrainian Internet consists of several large players with clear specialization. Despite the overall large number of autonomous systems in the country (as seen from the previous graph), it is precisely these ten companies that provide key connectivity, both internal and external. The consolidation process noted earlier only strengthens their central role in the functioning of the entire Ukrainian network segment.

The reduction in the number of active autonomous systems is a direct consequence of the war, occupation of part of the territories, and destruction of infrastructure. However, the high level of decentralization and the presence of numerous Internet exchange points that characterized the Ukrainian Internet before 2022⁵¹ created a significant margin of resilience. This allowed the overall operability and connectivity of the Ukrainian network segment to be maintained even under unprecedented challenges. The change in the structure of upstream providers, in particular the sharp decrease in dependence on Russian autonomous systems for international transit,⁵¹ is also an important strategic consequence of the war. This process leads to greater integration of the Ukrainian Internet with European and global networks, although it may have resulted in the loss of some previously existing backup routes through Russia (which, however, in the current geopolitical conditions is difficult to consider an unambiguous negative).

2.5. IPv6 adoption

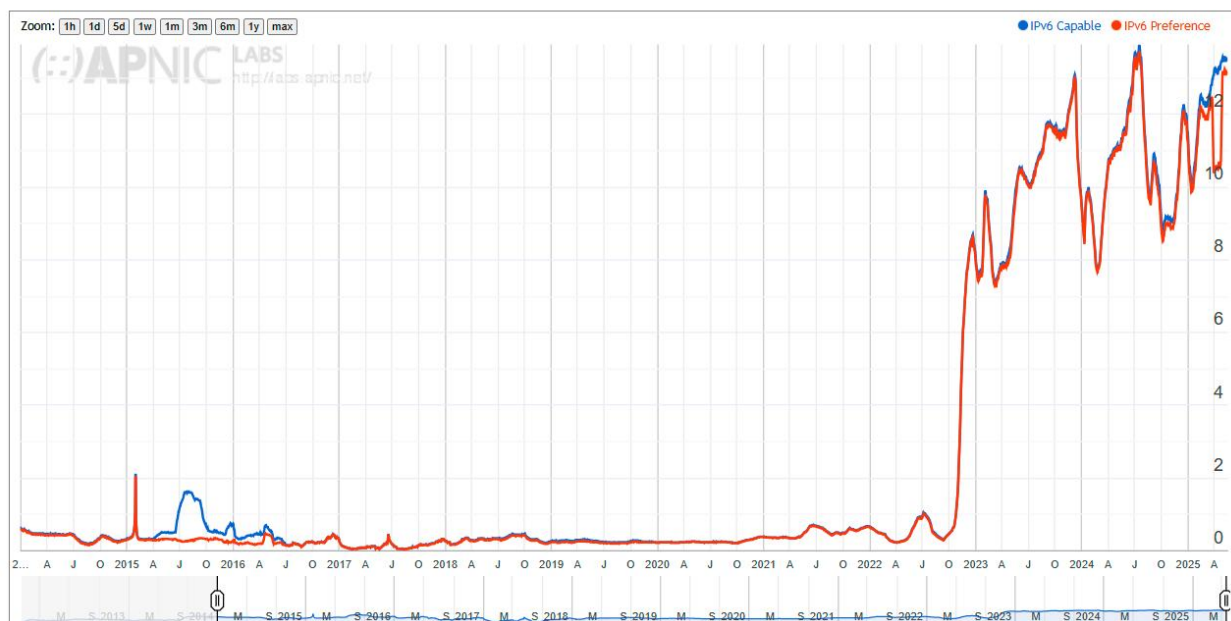
The level of adoption of the new Internet protocol version IPv6 in Ukraine is characterized by slow but steady growth; however, it currently significantly lags behind global and European averages.

As of September 2025, authoritative global monitoring systems show that the share of users accessing the Internet via the IPv6 protocol in Ukraine is about **13%**. In particular, Google statistics record this indicator at **12.99%**, which correlates with data from the analytical platform APNIC Labs.

For comparison, in May 2025, the global average IPv6 adoption level was **39.95%**, and for Europe as a whole — **33.26%**. Thus, Ukraine’s indicator is almost three times lower than the global average. At the same time, it is at the same level as the average for the Eastern Europe region, which is **13.44%**.

Graph 6: Dynamics of IPv6 adoption in Ukraine (2015–2025)

Use of IPv6 for Ukraine (UA)



Source: stats.labs.apnic.net

The graph shows that the IPv6 implementation process in Ukraine began around 2016 but remained practically at zero for the first few years. Noticeable growth began only in 2020, after which the dynamics became more stable. In the period from 2022 to 2025, there is a smooth increase in adoption from approximately **8%** to the current **13%**. Such dynamics

indicate the absence of sharp jumps and systematic, though slow, work by individual providers on transitioning to the new protocol.

It can be concluded that, despite some progress, mass transition to IPv6 in Ukraine has not yet occurred. The current adoption level, comparable to the Eastern European average, speaks of a regional trend but emphasizes the lag behind more developed markets. The main restraining factors are likely the sufficient stock of IPv4 addresses among key market players and the need for significant investments in network infrastructure modernization, which is not a priority task under current conditions. Nevertheless, further development of the digital economy and the Internet of Things (IoT) will require acceleration of the transition to the new protocol to ensure scalability and technological competitiveness of the country.

2.6. Connectivity Index

To assess the level of integration of an Internet segment, two key indicators are used, based on the analysis of pairwise connections (peerings) between Autonomous Systems (ASN).

Global Connectivity Index: This index represents the total number of unique connections between each local ASN and each external (foreign) ASN. Essentially, it measures how widely and diversely the Internet segment is connected to the rest of the world. The higher this indicator, the more “windows” the country has to the global network.

Local Connectivity Index: This index is calculated as the total number of unique connections between different local Ukrainian AS. It reflects the intensity and complexity of the internal Internet market, in particular the activity at Internet exchange points (IXP). A high indicator indicates a developed internal ecosystem that allows efficient internal traffic exchange, minimizing delays and dependence on external channels for local data.

Analysis of the ratio of these two indices allows understanding the strategic orientation of the national network: whether it is predominantly self-sufficient or deeply integrated into the global infrastructure.

Graph 7: Dynamics of global connectivity of Ukrainian Autonomous Systems (2019–2025)

Global connectivity statistics

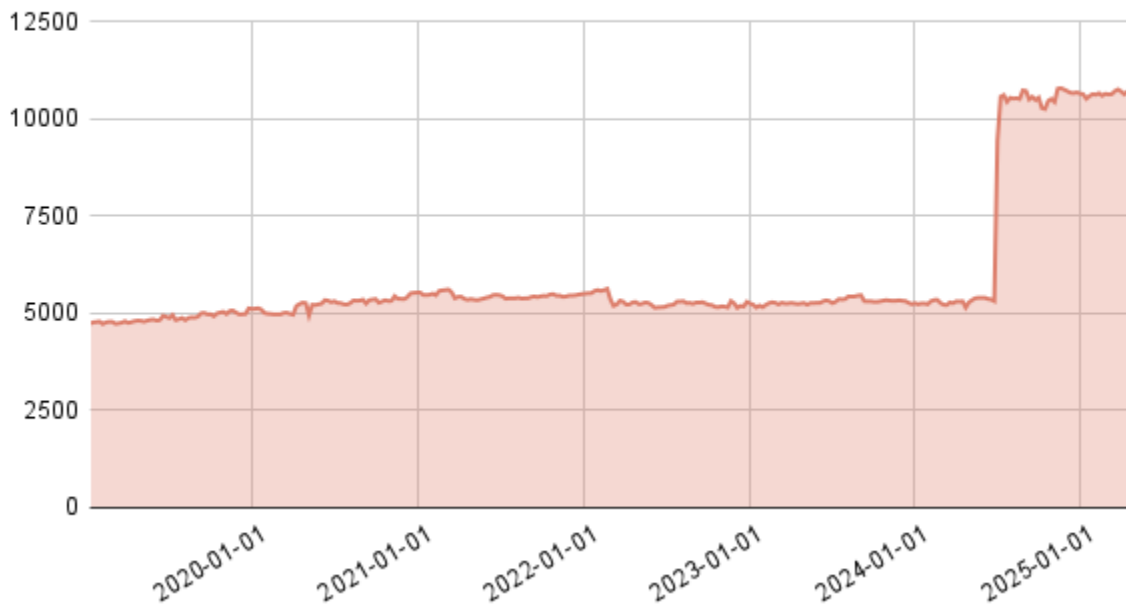


The graph shows the total number of unique connections between Ukrainian and foreign autonomous systems. Until the end of 2024, there was a smooth, organic growth from 2,500 to approximately 4,000 connections. This indicates a consistent increase in the number of “windows” to the outside world and diversification of international connections. The Ukrainian Internet segment was actively increasing its integration into the global network, connecting to an increasing number of foreign partners.

However, at the end of 2024 – beginning of 2025, there was an anomalously sharp, explosive increase in the indicator — more than doubled, to almost 10,000. Such a leap cannot be the result of organic growth and most likely indicates a major structural change: for example, the entry of a new large transit operator with an aggressive peering policy or a radical change in the counting methodology. With a total of 10,000 connections, on average, one of the 2,012 Ukrainian AS has about 5 foreign connections.

Graph 8: Dynamics of local connectivity of Ukrainian Autonomous Systems (2019–2025)

Local connectivity statistics

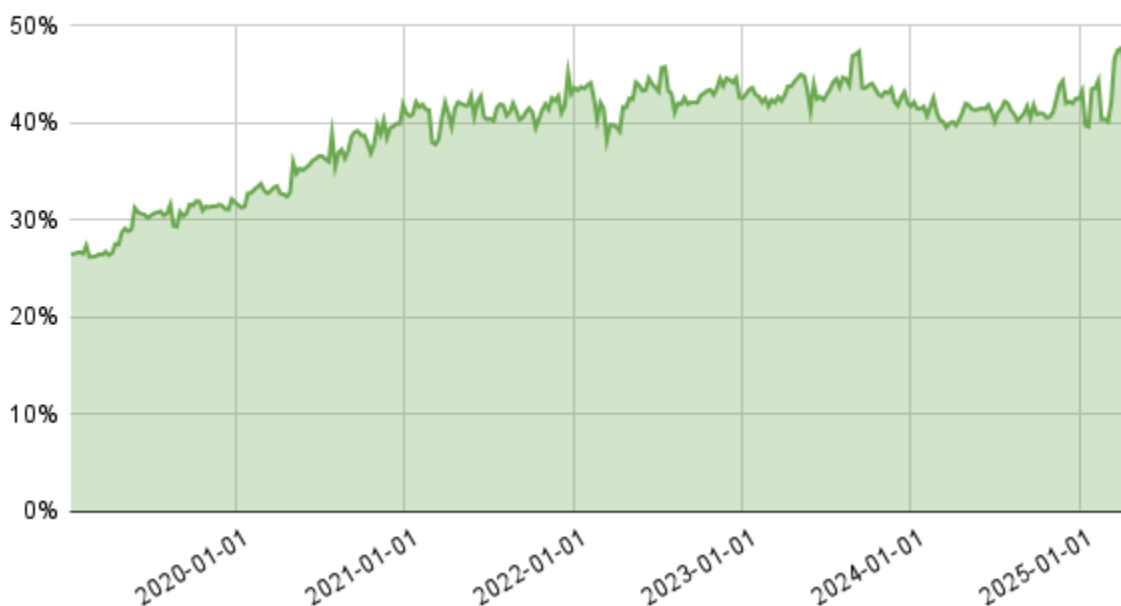


The local connectivity index demonstrates the number of unique connections between Ukrainian AS. For almost five years (from 2020 to the end of 2024), this indicator was incredibly stable, staying in a narrow corridor of 5,000–5,500 connections. Such stability indicates a mature, long-established internal market with established peering relationships, most likely concentrated around key Ukrainian Internet exchange points (IXP).

As with global connectivity, at the end of 2024 there was a one-time jump almost doubled — to 10,500 connections. This also indicates an extraordinary event, for example, the launch of a new powerful exchange point that connected many previously unconnected networks, or a change in the peering policy of one of the central players (such as Datagroup or Uar.net). On average, one Ukrainian AS has slightly more than 5 local connections, which indicates a high density of internal interaction.

Graph 9: Dynamics of the ratio of global and local connectivity of Ukrainian Autonomous Systems (2019–2025)

Total connectivity share



This graph shows the share of global connections in the total number of connections and is key to understanding the strategic orientation of the network. In the period from 2020 to mid-2021, the most important shift occurred: the share of international connections grew from 25% to more than 40%. This was a period of active internationalization when the Ukrainian Internet ceased to be predominantly a local ecosystem and became a deeply integrated part of the global network.

After 2021, the indicator stabilized in the 40–48% corridor. This indicates the achievement of a new balance. The Ukrainian Internet segment has found equilibrium between a developed internal self-sufficiency and broad international integration. The network is neither isolated nor completely dependent on external channels; it maintains a healthy proportion between local and global traffic, which is a sign of a mature and resilient national network infrastructure.

3. Legislation on the Internet

3.1. Principles of Internet governance

The principles of Internet governance in Ukraine are formed under the influence of several key factors: national legislation, obligations to harmonize with European norms and practices within the framework of the European integration course, as well as the current military-political situation related to the full-scale aggression of the Russian Federation. The fundamental legislative acts in this area are the Law of Ukraine “On Electronic Communications”⁵⁵ and the new Law of Ukraine “On Media”⁵⁷, which entered into force in 2023. State policy in the field of the Internet is aimed, on the one hand, at developing digital infrastructure, ensuring universal access to the network and information, supporting the digital economy, and on the other hand, at protecting national interests, information sovereignty, and actively countering disinformation and cyber threats, especially those emanating from the aggressor state.

Internet governance in Ukraine covers various aspects: technical regulation (management of the radio frequency spectrum, numbering resources, standards), economic regulation (ensuring competition in the electronic communications market, tariff policy, consumer rights protection), as well as content regulation (activities of online media, dissemination of information, combating illegal content). The country formally applies a multistakeholder model, involving interaction between state bodies, business (Internet providers, communication operators, technology companies), and civil society institutions. However, under war conditions, the role of the state, especially in matters of content regulation and ensuring national security in cyberspace, has noticeably increased.

3.1.1. Regulation

Internet regulation in Ukraine is carried out through a system of legislative and subordinate normative-legal acts. The key document defining the general legal foundations of activities in the field of electronic communications is the Law of Ukraine “On Electronic Communications” No. 1089-IX of December 16, 2020.⁵⁶ This law establishes the rights and obligations of providers and consumers of electronic communication services, the powers of state bodies in regulating the industry, principles of managing the radio frequency spectrum and numbering resources, as well as the foundations of ensuring universal access to services.

Significant changes in the regulation of the online space were introduced by the Law of Ukraine “On Media” No. 2849-IX of December 13, 2022, which entered into force on March 31, 2023.⁵⁷ This law for the first time comprehensively regulated the activities of online media in Ukrainian legislation, defined procedures for their voluntary registration, established content requirements, as well as liability measures for violations, including the possibility of applying sanctions by the National Council on Television and Radio Broadcasting.³⁶

Ukraine is actively working to harmonize its legislation with European Union norms, especially in the context of fulfilling the Association Agreement and candidate status for EU membership. This concerns, in particular, the implementation of the provisions of the General Data Protection Regulation (GDPR) and adaptation to the requirements of the EU Digital Services Act (DSA) and Digital Markets Act (DMA).⁶¹ Regulatory policy is also largely determined by the tasks of ensuring national security and defense, especially in the context of countering hybrid threats, Russian propaganda, and disinformation.

3.1.2. Regulatory bodies and responsible persons

Several state bodies are responsible for regulating the Internet and related areas in Ukraine:

- **National Commission for the State Regulation of Electronic Communications, Radio Frequency Spectrum and Postal Services (NCEC):** The main independent state collegial body responsible for regulating the electronic communications market. Its powers include licensing activities in the provision of electronic communication services, allocation and supervision of the use of the radio frequency spectrum and numbering resources, ensuring competition, consumer rights protection in telecommunications services, as well as technical regulation. NCEC was created by transforming the National Commission for the State Regulation of Communications and Informatization (NCCIR) in accordance with the Law “On Electronic Communications” from February 2022, aimed at strengthening its institutional independence and transparency, including through a new procedure for selecting commission members.³⁶

 - Official website: <https://nkek.gov.ua/> (previously <https://nkrzi.gov.ua/>).⁶²
 - NCEC leadership: The composition of NCEC members in earlier periods included Viktoriia Yuriivna Troshchenko, Ihor Ivanovych Kolesnyk, Andrii Ivanovych Semenchenko, Mykola Mykolaiovych Tkachenko.⁶⁴ The current composition and the name of the NCEC Chairman should be checked on the official website.
- **Ministry of Digital Transformation of Ukraine (MinTsifry):** The central executive body that forms and implements state policy in the field of digitalization, development of the digital economy, e-governance, provision of electronic public services (in particular through the “Diia” portal and application), development of digital skills among the population, as well as coordinating issues related to cybersecurity at the national level.⁶⁵

 - Head: Mykhailo Albertovych Fedorov – Vice Prime Minister of Ukraine – Minister of Digital Transformation of Ukraine.⁶⁵
 - Official website: <https://thedigital.gov.ua/>.⁶⁵

- **National Council of Television and Radio Broadcasting of Ukraine (NRada):** A constitutional, permanently operating collegial body whose main task is to oversee compliance with legislation in the field of television and radio broadcasting. With the adoption of the Law “On Media” in 2023, the powers of the National Council were significantly expanded and now include regulation of online media activities. This includes voluntary registration of online media, monitoring their content for violations (e.g., dissemination of prohibited information, hate speech, disinformation), as well as applying sanctions, up to fines and initiating court procedures for blocking resources.³⁶
 - Official website: <https://www.nrada.gov.ua/>.
- **Security Service of Ukraine (SBU) and Cyber Police Department of the National Police of Ukraine:** Law enforcement agencies playing a key role in ensuring state cybersecurity, combating cybercrime, countering foreign information operations and disinformation, as well as identifying and countering threats to national security in cyberspace. The SBU, in particular, actively participates in processes related to blocking Internet resources deemed threatening.³⁶

The Internet regulation system in Ukraine is multi-level and includes several agencies with partially overlapping and partially complementary functions. The transformation of NCCIR into NCEC and the significant expansion of the powers of the National Council on Television and Radio Broadcasting to the online media sphere³⁶ indicate attempts by the Ukrainian state to adapt its regulatory framework to modern digital challenges and bring it closer to European standards. However, the concentration of content regulation powers with the National Council, as well as the significant role of security agencies (especially the SBU) in initiating blocks and prosecutions for online activity, raise certain concerns among human rights organizations and media experts regarding potential risks to freedom of speech and the possibility of abuse of the granted powers, especially under martial law.³⁶

3.2. Market monopolization

Ukrainian legislation in the field of electronic communications and economic competition protection is formally aimed at preventing market monopolization and combating abuse of dominant position by individual business entities. The Antimonopoly Committee of Ukraine (AMCU) is the key state body responsible for monitoring compliance with competition legislation. However, in practice, especially in the Internet access and mobile communications markets, there are processes that raise concerns about possible concentration and reduction of competition.

In 2021, the AMCU granted permission to “Datagroup” company to acquire the group of companies operating under the “Volia” brand, which at that time was one of the three largest

Internet providers in Ukraine by subscriber count. According to estimates, “Volia’s” share in the fixed-line Internet market was about **9%**, while “Kyivstar” and “Ukrtelecom” each had approximately **15%**.⁴² This merger led to the creation of one of the largest players in the market and sparked discussions in the expert community about its potential impact on the level of competition.

The Internet Association of Ukraine (InAU), representing the interests of many market participants, has repeatedly expressed concern about statements by individual government officials and initiatives that could lead to monopolization of the Internet access market. In particular, InAU criticized the idea of the need for a mass transition of Internet providers from traditional Ethernet technology to PON (passive optical networks) technology. According to the association, such requirements may be unaffordable for many small and medium-sized providers that form the basis of a competitive market and lead to their displacement by larger players with sufficient resources for large-scale network modernization using PON technology.⁴⁴ The director of the fixed-line Internet development department of the Ministry of Digital Transformation, Yuriy Matsyk, also noted that under frequent power outages, there is a natural flow of subscribers to those providers that can provide more stable Internet access, which is often associated with the use of PON technology.⁴⁴ This objectively strengthens the positions of technologically more prepared companies.

Although there may formally be no absolute monopolists in the market, the largest players such as “Kyivstar”, “Vodafone Ukraine”, and “Lifecell” in the mobile communications market, as well as “Ukrtelecom”, the merged “Datagroup-Volia” company, and “Kyivstar” (in the fixed-line Internet market) occupy dominant or very significant market shares.⁴⁰ Their marketing strategies, pricing policies, and investment decisions have a significant impact on the development of the entire market and the position of other, smaller participants.

Despite the existence of antimonopoly legislation and AMCU oversight, trends toward consolidation in the Internet provider market, as well as technological challenges associated with the need for network modernization under war conditions and the energy crisis, may in the long term lead to a reduction in the number of independent small players and further strengthening of the positions of a limited circle of large companies. This, in turn, may negatively affect the level of competition, pricing, service quality, and the pace of innovation implementation, especially if small providers cannot adapt to changing conditions or are absorbed by larger competitors.

3.3. Internet shutdowns by government order

Ukrainian legislation provides for the possibility of temporary restriction or complete suspension of electronic communication networks and Internet access by decision of state bodies in certain, legally established cases. The main provisions concerning such measures are contained in the Law of Ukraine “On Electronic Communications”, in particular in its Article 115, which regulates the provision of electronic communication services under emergency situations, as well as martial law and emergency situations.⁶⁷ The exact content of this article and detailed procedures require direct reference to the full text of the law.⁶⁹

Under martial law, introduced throughout Ukraine since February 24, 2022, the government and military command received expanded powers that may potentially include establishing a special regime for communication enterprises and control over communications for defense and national security needs.³⁶ However, as noted by international observers, in particular Freedom House, the Ukrainian government on the territory under its control has so far refrained from the practice of nationwide or large-scale regional Internet shutdowns, despite the existence of such legal possibilities.³⁶ Internet outages and serious communication disruptions have mainly been associated with physical destruction of infrastructure as a result of hostilities, cyberattacks, or actions of Russian occupation forces in captured territories.

The decision-making process for Internet shutdowns, specific reasons for such actions, and the list of persons authorized to do so must be clearly detailed in Article 115 of the Law “On Electronic Communications” and relevant normative-legal acts regulating the regime of martial law or emergency situations. It is assumed that decisions of this level are made by the highest state authorities, such as the National Security and Defense Council (NSDC) chaired by the President of Ukraine, or the Cabinet of Ministers of Ukraine, and implemented through the National Commission for the State Regulation of Electronic Communications (NCEC), which communicates the relevant orders to operators and providers of electronic communication services. Grounds for such measures may include the need to ensure national security, defense of the country, maintenance of public order, prevention of mass riots, or conducting counter-terrorism or special military operations.

The existence of a legislative framework allowing Internet shutdowns by government order, especially under prolonged martial law and accompanying restrictions on democratic procedures, creates potential risks to freedom of access to information and freedom of expression. Although until now Ukrainian authorities on controlled territory have not resorted to large-scale arbitrary Internet shutdowns to suppress dissent or restrict access to information,³⁶ the presence of clear legal frameworks, an exhaustive list of grounds, transparent decision-making procedures, and effective control and appeal mechanisms is important to prevent possible abuse of such extraordinary powers. The lack of full transparency in these procedures may cause concern both within the country and among international partners.

3.4. Legislation on “words on the Internet”

In Ukraine, a set of legislative norms is in effect that establish liability for the dissemination of certain information on the Internet. Particular attention is paid to information qualified as “fakes”, disinformation, as well as statements containing calls for violent change or overthrow of the constitutional order, encroachment on the territorial integrity and inviolability of Ukraine, justification or denial of the armed aggression of the Russian Federation, or glorification of its participants.

The concepts of “disinformation” and “fakes” are the subject of active public and expert discussions. For example, there was a public petition to the President of Ukraine proposing the adoption of a special law on countering disinformation, which proposed defining disinformation as “information that may cause panic among the population and/or mislead”.⁷⁰ In practice, legal liability for disseminating “fakes” or disinformation may arise under various articles of the Criminal Code of Ukraine (CC) and the Code of Ukraine on Administrative Offenses (CAO).

After the start of the full-scale Russian invasion, Ukrainian legislation in this area was significantly tightened. In particular, the Criminal Code was supplemented with Article 436-2 “Justification, recognition as lawful, denial of the armed aggression of the Russian Federation against Ukraine, glorification of its participants”.³⁶ This article provides for criminal liability for the production and dissemination of materials containing such statements. Articles of the Criminal Code that existed earlier but acquired new significance in the context of the war are also actively applied: Article 109 (actions aimed at violent change or overthrow of the constitutional order or seizure of state power), Article 110 (encroachment on the territorial integrity and inviolability of Ukraine), and Article 161 (violation of citizens’ equality based on their racial, national affiliation, religious beliefs, disability, and other grounds).³⁶

The new Law of Ukraine “On Media”, which entered into force in March 2023, also contains a list of information whose dissemination in media (including online media) is prohibited. Such information includes, among other things, denial or justification of the criminal nature of communist and national-socialist (Nazi) totalitarian regimes, creation of a positive image of persons who held leadership positions in the communist party or higher bodies of the USSR and Ukrainian SSR, humiliation or insult to the state (Ukrainian) language. Under conditions of armed aggression, it is prohibited to disseminate information that presents the armed aggression against Ukraine as an internal conflict, civil conflict, or civil war, as well as dissemination of unreliable materials regarding the armed aggression and actions of the aggressor state if their consequence is incitement of enmity and hatred or calls for violation of territorial integrity.³⁶

In addition to criminal liability, administrative liability is provided for disseminating false rumors capable of causing panic among the population or disrupting public order under Article 173-1 of the CAO.³⁶ Article 259 of the Criminal Code (“Knowingly false report of a threat to the safety of citizens, destruction or damage to property”) may also be applied to certain types of socially dangerous fake news, for example, about mining of objects or fictitious man-made disasters.⁷²

The Civil Code of Ukraine (Article 277) grants an individual whose non-property rights have been violated as a result of the dissemination of unreliable information about them the right to reply as well as to refutation of such information.⁷¹

Under the ongoing full-scale war, Ukraine has taken significant steps to tighten legislation regarding statements that may be regarded as support for the aggressor state, undermining national security, or disseminating harmful disinformation. Although these measures are aimed at combating real and serious threats to information security, broad and sometimes insufficiently clear formulations in certain legislative acts (for example, the definition of “disinformation causing panic”⁷⁰, or criteria for “collaborative activity” in the information space³⁶) create potential risks to freedom of speech. There is concern that such norms may be used to prosecute critical or unpopular opinions not directly related to support for aggression or high treason. For a democratic society, it is extremely important to maintain a balance between ensuring national security and protecting fundamental human rights, including freedom of expression. This requires clear legal definitions, procedural guarantees, consideration of the context of statements, and effective mechanisms to protect against unjustified prosecution.

3.5. Legislation on Internet blocking

Ukrainian legislation provides for several different mechanisms for blocking (restricting access) to Internet resources. These mechanisms have been formed and evolved over recent years, especially intensively after 2014 and with the start of the full-scale Russian invasion in February 2022, when issues of information security and countering hostile influence in cyberspace became of paramount importance.

One of the key and most widely used blocking mechanisms is the application of sanctions by the National Security and Defense Council of Ukraine (NSDC). NSDC decisions on the application of personal special economic and other restrictive measures (sanctions), which may include a ban for Internet providers to provide access to certain web resources, are put into effect by decrees of the President of Ukraine.⁷³ This mechanism is mainly used to block

Internet resources associated with the aggressor state (Russian Federation), its state bodies, propaganda media, as well as individuals and legal entities under sanctions.

3.5.1. Legislation

The legal basis for blocking Internet resources in Ukraine consists of several key legislative acts:

- **Law of Ukraine “On Electronic Communications” (No. 1089-IX of 16.12.2020):** This law contains special articles regulating the procedure for restricting access to websites on various grounds. In particular, Article 115-1 defines the procedure for restricting access to websites used for providing online media services in violation of the law. Article 115-2 establishes the procedure for restricting access to websites used for providing media-on-demand services and audiovisual service provider services if these services are controlled by or originate from the aggressor state. Article 115-3 regulates restriction of access to websites used for organizing or conducting gambling without an appropriate license or providing access to such games.⁶⁷
- **Law of Ukraine “On Media” (No. 2849-IX of 13.12.2022, entered into force on 31.03.2023):** This comprehensive law granted the National Council of Ukraine on Television and Radio Broadcasting (National Council) significant powers to regulate online media activities. The National Council received the right to apply various sanctions to online media for violations of the law, including imposing fines, canceling registration (for registered online media), and, in case of systematic or gross violations, applying to court with a claim for blocking (restricting access) to the relevant online media.³⁶
- **Law of Ukraine “On Sanctions” (No. 1644-VII of 14.08.2014):** This law is the legal basis for Ukraine’s application of sanctions against foreign states, foreign legal and natural persons, as well as other entities involved in terrorist activities or otherwise threatening national interests, national security, sovereignty, and territorial integrity of Ukraine. Decisions on the application, cancellation, and amendment of sanctions are made by the NSDC and put into effect by a decree of the President of Ukraine. Blocking of Internet resources is one of the types of sanctions provided for by this law.
- **Criminal Procedure Code of Ukraine (CPC of Ukraine):** In the framework of criminal proceedings, especially those concerning cybercrime, dissemination of child pornography, fraud, illegal trafficking of drugs or weapons, as well as crimes against the foundations of national security, courts may make decisions to restrict access to web resources. This is often done by imposing an arrest on “property rights of intellectual property that arise for Internet users when using a web resource”.⁷⁵ This practice is subject to criticism from human rights defenders due to its lack of

transparency, broad interpretation, and potential for abuse, as it can lead to blocking entire platforms or resources not directly related to the substance of the criminal case.

3.5.2. Blocking procedures

Blocking procedures for Internet resources in Ukraine depend on the legal mechanism applied in each specific case:

- **Blocking based on NSDC decision (sanctions mechanism):**
 1. The National Security and Defense Council of Ukraine at its meeting adopts a decision on the application of sanctions, which includes a list of specific individuals and legal entities, as well as web resources subject to blocking.
 2. The President of Ukraine by his decree puts this NSDC decision into effect.⁷³ The decree together with appendices (lists) is published on the official website of the President.
 3. The decree and the relevant NSDC decision are sent to the National Commission for the State Regulation of Electronic Communications, Radio Frequency Spectrum and Postal Services (NCEC).
 4. NCEC (previously NCCIR) brings this decision to the attention of all providers of electronic communication services (Internet providers and mobile operators), who are obliged to technically ensure the blocking of the specified resources for their subscribers.⁷⁵
- **Blocking by decision of the National Council on Television and Radio Broadcasting (in accordance with the Law “On Media”):**
 1. The National Council monitors the activities of media, including online media.
 2. In case of detection of violations of the law (for example, dissemination of prohibited information, hate speech, disinformation), the National Council may issue an order to the media entity to eliminate the violation and/or impose a fine.
 3. In case of significant or gross violations committed by an entity in the field of online media, or repeated violations after fines have been applied, the National Council has the right to apply to court with a claim for temporary prohibition (blocking) of the dissemination of an unregistered online media on the territory of Ukraine or for cancellation of registration of a registered online media and prohibition of its dissemination.³⁶ The decision on blocking is made by the court.
- **Blocking by court decision (within criminal proceedings):**
 1. During pre-trial investigation, the investigator or prosecutor, if there are grounds to believe that a certain web resource is used to commit a criminal offense or contains evidence, applies to the investigating judge with a motion to

impose an arrest on property rights of intellectual property related to the functioning of the given web resource.

2. The investigating judge considers the motion and issues a ruling (uhvala) granting the motion or refusing it.
 3. In case of a decision to arrest property rights and actual blocking of the resource, this court ruling is sent to NCEC, which in turn informs Internet providers of the need to technically restrict access to the specified resource.⁷⁵ This procedure is often criticized for insufficient adversarial nature, lack of proper notification of resource owners before blocking, and difficulties with prompt appeal of such decisions.
- **Blocking on grounds provided for in Articles 115-1, 115-2, 115-3 of the Law “On Electronic Communications”:** Detailed procedures for these specific cases (illegal online media, services of the aggressor state, illegal gambling) must be prescribed in the law itself and subordinate acts. It is assumed that decisions are made by authorized state bodies (probably the National Council on Television and Radio Broadcasting or NCEC upon submission by other competent bodies, such as the SBU or the Commission on Regulation of Gambling and Lotteries) and then executed by Internet providers.

3.5.3. Registries of blocked Internet resources

In Ukraine, there is currently no single, official, public, and comprehensive registry of all blocked Internet resources that would be updated in real time, contain clear legal grounds for each blocking, information about the body that made the decision, blocking periods, and appeal procedures. This creates certain problems with transparency and accountability of the entire blocking process, as well as complicates the ability of resource owners and the public to track and challenge such decisions.

Information about blockings is scattered across various sources:

- **NCEC** (previously NCCIR) on its official website publishes some orders, letters, and recommendations concerning the need to block certain resources. This usually occurs in execution of NSDC decisions or court rulings.⁷⁵ However, these publications are not always systematic and do not constitute a single, easily accessible database.
- **Decrees of the President of Ukraine** on putting NSDC decisions into effect are official documents and are published on the President’s website. Lists of sanctioned persons and companies, as well as lists of web resources subject to blocking, are often contained in appendices to these decrees. These documents are public, but searching for specific information about the blocking of a particular site can be difficult due to the large volume of data and the lack of a specialized search interface.

- **Court decisions** on the arrest of property rights of intellectual property related to web resources are contained in the Unified State Register of Court Decisions. However, access to them and searching for information about specific blocked sites also require certain efforts and are not always obvious to the general public.

The absence of a single, centralized, and easily accessible official registry of blocked resources is a significant shortcoming of the Internet regulation system in Ukraine. This reduces the level of legal certainty, complicates public control over the actions of authorities in this sensitive area, and can lead to cases of erroneous or excessive blocking.

As already noted, there is no single official and exhaustive registry of blocked Internet resources in Ukraine. However, information can be found in the following sources:

Official (or quasi-official) sources:

- Orders and letters of **NCEC** (National Commission for the State Regulation of Electronic Communications, Radio Frequency Spectrum and Postal Services): Published on the official NCEC website (<https://nkek.gov.ua/>; previously <https://nkrzi.gov.ua/>). These documents usually contain lists of resources subject to blocking based on NSDC decisions or courts and are addressed to Internet providers for execution.⁷⁵ However, these are separate documents, not a single database.
- **Decrees of the President of Ukraine** on putting NSDC decisions into effect: Published on the official website of the President of Ukraine. Lists of blocked web resources are contained in appendices to these decrees.⁷³
- **Unified State Register of Court Decisions**: Contains texts of court decisions, including rulings of investigating judges on the arrest of property rights of intellectual property related to web resources, which effectively means their blocking. Search requires knowledge of case details or keywords.

Unofficial registries and monitoring projects:

- **UABlacklist.net**: This resource positions itself as an open and publicly available registry of Internet resources blocked on the territory of Ukraine. The project collects information from various open sources, including court decisions, decrees of the President (NSDC decisions), NCEC orders, and other official documents. For each blocked resource, they try to indicate the domain, reason for blocking, date of the decision, and the body that made it.⁷⁷ Link: <https://uablacklist.net/uk/>. The portal allows users to check the blocking status of a specific Internet resource.
- Projects of public organizations and media: Some Ukrainian non-governmental organizations dealing with digital rights and freedom of speech issues (e.g., “Laboratory of Digital Security”, “Institute of Mass Information”), as well as specialized

media, periodically publish analytical materials and reviews of blocking practices, sometimes with lists of affected resources. For example, the “Laboratory of Digital Security” mentioned the blocking of 191 sites during the war.⁷⁶ The National Commission for State Language Standards may also publish lists of sites violating language legislation, which may potentially lead to sanctions. Ukrinform reported on the expansion of the list of banned sites with pirated movies, including numerous mirrors of Baskino, Filmix, HD REZKA.⁷⁹

The work of unofficial registries such as UABlacklist.net is important for increasing transparency in the field of blocking, providing aggregated information in a user-friendly form. However, the completeness and timeliness of such resources depend on the availability and timeliness of updating information from official sources.

3.5.4. Development of Blocking

Data from the Open Observatory of Network Interference (OONI), a global project for monitoring internet censorship, provide valuable information on blocking practices in Ukraine, especially in the context of the Russian invasion. OONI uses software run by volunteers to detect blocking of websites, applications, and the presence of traffic filtering systems (middleboxes).⁸⁰

Key points from reports and data concerning Ukraine and the region (including Russia's actions affecting Ukraine):

- Censorship in Russia affecting occupied territories of Ukraine: After the full-scale invasion in February 2022, Russian internet providers began massively blocking access to independent news resources, social networks (Twitter, Facebook, Instagram) and sites of international media (BBC, Deutsche Welle, Radio Free Europe, Voice of America, Meduza, etc.).⁸⁰ These same blocks extended to occupied territories of Ukraine, where internet traffic was forcibly rerouted through Russian networks. For example, in April 2022 in occupied Kherson, internet connections were rerouted through Russian networks, leading to blocking of Ukrainian news sites, Instagram and Facebook.³⁵
- Geoblocking: A study conducted after the 2022 invasion revealed cases of geoblocking both from Russian state domains (restricting access for users outside Russia and Kazakhstan), and from foreign news and educational resources that blocked access for Russian users.⁸² This reflects a broader picture of “internet fragmentation”.
- Blocking in Ukraine itself (controlled territory): Freedom House in the “Freedom on the Net 2023” report (covering the period up to May 2023) notes that the Ukrainian government blocks numerous Russian and pro-Russian websites based on “sanctions”

introduced since 2017. After the 2022 invasion, NCEC ordered the blocking of more than 48 million Russian IP addresses used for disinformation or cyberattacks. In March 2023, a phishing domain filtering system was deployed, raising concerns about possible excessive blocking.³⁶

- OONI data on Ukraine: Direct search in the OONI Explorer database⁸³ is necessary to obtain current and detailed results on specific blocked sites and applications on Ukrainian territory. OONI confirmed blocking of various resources in different periods.
- General trends in the region: OONI reports record growth in internet censorship and blocking during conflicts and political instability.⁸⁰ The war in Ukraine has become a catalyst for strengthening information control on both sides.

Conclusion on the development of blocking:

The practice of blocking internet resources in Ukraine significantly intensified after 2014 and especially after Russia's full-scale invasion in 2022. The main goals of blocking by Ukrainian authorities are countering Russian propaganda and disinformation, protecting national security and combating cyber threats. For this, sanction mechanisms (NSDC decisions), court decisions and new powers of regulators (National Council on TV and Radio Broadcasting) are used. In territories occupied by Russia, the imposition of the Russian model of internet censorship with blocking of Ukrainian and independent international resources is observed. Although the actions of Ukrainian authorities to block hostile resources under war conditions may be justified by national security considerations, it is important to ensure transparency of procedures, possibility of appeal and protection against excessive or unjustified restriction of access to information, so as not to cause disproportionate damage to freedom of speech.

4. Human Rights Violations on the Internet

In Ukraine, especially in the context of the ongoing full-scale armed aggression by the Russian Federation, various human rights violations on the internet are recorded. These violations have different natures: some are related to actions of Ukrainian authorities in ensuring national security and countering hostile propaganda, others, much more massive and gross, are a consequence of actions by Russian occupation forces in captured territories and cyberattacks directed against Ukraine.

Reports from international human rights organizations, such as Freedom House and the US State Department, indicate that under martial law in Ukraine, certain restrictions on democratic freedoms were introduced, including freedom of the press and access to information, although it is noted that these restrictions are not comparable in scale to violations committed by Russia.⁸⁴ Main concerns relate to website blocking procedures, criminalization of certain statements and pressure on media. In occupied territories, the situation with digital rights is catastrophic: Ukrainian communication is disconnected, forced switching to Russian internet with its censorship, persecution for pro-Ukrainian statements and use of Ukrainian online resources.

4.1. Internet Shutdown by Government Order

In practice, in territories controlled by the Ukrainian government, large-scale internet or communication service shutdowns by direct government order to suppress protests or restrict access to information for broad segments of the population from 2019 to 2025 have not been recorded in reports from international observers such as Freedom House.³⁶ The Ukrainian government, despite the existence of legislative possibilities for introducing restrictions on communication networks under martial law (according to Article 115 of the Law "On Electronic Communications" and general provisions on martial law)³⁶, refrained from applying such measures on a national scale.

However, the situation is radically different in territories temporarily occupied by the Russian Federation in Ukraine. There, Russian occupation authorities systematically resort to disconnecting Ukrainian mobile operators and internet providers, forcibly rerouting internet traffic through Russian networks subject to strict censorship and filtering, as well as complete or partial blocking of internet access.³⁵

- Examples and cases (in occupied territories and as a result of RF actions):
 - Cyberattack on Viasat (February 2022): One of the first acts of war was a Russian cyberattack on the Viasat satellite network, which provided internet connectivity for part of Ukrainian users and military. This led to large-scale disruptions in internet access not only in Ukraine but also in other European countries.⁸⁵
 - Kherson (April 2022 and onward): After the occupation of Kherson, Russian military rerouted internet traffic through Russian networks, blocking access to Ukrainian news sites, Facebook, Instagram, and other resources banned in the RF.³⁵ Ukrainian mobile communication was disconnected.

- Mariupol (spring 2022): During the siege and capture of Mariupol, Russian troops deliberately destroyed communication infrastructure, leading to a complete information vacuum for the city's residents.⁸⁵
- Other occupied territories: Similar practices of disconnecting Ukrainian networks, blocking Ukrainian resources, and imposing Russian internet were observed in other occupied districts of Zaporizhzhia, Luhansk, Donetsk oblasts.⁸⁶
- Targeted attacks on infrastructure: Russian troops repeatedly struck telecommunications infrastructure, including television towers and mobile base stations, leading to temporary or prolonged communication outages in various regions.⁸⁵
- Shutdowns related to hostilities and destruction of energy infrastructure: Massive Russian strikes on Ukraine's energy facilities from autumn 2022 led to large-scale power outages, which in turn caused disruptions in the operation of internet providers and mobile operators, as their equipment requires power supply. These were not shutdowns "by order of Ukrainian authorities", but a consequence of the aggressor's military actions.³⁶

Thus, cases of shutdowns and large-scale internet outages in Ukraine from 2019 are predominantly related to actions of the Russian Federation both in occupied territories and as a result of cyberattacks and shelling of infrastructure in territory controlled by the Ukrainian government.

4.2. Criminalization of Statements on the Internet

In Ukraine, especially after the start of the full-scale Russian invasion in February 2022, there is a tightening of legislation and law enforcement practice regarding statements on the internet that may be regarded as a threat to national security, support for aggression, or dissemination of disinformation. This has led to an increase in the number of criminal and administrative cases initiated against citizens for their online activity.

- Legislative basis: As mentioned in section 3.4, the key articles of the Criminal Code of Ukraine applied for prosecution for statements on the internet are:
 - Article 109: Actions aimed at violent change or overthrow of the constitutional order or seizure of state power.
 - Article 110: Encroachment on the territorial integrity and inviolability of Ukraine.
 - Article 111-1: Collaborative activity (including public denial of armed aggression, public calls for support of decisions/actions of the aggressor state).

- Article 436-2: Justification, recognition as lawful, denial of the armed aggression of the Russian Federation against Ukraine, glorification of its participants.³⁶
- Administrative liability may arise under Article 173-1 of the CAO for disseminating false rumors capable of causing panic.³⁶
- Practice of application and cases:
 - According to Freedom House, after the 2022 invasion, Ukrainian courts began actively issuing guilty verdicts under Articles 109, 110, 111-1, and 436-2 of the Criminal Code. As of March 20, 2023, 1,609 criminal proceedings were opened under Article 436-2 (justification of aggression).³⁶
 - In 2022, according to the same source, 230 people were imprisoned for disseminating anti-Ukrainian propaganda.³⁶
 - Examples of cases (from Freedom House report³⁶ and other sources):
 - Several men were sentenced to imprisonment for posts on social networks expressing support for Russian military or justifying the invasion.
 - One person was convicted for creating a propaganda website.
 - A blogger was arrested for disseminating pro-Kremlin disinformation.
 - Persons expressing support for the Wagner PMC or calling for overthrow of the government also became defendants in criminal cases.
 - A person working for politician Viktor Medvedchuk (accused of treason) was charged with treason for disseminating false information.
 - A case was recorded where a pensioner was convicted for "likes" under videos of Russian military attacks.
 - The administrator of a pro-Russian Telegram channel was sentenced to six years in prison.
 - A woman was convicted for insulting a military officer on Facebook.
 - Another resident was convicted for calls for violent overthrow of power on TikTok.
 - Pro-Russian bloggers were detained and charged with treason.
 - In occupied territories, Russian authorities also persecute citizens for pro-Ukrainian statements on the internet, conducting phone searches and holding accountable for subscriptions to "propaganda resources of the Kyiv regime".³⁶
 - Article 259 of the Criminal Code (knowingly false report of a threat) may also be applied to disseminating fake news, for example, about "chemtrails".⁷²
 - In 2023, the Cyber Police Department received 18,716 citizen appeals (9% of the total) regarding calls from fake banks and 15,233 appeals (7%) regarding phishing.⁸⁹ Although this is not direct criminalization of statements, it shows

activity in the field of online fraud, which may also affect freedom of information.

Although the authorities' efforts to counter real information threats and aggressor propaganda are understandable under war conditions, human rights defenders express concern about the breadth of some formulations in legislation and the risk of their selective application. It is important to ensure that prosecution for online statements is not used to suppress legitimate criticism or opposition opinions not related to direct support for aggression or calls for violence.

4.3. Persecution of Media and NGOs

With the start of the full-scale Russian invasion in February 2022, Ukrainian mass media (media) and non-governmental organizations (NGOs) faced unprecedented challenges and threats. The main mass of persecution and pressure cases come from the Russian Federation and its occupation forces in captured territories. However, in territory controlled by the Ukrainian government, situations also arise that cause concern among the media community and human rights defenders.

- Actions of Russia and occupation authorities:
 - The Institute of Mass Information (IMI) recorded 836 crimes committed by Russia against journalists and media in Ukraine over three years and three months of full-scale invasion (as of May 2025).⁹⁰
 - These crimes include murders and injuries of journalists, abductions, hostage-taking (including relatives of journalists, as in the case with the father of the "RIA-Melitopol" journalist⁹⁰), illegal detentions (for example, Zaporizhzhia journalist Iryna Dubchenko⁹⁰), shelling of editorial offices, cyberattacks on media sites, seizure and destruction of equipment, coercion to cooperate, dissemination of disinformation and propaganda through captured media.
 - In occupied territories, Ukrainian journalists and independent media were forced to either cease operations, go underground, or evacuate. Occupation authorities create their own propaganda media and block access to Ukrainian information resources.
- Situation in territory controlled by the Ukrainian government:
 - Pressure and restrictions of wartime: Under martial law, media activities are regulated more strictly. A single information telethon "United News" was introduced, which, in the opinion of some observers, limits pluralism of opinions on air.¹⁹ Journalists face restrictions on access to information, especially in

combat zones, and the need to coordinate materials concerning military operations.

- Law "On Media": The new Law "On Media", which entered into force in March 2023, expanded the powers of the National Council on Television and Radio Broadcasting, granting it the right to register and apply sanctions to online media.³⁶ Although the law is aimed at harmonization with European standards, some of its provisions and the broad powers of the regulator cause concerns among part of the media community regarding possible pressure on independent media.
- Cases of pressure and obstruction:
 - The National Union of Journalists of Ukraine (NUJU) expressed concern about statements from the editorial office of the online publication "Ukrainska Pravda" and other journalists about pressure from individual representatives of power structures, in particular the Office of the President.⁹¹
 - In Rivne Oblast in 2024, investigative journalists faced black PR, DDoS attacks on their sites, threats in messengers, and obstruction in work. Police opened criminal proceedings on some of these facts.⁹² For example, a journalist was not allowed to a meeting on financing voluntary formations, on which fact a case was opened for obstruction of journalistic activity.⁹²
- Cyberattacks: Ukrainian online media regularly become targets of cyberattacks, mainly from Russian hacker groups. This includes DDoS attacks, hacks of sites and social media accounts, phishing campaigns.³⁶
- Financial difficulties: Many independent media experience serious financial difficulties due to the fall of the advertising market caused by the war, making them more vulnerable and dependent on grant support or other funding sources.³⁶

Overall, the main threat to media and NGOs in Ukraine comes from Russian aggression. However, in controlled territory, there are also challenges related to the need to maintain a balance between information security under war conditions and freedom of speech, as well as preventing unwarranted pressure on independent media and public organizations. Transparency of online media in Ukraine, according to IMI data, grew to 80% in 2024, mainly due to disclosure of information about leaders.⁹⁴

5. Civil Society in the Field of Internet Governance

Civil society in Ukraine plays an active role in issues related to Internet governance, protection of digital rights and freedoms. Ukrainian non-governmental organizations (NGOs), expert groups, and activists participate in legislation development, monitor human rights violations in the online environment, engage in educational activities in digital security, and advocate for the preservation of an open, free, and secure Internet. Their role has especially increased after 2014 and with the start of Russia's full-scale invasion, when digital space became one of the arenas of confrontation.

Many organizations focus on aspects such as freedom of speech on the Internet, protection of personal data, countering disinformation, cybersecurity for activists and journalists, as well as monitoring Internet resource blocks. They cooperate with international partners, state bodies (where possible and appropriate), and Internet business to promote human rights standards in the digital sphere. Under war conditions, the activities of many NGOs are also aimed at documenting war crimes using digital evidence and providing assistance to victims of cyberattacks and information wars.

5.1. Organizations

In Ukraine, there is a number of organizations actively engaged in protecting citizens' rights on the Internet, promoting digital freedoms, and developing responsible Internet governance. Among them are:

- **Digital Security Lab Ukraine (Лабораторія цифрової безпеки):** This non-governmental organization, founded in 2017, provides assistance to journalists, civil activists, and human rights defenders in solving digital security problems. DSLU also promotes the protection of human rights on the Internet, influencing state policy in the field of digital rights.⁶¹ The organization conducts digital security trainings, security audits for NGOs and media, provides support in cyber incidents, develops educational materials (for example, for the YAK platform), and actively participates in the development of legislation concerning personal data protection, regulation of artificial intelligence, and media freedom.⁶¹ In 2023, DSLU was awarded the Front Line Defenders award for human rights defenders at risk.⁹⁵
 - Website: <https://dslua.org/>

- Reports and publications: DSLU regularly publishes reports and analytical materials, such as "Human Rights in the Digital Dimension 2024"⁹⁶, annual reports on its activities⁶¹, as well as studies on disinformation and media regulation.⁹⁷
- **Інститут масової інформації (IMI):** Leading Ukrainian non-governmental media organization engaged in monitoring freedom of speech, violations of journalists' rights, researching media content quality, combating disinformation and "jeansa" (hidden advertising). IMI actively tracks crimes against journalists and media, especially in the context of Russian aggression.⁹⁰ The organization also conducts research on online media transparency⁹⁴ and analyzes pressure on journalists.
 - Website: <https://imi.org.ua/>
 - Reports and monitorings: IMI regularly publishes "Barometer of Freedom of Speech", monitorings of Russian crimes against media, studies of jeansa, fakes, and other analytical materials.¹⁰
- **Інтерньюз-Україна (Internews Ukraine):** One of the largest NGOs in Ukraine working in the field of media and communications. The organization implements projects aimed at developing independent media, increasing media literacy, supporting quality journalism, countering disinformation, and developing digital rights. "Інтерньюз-Україна" conducts research on Ukrainians' media consumption⁹⁹, releases analytical reports on the state of the media sphere, including regional media¹⁰⁰, and organizes educational events.
 - Website: <https://internews.ua/>
 - Reports: Annual activity reports¹⁰⁰, media consumption studies⁹⁹, reports on digital rights in the context of the COVID-19 pandemic¹⁰¹ and war.¹⁰²
- **Freedom House Ukraine:** Representation of the international human rights organization that monitors the state of political rights and civil liberties in Ukraine, including Internet freedom. Publishes annual "Freedom on the Net" and "Freedom in the World" reports on Ukraine, analyzing legislation, blocking practices, cases of persecution for online activity, and other aspects of digital rights.¹⁹
 - Website (global with section on Ukraine): <https://freedomhouse.org/country/ukraine>

These and other organizations make a significant contribution to shaping the agenda in the field of digital rights, provide practical assistance to users and organizations, and act as important partners for state bodies in the process of reforming legislation and practices in accordance with international standards.

5.2. VPN and Means of Bypassing Blocks

The use of VPN (Virtual Private Network) and other means of bypassing blocks has gained additional relevance in Ukraine, especially in the context of blocking Russian internet resources by Ukrainian authorities and, much more importantly, for residents of temporarily occupied territories, where Russian occupation authorities block access to Ukrainian and independent international information resources, as well as impose the use of Russian internet with its system of total censorship. VPN services allow encrypting internet traffic, changing the user's IP address, bypassing geographical restrictions and blocks, as well as increasing the level of anonymity and security on the network.¹⁰³

In territory controlled by the Ukrainian government, the use of VPN is not prohibited and is a common practice for accessing content that may be restricted geographically (e.g., streaming services), for protecting data when using public Wi-Fi networks, as well as for accessing sites blocked under sanctions (e.g., previously popular Russian social networks). In temporarily occupied territories, VPN becomes a vital tool for accessing objective information, communicating with relatives in free territory, and protecting from surveillance by occupation authorities.⁸⁶

5.2.1. Status of VPN Services

In Ukrainian territory controlled by the government, the use of VPN services is legal and not prohibited.¹⁰⁵ There is no special legislation that would directly regulate, restrict, or prohibit the use, advertising, or sale of VPN services for ordinary citizens. Ukrainian users can freely choose and use VPN services at their discretion.

Ukrainian state bodies, in particular the Center for Countering Disinformation under the NSDC and the State Service for Special Communications and Information Protection, even recommended the use of VPN services for citizens in temporarily occupied territories or in areas where their internet traffic may be intercepted or filtered by Russian providers. This is done to ensure access to Ukrainian information resources, protect personal data, and bypass Russian censorship.⁸⁶

The situation is different in territories temporarily occupied by Russia in Ukraine. There, occupation authorities try to block not only access to independent sites but also to VPN services themselves, applying the same methods as in the Russian Federation. Roskomnadzor (Russian regulator) actively fights VPN, blocking IP addresses of VPN servers and information on ways to bypass blocks.¹⁰⁶ These measures extend to occupied Ukrainian territories.

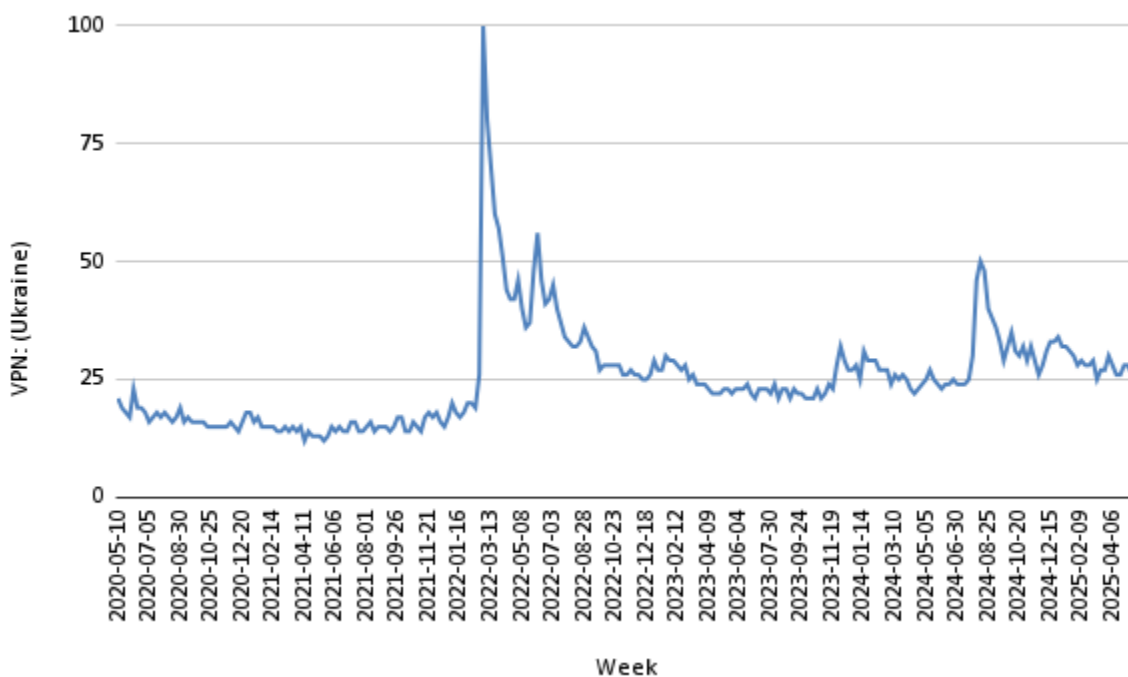
Thus, the legal status of VPN services in Ukraine (in controlled territory) remains free, and they are considered a legitimate tool for ensuring privacy and access to information.

5.2.2. Number of VPN Users

Accurate data on the number of VPN users in Ukraine and their dynamics by year is quite difficult to collect, as many VPN services do not publish detailed statistics by country, and VPN use is often situational. However, based on indirect data and general trends, one can judge the growth in VPN popularity, especially after 2014 (start of blocking Russian sites) and especially after February 2022 (full-scale invasion and intensification of information confrontation).

- Global and regional trends:
 - According to AtlasVPN, in 2020, 277 million VPN app downloads were recorded worldwide, in 2021 — 785 million, and in 2022 — 353 million.¹⁰⁸ In 2023, the number of downloads was about 328 million.¹⁰⁹
 - In March 2022, after the Russian invasion, search interest in VPN in Ukraine grew by about 600% compared to the previous 30-day period. This was associated both with Russian cyberattacks on Ukrainian online infrastructure and with users' desire to access blocked resources or increase their security.¹¹⁰
 - In Russia, demand for VPN also sharply increased (by 668% for the same period¹¹⁰, and according to AtlasVPN, by 1906% per week¹⁰⁹) due to blocking of Western social networks and media. This indirectly indicates that in occupied territories of Ukraine, where Russian internet is imposed, the need for VPN should also have been high.
- Data on Ukraine (limited):
 - Reports from Statista and Top 10 VPN mention a sharp surge in VPN search queries in Ukraine in February–March 2022.¹¹⁰
 - Data on the share of the population using VPN by year for Ukraine are absent in the provided materials. Global reports (e.g., from GWI, Surfshark¹⁰⁸) often do not highlight Ukraine separately or provide generalized data by regions.

Graph 10: Dynamics of search queries for VPN in Ukraine (2020–2025)



Source: trends.google.com

Interest in VPN in Ukraine has a pronounced event-driven character and directly correlates with threats to digital freedom and stability of access to information. Before the beginning of 2022, demand for VPN was stably low, indicating its use mainly by technically savvy audiences. However, after February 2022, the situation changed radically, and the level of interest in VPN permanently increased, indicating that it has become a tool for the broad masses.

Analysis of key peaks

1. Main peak (end of February — March 2022): The maximum surge in interest (100 points) exactly coincides with the beginning of Russia's full-scale invasion. This was caused by a complex of reasons:
 - Fear of censorship: Citizens in occupied and frontline territories began massively installing VPN, fearing disconnection from Ukrainian internet and introduction of Russian military censorship.
 - Access to blocked resources: In the first days of the war, there were disruptions in access to state sites and banking apps due to DDoS attacks. VPN could be used as a means to bypass these problems.

- Cybersecurity: Under war conditions, awareness of the need to protect personal data and encrypt traffic sharply increased.
- 2. Secondary peaks (May–June 2024, September–October 2024): Smaller but distinct surges in interest in 2024 are most likely related to internal events. In particular, during this period, initiatives to block the Telegram messenger and other online platforms perceived as a threat to national security were actively discussed in Ukrainian society and parliament. These public discussions and bills traditionally cause a preventive reaction among citizens — searching for tools to bypass possible future blocks.

Overall, the graph shows that VPN has transformed from a niche product into a mass tool for ensuring information security and freedom of access to information for Ukrainians. The baseline level of interest after February 24, 2022, has settled at twice the level before the invasion, indicating irreversible changes in the population's digital habits.

In territories temporarily occupied by Russia in Ukraine, the situation is different. Russian authorities and providers controlled by them try to block VPN services using the same methods as in the Russian Federation:

- Blocking IP addresses of known VPN servers: This is the most common method.¹⁰⁷
- Blocking ports used by VPN protocols (e.g., PPTP, L2TP).¹⁰⁷
- Blocking sites of VPN providers where apps can be downloaded or information obtained.
- Deep traffic inspection (DPI) to detect and block VPN traffic, even if masked (obfuscated).
- Roskomnadzor from November 30, 2024, introduced restrictions on disseminating information about the operation of VPN services and ways to bypass blocks, which also extends to occupied territories.¹⁰⁶

To bypass VPN blocks, users in occupied territories can use¹⁰⁴:

- Less known or new VPN services.
- Setting up own VPN servers.
- Using VPN protocols with obfuscation (e.g., WireGuard, OpenVPN with additional setup, special "masking" protocols of some VPN services).¹⁰⁷
- VPN browser extensions.

5.2.3. Cases of Persecution for Using VPN

In Ukrainian territory controlled by the government, as of available information, cases of criminal or administrative persecution of citizens or organizations solely for the fact of using

VPN services have not been recorded. Using VPN to access blocked resources or to protect one's privacy is not an offense.

However, if VPN is used to commit illegal actions (e.g., cybercrimes, dissemination of prohibited information such as child pornography, fraud, terrorist activity), the person may be held liable for these main offenses, and using VPN may be considered as a tool for committing the crime or as an aggravating circumstance aimed at concealing traces.

In territories temporarily occupied by the Russian Federation in Ukraine, the situation is fundamentally different. Russian legislation, which occupation authorities try to impose, provides for fighting VPN services and means of bypassing blocks. Although there are no direct data on mass persecutions specifically for using VPN by civilians in the provided materials, it is known that Russian security forces in occupied territories conduct checks of citizens' mobile phones for the presence of "prohibited" content, subscriptions to Ukrainian resources, or using VPN.³⁶ In such a situation, detecting a VPN app can become a reason for closer attention, interrogation, or other forms of pressure. In addition, organizers or providers of VPN services, if they operated openly in these territories and violated Russian prohibitions, would certainly be persecuted.

Thus, risks associated with using VPN radically differ depending on whether the person is in territory controlled by the Ukrainian government or in territory occupied by Russia.

5.2.4. Monitoring of Blocks

Monitoring of Internet resource blocks in Ukraine is carried out by several types of organizations and projects:

- International organizations and projects:
 - **Open Observatory of Network Interference (OONI):** A global project that collects data on internet censorship, blocks of sites and apps, as well as the presence of traffic filtering systems worldwide, including Ukraine. Data is collected with the help of volunteers running special software (OONI Probe). Results are available through OONI Explorer and API.⁸⁰ OONI recorded blocks in Ukraine and Russia, including those related to the war.³⁵
 - Digest of OONI messages (and related studies) over the last 5 years (regarding Ukraine and regional context):
 - Before 2022: OONI periodically recorded blocks of individual sites in Ukraine, often related to court decisions or sanctions against Russian resources.

- February–March 2022 (start of full-scale invasion): OONI and other researchers (e.g., Censored Planet, IODA, Route Views) recorded a sharp increase in internet censorship in Russia, including blocking Twitter, Facebook, Instagram, numerous news sites (BBC, Deutsche Welle, Meduza, etc.).⁸⁰ These blocks directly affected occupied territories of Ukraine where traffic was rerouted through the RF.³⁵ Attempts at geoblocking from Russian state sites and reciprocal geoblocking of Russian users by some foreign resources were also recorded.⁸²
- 2022–2024 (continuation of the war): OONI continued to collect data. In territory controlled by Ukraine, the main objects of blocks remained Russian and pro-Russian resources, as well as sites related to cybercrime or copyright infringement. In occupied territories, the imposition of the Russian censorship system continued.³⁶ Reports indicated attempts by Russian authorities to block VPN services.
- General OONI methodology: Uses Web Connectivity tests (to check site availability), tests for blocking apps (WhatsApp, Telegram, Facebook Messenger), tests for middlebox presence (filtering systems).⁸⁰
- Ukrainian public organizations and initiatives:
 - **UABlacklist.net**: Unofficial open registry of sites blocked in Ukraine. Collects information from court decisions, decrees of the President (NSDC), NCEC orders.⁷⁷ Allows tracking which resources and on what basis were blocked.
 - **Digital Security Lab Ukraine (Лабораторія цифрової безпеки)**: Conducts monitoring of digital rights, including freedom of access to information and cases of blocks. Publishes reports and analytics.⁶¹
 - **Інститут масової інформації (IMI)**: Tracks violations of freedom of speech, including blocks of media resources, especially in the context of war.⁹⁰
 - **Інтерньюз-Україна**: Also deals with issues of media freedom and access to information.¹⁰⁰
- State bodies (indirect monitoring or publication of decisions):
 - **NCEC** (previously NCCIR): Publishes orders on blocks on its website, but this is not systematic monitoring in public access.⁷⁵
 - **National Council on Television and Radio Broadcasting**: With the adoption of the Law "On Media", received powers to monitor online media and initiate blocks through court.⁵⁹

Monitoring of blocks in Ukraine shows that the main mass of restrictions is related to countering Russian aggression and propaganda, as well as combating illegal content (piracy, fraud, gambling). However, the opacity of some procedures and the absence of a single official registry create difficulties for public control. In occupied territories, the situation is characterized by total censorship from the RF.

6. Conclusion

The analysis of the state of the internet and digital rights in Ukraine for the period from 2019 to 2025 reveals a complex and dynamic picture, deeply affected by the full-scale Russian invasion in February 2022. Despite unprecedented challenges related to the war, destruction of infrastructure, economic downturn, and mass population migration, the Ukrainian internet sector has demonstrated significant resilience and adaptability.

Observance of human rights in the field of access to information:

In territory controlled by the Ukrainian government, the right to access information is generally preserved but is influenced by martial law and the need to ensure national security.

- Positive aspects:
 - High level of internet penetration and its further growth even under war conditions.²⁹
 - Resilience of backbone internet infrastructure and providers' efforts to restore networks.³⁶
 - Active development of digital state services (Diia portal).
 - Absence of nationwide shutdown practices by order of Ukrainian authorities.³⁶
 - Legality of using VPN and other means of bypassing blocks.¹⁰⁵
 - Active role of civil society in protecting digital rights.⁶¹
- Negative aspects and risks:
 - Blocking of internet resources (mainly Russian and pro-Russian) based on NSDC decisions and courts, sometimes with opaque procedures and absence of a single public registry.³⁶
 - Tightening of legislation on liability for statements on the internet, especially concerning justification of aggression, which with broad interpretation may lead to restriction of freedom of speech.³⁶
 - Increase in the number of criminal cases for online activity related to support for the aggressor or dissemination of disinformation.³⁶
 - Pressure on media and restrictions on information dissemination under martial law, including the format of "single telethon".¹⁹

- Expansion of powers of state regulators

Sources

1. Geography of Ukraine - Wikipedia, last accessed: June 13, 2025, https://ru.wikipedia.org/wiki/%D0%93%D0%B5%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F_%D0%A3%D0%BA%D1%80%D0%B0%D0%B8%D0%BD%D1%8B
2. Geography of Ukraine — Ruwiki: Internet Encyclopedia, last accessed: June 13, 2025, https://ru.ruwiki.ru/wiki/%D0%93%D0%B5%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F_%D0%A3%D0%BA%D1%80%D0%B0%D0%B8%D0%BD%D1%8B
3. Population of Ukraine - Wikipedia, last accessed: June 13, 2025, https://ru.wikipedia.org/wiki/%D0%9D%D0%B0%D1%81%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5_%D0%A3%D0%BA%D1%80%D0%B0%D0%B8%D0%BD%D1%8B
4. Ukraine Population (2025) - Worldometer, last accessed: June 13, 2025, <https://www.worldometers.info/world-population/ukraine-population/>
5. World Development Indicators | DataBank, last accessed: June 13, 2025, <https://databank.worldbank.org/reports.aspx?source=2&country=UKR>
6. IMF worsened the forecast of population decline in Ukraine, last accessed: June 13, 2025, <https://www.rbc.ua/ukr/news/mvf-uhudshil-prognoz-sokrashcheniya-naseleniya-1602764758.html>
7. Economy of Ukraine - Wikipedia, last accessed: June 13, 2025, https://ru.wikipedia.org/wiki/%D0%AD%D0%BA%D0%BE%D0%BD%D0%BE%D0%BC%D0%B8%D0%BA%D0%B0_%D0%A3%D0%BA%D1%80%D0%B0%D0%B8%D0%BD%D1%8B
8. Economy of Ukraine - Wikipedia, last accessed: June 13, 2025, https://en.wikipedia.org/wiki/Economy_of_Ukraine
9. Ukraine ranked 58th in the global economic ranking CEBR - Forbes.ua, last accessed: June 13, 2025,

- <https://forbes.ua/ru/news/ukraina-zaynyala-58-me-mistse-u-svitovomu-ekonomichno-mu-reytingu-cebr-26122024-25896>
10. Real GDP increased by 2.9% in 2024 – State Statistics – Forbes.ua, last accessed: June 13, 2025,
<https://forbes.ua/ru/news/zrostannya-ekonomiki-u-2024-mu-spovilnilos-do-29-derzhstat-31032025-28451>
 11. Ukraine's GDP growth seen slowing slightly to 3.3 per cent in 2025 – EBRD, last accessed: June 13, 2025,
<https://www.ebrd.com/home/news-and-events/news/2025/rep-may-25-ukraine.html>
 12. Inflation to Slow into Single Digits by End-2025, Economic Growth to Continue, last accessed: June 13, 2025,
<https://bank.gov.ua/en/news/all/inflyatsiya-za-pidsumkami-2025-roku-znizitsya-do-od-noznakovogo-rivnya-a-zrostannya-ekonomiki-trivatime--inflyatsiyniy-zvit>
 13. Ukraine GDP 1987–2025 – Macrotrends, last accessed: June 13, 2025,
<https://www.macrotrends.net/global-metrics/countries/ukr/russia/gdp-gross-domestic-product>
 14. Gross domestic product (GDP) in Ukraine 2025 – Rates, indices, tariffs, last accessed: June 13, 2025, <https://index.minfin.com.ua/economy/gdp/>
 15. Ukraine's economy survives (and even grows!) in the fourth year of war. But what should the country do if the West reduces aid after 2025? Analytical project Re: Russia — on plan B for Kyiv – Meduza, last accessed: June 13, 2025,
<https://meduza.io/feature/2025/06/13/ekonomika-ukrainy-vyzhivaet-i-dazhe-rastet-na-chetvertyy-god-voiny-no-cho-delat-strane-esli-zapad-sokratit-pomosch-posle-2025-go>
 16. What industries are developed in Ukraine? – Neuro Library – Yandex, last accessed: June 13, 2025,
https://ya.ru/neurum/c/ekonomika-i-finansi/q/kakie_otrasli_promyshlennosti_razvity_v_ukraine_4106022a
 17. Current economic problems, last accessed: June 13, 2025,
https://nam.kyiv.ua/apen_01_5-6/Minin.htm
 18. www.google.com, last accessed: June 13, 2025,
<https://www.google.com/search?q=%D0%BF%D0%BE%D0%BB%D0%B8%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%BE%D0%B5+%D1%83%D1%81%D1%82%D1%80%D0%BE%D0%B9%D1%81%D1%82%D0%B2%D0%BE+%D0%A3%D0%BA%D1%80%D0%B0%D0%B8%D0%BD%D1%8B>
 19. Ukraine: Freedom in the World 2024 Country Report, last accessed: June 13, 2025,
<https://freedomhouse.org/country/ukraine/freedom-world/2024>
 20. Ukraine: Freedom in the World 2023 Country Report, last accessed: June 13, 2025,
<https://freedomhouse.org/country/ukraine/freedom-world/2023>

21. Administrative division of Ukraine - Wikipedia, last accessed: June 13, 2025, https://ru.wikipedia.org/wiki/%D0%90%D0%B4%D0%BC%D0%B8%D0%BD%D0%B8%D1%81%D1%82%D1%80%D0%B0%D1%82%D0%B8%D0%B2%D0%BD%D0%BE%D0%B5_%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5_%D0%A3%D0%BA%D1%80%D0%B0%D0%B8%D0%BD%D1%8B
22. New districts of Ukraine as a result of administrative-territorial enlargement, last accessed: June 13, 2025, https://kartmag.com.ua/ru/index.php?route=octemplates/blog/oct_blogarticle&blogarticle_id=42
23. .ua — Wikipedia, last accessed: June 13, 2025, <https://ru.wikipedia.org/wiki/.ua>
24. Top-level domain UA: history and characteristics - RX-NAME, last accessed: June 13, 2025, <https://rx-name.net/blog/domen-verhnego-urovnya-ua-istoriya-i-harakteristiki>
25. HostMaster.UA, last accessed: June 13, 2025, <https://www.hostmaster.ua/>
26. LLC Hostmaster - DOU, last accessed: June 13, 2025, <https://jobs.dou.ua/companies/hostmaster/>
27. Is registration of the “UA” domain possible without trademarks?, last accessed: June 13, 2025, <https://deltahost.ua/vozmozhna-li-registraciya-domena-ua-bez-torgovyx-marok.html>
28. UA domain: how to register, registration rules, trademark and price, last accessed: June 13, 2025, <https://profitmark.ua/blog/domen-ua-kak-zaregistrirovat-pravila-registracii-tm-drugie-osobennosti>
29. Digital 2025: Ukraine — DataReportal – Global Digital Insights, last accessed: June 13, 2025, <https://datareportal.com/reports/digital-2025-ukraine>
30. In Ukraine, the number of people increased, and 31.5 million people use the internet — Digital 2025 report on the internet audience - Mezha.Media, last accessed: June 13, 2025, <https://mezha.media/news/v-ukrajini-pobilshalo-lyudey-internetom-koristuyutsya-bilsh-e-30-mln-ukrajinciv-300438/>
31. Internet audience in Ukraine 2025: population grew, but Yandex is still in 2nd place among search engines | Scroll Media, last accessed: June 13, 2025, <https://scroll.media/2025/03/13/internet-audytoriya-v-ukrayini-2025/>
32. Ukraine data - ITU DataHub, last accessed: June 13, 2025, <https://datahub.itu.int/data/?e=UKR&Markets=Taxation&Connectivity=Use&Sustainability=e-Applications&Trust=Digital+identity>
33. List of countries by number of Internet users - Wikipedia, last accessed: June 13, 2025, https://ru.wikipedia.org/wiki/%D0%A1%D0%BF%D0%B8%D1%81%D0%BE%D0%BA_%D1%81%D1%82%D1%80%D0%B0%D0%BD_%D0%BF%D0%BE_%D1%87%D0%B8%D1%81%D0%BB%D1%83_%D0%BF%D0%BE%D0%BB%D1%8C%D0%B7%D0%BE%D0

- [%B2%D0%B0%D1%82%D0%B5%D0%BB%D0%B5%D0%B9_%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0](#)
34. Ukraine Internet users - data, chart - TheGlobalEconomy.com, last accessed: June 13, 2025, https://www.theglobaleconomy.com/Ukraine/Internet_users/
 35. Ukraine: Freedom on the Net 2022 Country Report, last accessed: June 13, 2025, <https://freedomhouse.org/country/ukraine/freedom-net/2022>
 36. Ukraine: Freedom on the Net 2023 Country Report | Freedom House, last accessed: June 13, 2025, <https://freedomhouse.org/country/ukraine/freedom-net/2023>
 37. How the Ukrainian fixed-line internet services market changed (infographic) - Finance.ua, last accessed: June 13, 2025, <https://news.finance.ua/ua/yak-zminyvsya-ukrains-kyy-rynok-posluh-fiksovanoho-internetu-infohrafika>
 38. 25 billion UAH investments, 7.1 million lost subscribers and another 16 facts about ups and downs of the telecom industry in 2024 | Mind.ua, last accessed: June 13, 2025, <https://mind.ua/publications/20287282-25-mlrd-grn-investicij-71-mln-vtrachenih-abonentiv-ta-shche-16-faktiv-pro-zloti-j-padinnya-telekom-ind>
 39. Internet (Ukrainian market) - TAdviser, last accessed: June 13, 2025, [https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_\(%D1%80%D1%8B%D0%BD%D0%BE%D0%BA_%D0%A3%D0%BA%D1%80%D0%B0%D0%B8%D0%BD%D1%8B\)](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_(%D1%80%D1%8B%D0%BD%D0%BE%D0%BA_%D0%A3%D0%BA%D1%80%D0%B0%D0%B8%D0%BD%D1%8B))
 40. Internet providers' revenues in 2024 amounted to 258 billion UAH, last accessed: June 13, 2025, <https://minfin.com.ua/2025/05/21/151301142/>
 41. Revenues of internet providers in 2024 amounted to 258 billion UAH - reNews, last accessed: June 13, 2025, <https://renews.com.ua/ekonomika/biznes/dohodi-internet-provaiderv-y-2024-roci-skla-li-258-mlrd-grn/>
 42. How Datagroup is moving towards market monopolization - NASHI GROSHI, last accessed: June 13, 2025, <https://nashigroshi.org/2022/01/15/yak-datahrup-rukhaiet-sia-do-monopolizatsii-rynku/>
 43. Speed leaders: how Ukrainian internet providers serve Steam gamers in 2024 - Telecomsvit, last accessed: June 13, 2025, <https://www.telecomsvit.com/news/lidery-shvydkosti-yak-ukrainski-internet-provaidery-obsluhovuiut-heimeriv-steam-u-2024-rotsi>
 44. InAU calls not to displace classical technology internet providers from the market, last accessed: June 13, 2025, <https://detector.media/rinok/article/218336/2023-10-20-inau-zaklykaie-ne-vytisnyaty-z-rynku-internet-provayderiv-klasychnoi-tekhnologii/>

45. Over 83 billion UAH revenue, almost 27 million 4G subscribers, 5,544 complaints. And another 15 most interesting facts from the telecom regulator's report | Mind.ua, last accessed: June 13, 2025,
<https://mind.ua/publications/20255539-ponad-83-mlrd-grn-dohodu-majzhe-27-mln-4-g-abonentiv-5544-skarg-ta-shche-15-najcikavishih-faktiv-iz-zvi>
46. Number of mobile operators' subscribers in 2022 and 2023, last accessed: June 13, 2025,
<https://skilky-skilky.info/kilkist-abonentiv-mobilnoho-zv-iazku-zrosla-na-1-milyon-u-2023-rotsi/>
47. The country's largest mobile operator increased revenue but reduced the number of subscribers - NV Business, last accessed: June 13, 2025,
<https://biz.nv.ua/markets/krupneyshiy-mobilnyy-operator-strany-uvelichil-dohod-no-s-okratil-kolichestvo-abonentov-50466496.html>
48. Internet in Ukraine “accelerated” to 83.81 Mbit/s, and the number of users grew to 31.5 million people — DataReportal report - ITC, last accessed: June 13, 2025,
<https://itc.ua/news/ynternet-v-ukrayne-razognalsya-do-83-81-mbyt-s-a-kolychestvo-polzovatelej-vyroslo-do-31-5-mln-chelovek-otchet-datareportal/>
49. Speedtest published internet speed ranking — Ukraine in 71st place - ITC, last accessed: June 13, 2025,
<https://itc.ua/news/speedtest-opublykoval-rejtyng-skorosty-ynterneta-ukrayna-na-71-m-meste/>
50. Case Study: Ukraine – A Role Model for Internet Resilience, last accessed: June 13, 2025,
<https://pulse.internetsociety.org/blog/case-study-ukraine-a-role-model-for-internet-resilience>
51. The Resilience of the Internet in Ukraine - One Year On - RIPE Labs, last accessed: June 13, 2025,
<https://labs.ripe.net/author/emileaben/the-resilience-of-the-internet-in-ukraine-one-year-on/>
52. Statistics per country - 6lab IPv6 website, last accessed: June 13, 2025,
<https://6lab.cisco.com/stats/search.php>
53. IPv6 Measurement Maps - APNIC Labs, last accessed: June 13, 2025,
<https://labs.apnic.net/ipv6-measurement/>
54. The IPv6 Paradox: Why the Internet's Future Protocol Remains in Transition - SOUTHEAST - NEWS CHANNEL NEBRASKA, last accessed: June 13, 2025,
<https://southeast.newschannelnebraska.com/story/52777023/the-ipv6-paradox-why-the-internets-future-protocol-remains-in-transition>
55. Law on electronic communications: universal access, Internet subsidies, personal data protection, and risk of shutdowns in the ATO zone - Digital Security Laboratory, last

- accessed: June 13, 2025,
<https://dslua.org/publications/zakon-pro-elektronni-komunikatsii-universalnyy-dostup-subsydii-na-internet-zakhyst-personalnykh-danykh-ta-ryzyk-shatdauniv-v-zoni-ato/>
56. On electronic communications of 16.12.2020 | LIGA:ZAKON, last accessed: June 13, 2025, <https://ips.ligazakon.net/document/t201089>
 57. The law on media came into force today - Institute of Mass Information, last accessed: June 13, 2025,
<https://imi.org.ua/news/sogodni-nabuv-chynnosti-zakon-pro-media-i51823>
 58. On media of 13.12.2022 | LIGA:ZAKON - IPS LIGA:ZAKON, last accessed: June 13, 2025,
<https://ips.ligazakon.net/document/T222849>
 59. National Council registered the most print media in a year of the Law "On Media", last accessed: June 13, 2025,
<https://imi.org.ua/news/natsrada-za-rik-diyi-zakonu-pro-media-najbilshe-zareyestruva-la-drukovanyh-media-i60322>
 60. The Law “On Media” is already in effect. Here are the main explanations from the National Council on television and radio broadcasting - Mediamaker, last accessed: June 13, 2025,
<https://mediamaker.me/zakon-pro-media-vzhe-diye-os-osnovni-rozysnennya-vid-na-czrady-z-pytan-telebachennya-i-radiomovlennya-1895/>
 61. Annual Report 2024 - Digital Security Laboratory, last accessed: June 13, 2025,
<https://dslua.org/publications/annual-report-2024/>
 62. Contact information of the National Commission for the State Regulation of Electronic Communications, Radio Frequency Spectrum and Postal Services (NCEC), last accessed: June 13, 2025,
<https://me.gov.ua/Documents/Detail?lang=uk-UA&id=8ddf2c38-4091-404c-a39e-3fbb6f9afd5b&title=NatsionalnoiKomisii-SchoZdiisniuDerzhavneRegulivanniaUSferakhElektronnikhKomunikatsii-RadiochastotnogoSpektraTaNadanniaPoslugPoshtovogoZv'язku-nkek->
 63. National Commission for the State Regulation of Electronic Communications, Radio Frequency Spectrum and Postal Services - Main, last accessed: June 13, 2025,
<https://uvaga.gov.ua/uk/Main/Agency/Agency/141>
 64. Leadership | National Commission for the State Regulation of Electronic Communications, Radio Frequency Spectrum and Postal Services, last accessed: June 13, 2025, <https://nkek.gov.ua/pro-nkek/kerivnytstvo-nkek/persons>
 65. MINISTRY OF DIGITAL TRANSFORMATION OF UKRAINE | EDRPOU 43220851 — contacts, address, phone, director, services | Kyiv - UA-Region, last accessed: June 13, 2025, <https://www.ua-region.com.ua/43220851>
 66. 43220851 — MINCYFRY - Opendatabot, last accessed: June 13, 2025,
<https://opendatabot.ua/c/43220851>

67. Article 115-2. Procedure for restricting access to websites used for providing on-demand media services and audiovisual services of the aggressor state – On Electronic Communications, accessed June 13, 2025, https://protocol.ua/ua/pro_elektronni_komunikatsii_statnya_115_2/
68. Article 115. Provision of electronic communication services under emergency situations, martial law, and state of war – On Electronic Communications – Laws of Ukraine | Protocol, accessed June 13, 2025, https://protocol.ua/ua/pro_elektronni_komunikatsii_statnya_115/
69. zakon.rada.gov.ua, accessed June 13, 2025, <https://zakon.rada.gov.ua/laws/show/1089-20#Text>
70. Countering disinformation in Ukraine. Draft Law of Ukraine “On Amendments to Certain Legislative Acts of Ukraine on Countering Disinformation.” Today, the creation and dissemination of disinformation poses a threat to Ukraine’s national security, the interests of individuals and legal entities, and their right to reliable and objective information. Therefore, having developed the relevant draft law, we propose to consider improving Ukrainian legislation to establish real liability for persons who harm public interests by misleading the population. – Electronic Petitions, accessed June 13, 2025, <https://petition.president.gov.ua/petition/130114>
71. From fines to imprisonment: how fake news about the war is punished in Ukraine, accessed June 13, 2025, <https://www.rbc.ua/rus/news/vid-shtrafiv-tyuremnogo-uv-yaznennya-k-karayut-1737468356.html>
72. Information warfare and criminal justice. Legal consequences of spreading fake news and manipulative information | Law Firm “Donets and Partners”, accessed June 13, 2025, <https://donets.partners/%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0-%D0%B2%D1%96%D0%B9%D0%BD%D0%B0-%D1%82%D0%B0-%D0%BA%D1%80%D0%B8%D0%BC%D1%96%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%B5-%D0%BF%D1%80/>
73. Sanctions and website blocking in Ukraine: how to bypass it unnoticed – Digital Security Lab Ukraine, accessed June 13, 2025, https://dslua.org/wp-content/uploads/2021/06/Sanctions_and_Internet_UPD_2.pdf
74. Decree of the President of Ukraine No. 81/2025 – Official website of the President of Ukraine, accessed June 13, 2025, <https://www.president.gov.ua/documents/812025-53777>
75. Website blocking: illegal but works – Vasyl Kisil & Partners, accessed June 13, 2025, <https://vkp.ua/publication/blokuвання-saytiv-nezakonno-ale-pratsyuie>
76. Wartime blocking: providers must restrict access to 191 websites – Digital Security Lab Ukraine, accessed June 13, 2025,

- <https://dslua.org/publications/blokuвання-voiennoho-chasu-provaydery-maiut-obmezhyty-dostup-do-191-saytu/>
77. List of websites banned in Ukraine – Ukrainian Blacklist, accessed June 13, 2025, <https://uablacklist.net/uk/>
78. Banned internet resources in Ukraine – full list now available on Uablocklist – Zlatopil, accessed June 13, 2025, <https://zlatopil.com.ua/zaboroneni-internet-resursi-v-ukrayini-perelik-vsih-sajtiv-teper-dostupnij-na-uablocklist>
79. Ukraine expands list of banned websites hosting pirated movies – Ukrinform, accessed June 13, 2025, <https://www.ukrinform.ua/rubric-society/3952249-v-ukraini-zbilsili-spisok-zaboronenihsajtiv-z-piratskimi-filmami.html>
80. OONI – Wikipedia, accessed June 13, 2025, <https://en.wikipedia.org/wiki/OONI>
81. How Internet censorship changed in Russia during the 1st year of military conflict in Ukraine – Open Observatory of Network Interference (OONI), accessed June 13, 2025, <https://msg.ooni.io/documents/russia-military-conflict-en.pdf>
82. Network Responses to Russia’s Invasion of Ukraine in 2022: A Cautionary Tale for Internet Freedom – USENIX, accessed June 13, 2025, <https://www.usenix.org/system/files/sec23fall-prepub-380-ramesh.pdf>
83. OONI Explorer, accessed June 13, 2025, <https://explorer.ooni.org/>
84. 2023 Country Reports on Human Rights Practices: Ukraine – U.S. Department of State, accessed June 13, 2025, <https://www.state.gov/reports/2023-country-reports-on-human-rights-practices/ukraine/>
85. Internet shutdowns and atrocities in Ukraine – Access Now, accessed June 13, 2025, <https://www.accessnow.org/internet-shutdowns-and-atrocities-in-ukraine/>
86. Advice for Ukrainians in occupied territories where access to Ukrainian internet and mobile communication is cut off – State Service of Special Communications and Information Protection of Ukraine, accessed June 13, 2025, <https://cip.gov.ua/ua/faqs/poradi-dlya-ukrayinciv-na-okupovanikh-teritoriyakh-de-vidrizanii-dostup-do-ukrayinskogo-internetu-ta-mobilnogo-zv-yazku>
87. “Powerful strike on substations”: Did the Armed Forces of Ukraine cause a blackout in occupied territories? – Radio Svoboda, accessed June 13, 2025, <https://www.radiosvoboda.org/a/novyny-pryazovya-blyakayut-v-okupatsiyi/33439047.html>
88. Why 2024 Was The Worst Year for Internet Shutdowns – TechPolicy.Press, accessed June 13, 2025, <https://www.techpolicy.press/why-2024-was-the-worst-year-for-internet-shutdowns/>

89. In 2023, scammers in Ukraine earned over UAH 3 billion. Top 5 fraud schemes – Ukr.net, accessed June 13, 2025, <https://www.ukr.net/news/details/criminal/104006838.html>
90. 836 crimes committed by Russia against journalists and media in Ukraine in three years and three months of full-scale war – Institute of Mass Information, accessed June 13, 2025, <https://imi.org.ua/monitorings/836-zlochyniv-vchynyla-rf-proty-zhurnalistiv-ta-media-v-ukrayini-try-roky-i-try-misyatsi-i68403>
91. NSJU concerned about statements regarding pressure on Ukrainska Pravda – National Union of Journalists of Ukraine, accessed June 13, 2025, <https://nsju.org/novini/nszhu-sturbovana-zayavamy-pro-tysk-na-ukrayinsku-pravdu/>
92. Threats on social media, DDoS attacks, and obstruction: which journalist cases are being investigated in Rivne region – Institute of Mass Information, accessed June 13, 2025, <https://imi.org.ua/blogs/pogrozy-v-sotsmerezah-ddos-ataky-i-pereshkodzhannya-ya-ki-zhurnalisty-spravy-rozsliduyut-na-i67592>
93. Hello O-Days, My Old Friend: A 2024 Zero-Day Exploitation Analysis – Google Cloud Blog, accessed June 13, 2025, <https://cloud.google.com/blog/topics/threat-intelligence/2024-zero-day-trends>
94. IMI study: Transparency of Ukrainian online media increased to 80% in 2024 (updated) – Institute of Mass Information, accessed June 13, 2025, <https://imi.org.ua/monitorings/doslidzhennya-imi-prozorist-onlajn-media-ukrayiny-zros-la-do-78-u-2024-rotsi-i64056>
95. Digital Security Lab Ukraine (DSLUI) – Front Line Defenders, accessed June 13, 2025, <https://www.frontlinedefenders.org/en/organization/digital-security-lab-ukraine-dslu>
96. Report: Human Rights in the Digital Dimension 2024 – Digital Security Lab Ukraine, accessed June 13, 2025, <https://dslua.org/publications/zvit-prava-liudyny-u-tsyfrovomu-vymiri-2024/>
97. Annual Report 2023 – Digital Security Lab Ukraine, accessed June 13, 2025, https://dslua.org/wp-content/uploads/2024/04/Richnyy-zvit_upd.pdf
98. Research – Institute of Mass Information, accessed June 13, 2025, <https://imi.org.ua/monitorings>
99. USAID-Internews 2024 Study on Media Consumption of Ukrainians – Mediamaker, accessed June 13, 2025, <https://mediamaker.me/usaaid-internews-2024-mediaspozhyvannya-ukraincziv-12518/>
100. Annual Report 2023 – Internews Ukraine, accessed June 13, 2025, <https://internews.ua/report/2023-year>
101. Digital rights or public health – Institute of Innovative Governance, accessed June 13, 2025, https://instingov.org/wp-content/uploads/2021/10/Report_ukarine-ukr-.pdf

102. June 30 – presentation of the analytical report “War in the Digital Dimension and Human Rights”, accessed June 13, 2025, <https://cs.detector.media/ability/texts/184856/2022-06-24-30-cherwnya-prezentatsiya-analitychnogo-zvitu-viyna-u-tsyfrovomu-vymiri-i-prava-lyudyny/>
103. State Special Communications Service: What is VPN and how to use it safely – Mankivska community, accessed June 13, 2025, <https://mankivska-gromada.gov.ua/news/1653892813/>
104. How to bypass VPN blocking in occupied territories and protect messages in messengers – Forbes.ua, accessed June 13, 2025, <https://forbes.ua/innovations/vpn-tor-ta-spilkuvannya-u-messendzherakh-yak-pidtrimuvati-zvyazok-na-okupovanikh-teritoriyakh-detalna-instruktsiya-10082022-7616>
105. Is VPN allowed in your country? – HideMyAss Blog, accessed June 13, 2025, <https://blog.hidemypass.com/uk/vpn-country-guide>
106. Russia tightens internet control in temporarily occupied territories: VPN services banned until 2029, accessed June 13, 2025, <https://farwatermedia.com/news/rf-posyliuie-kontrol-nad-internetom-na-tot-vpn-servisy-pid-zaboronoiu-do-2029-roku/>
107. Obfuscated VPN servers: what they are and why you need them – Surfshark, accessed June 13, 2025, <https://surfshark.com/uk/features/obfuscated-servers>
108. 25 VPN Statistics 2025: Usage, Market & Trends – Demand Sage, accessed June 13, 2025, <https://www.demandsage.com/vpn-statistics/>
109. VPN statistics: VPN usage by country & more – Comparitech, accessed June 13, 2025, <https://www.comparitech.com/vpn/vpn-statistics/>
110. Chart: VPN Use Surges in Ukraine and Russia – Statista, accessed June 13, 2025, <https://www.statista.com/chart/27002/vpn-search-surges-2022/>
111. Atlas VPN blog, accessed June 13, 2025, <https://atlasvpn.com/blog/reports/16>
112. IPv6 Capability Metrics – APNIC Labs Measurements (Ukraine), accessed June 13, 2025, <https://stats.labs.apnic.net/ipv6/UA>