Flygtningenævnets baggrundsmateriale

Bilagsnr.:	**521**
Land:	Ukraine
Kilde:	Freedom House
Titel:	Freedom on the Net 2024 – Ukraine
Udgivet:	16. oktober 2024
Optaget på baggrundsmaterialet:	7. november 2024

Freedom House

FREEDOM ON THE NET 2024

Ukraine

PARTLY FREE

59 /100

A. Obstacles to Access	18 /25
B. Limits on Content	22 /35
C. Violations of User Rights	19 /40

LAST YEAR'S SCORE & STATUS

59 /100 **Partly Free**

Scores are based on a scale of 0 (least free) to 100 (most free). See the research methodology and report acknowledgements.

Key Developments, June 1, 2023 – May 31, 2024

The February 2022 full-scale invasion of Ukraine by the Russian military continues to undermine internet freedom in the country. The Russian military's attacks have caused severe damage to Ukraine's internet infrastructure, resulting in network disruptions. The Ukrainian government blocks a wide variety of Russian and Kremlin-backed websites including blogs and news outlets, social media sites, and sites that provide other services. Additionally, courts have sentenced individuals accused of producing pro-Kremlin propaganda, collaborating with the Russian government to produce online content, or posting information online about evading the draft. Cyberattacks by Russian actors against state institutions, critical infrastructure, and the media are routine.

- The Kremlin's full-scale invasion has resulted in damage to least 30,000 kilometers (18,600 miles) of fiber-optic cables, 4,300 mobile base stations, and a quarter of Ukraine's internet networks, and caused severe network disruptions throughout the coverage period (see A1 and A3).
- In December 2023, Kyivstar, a major internet service provider (ISP), suffered a severe Russian hacking attack, disrupting infrastructure and user connectivity (see A1 and C8).
- Since September 2023, the Ministry of Digital Transformation has become the leading authority in safeguarding and expanding internet infrastructure, including coordinating the restoration of internet and mobile networks in previously occupied areas (see A5).
- In November 2023, reports emerged that Oleksiy Matsuka, the director general of state news agency Ukrinform, had followed instructions from the office of the Ukrainian president about how to cover news (see B5).
- Reports emerged that employees of two leading investigative journalism agencies faced a conscription attempt and unlawful surveillance, respectively, by members of the State Security Service (SSU). Meanwhile, anticorruption activists were targeted by disinformation campaigns (see B5 and C7).

- The Russian occupying authorities in Melitopol detained several administrators of critical Telegram channels in August 2023 (see C3 and C7).

Political Overview

In the past decade, Ukraine has enacted a series of reforms to address issues like widespread corruption, a politicized judiciary, and attacks against journalists, activists, and members of ethnic and other minority groups. However, government initiatives to solve these problems sometimes suffer from a lack of political will, and have experienced setbacks. While the 2022 invasion forced the government to shift its primary focus from reform programs to more pressing wartime needs, authorities have continued work toward aligning legislation with European Union (EU) law. Since the Russian invasion of Crimea in 2014, the Ukrainian government has prosecuted individuals or groups perceived as threatening Ukrainian sovereignty.

Note: To align this survey with Freedom House's Freedom in the World *survey,* Freedom on the Net *has excluded Russian-occupied eastern Donbas, based on boundaries established prior to the Kremlin's full-scale invasion of Ukraine in February 2022, and Crimea from its analysis of Ukraine in recent years. Disputed or occupied territories are sometimes assessed separately by* Freedom in the World *if they meet certain criteria, including boundaries that are sufficiently stable to allow year-on-year comparisons. Readers can access Freedom House's criteria for evaluating territories separately* ***here***.

A. Obstacles to Access

A1 0-6 pts

Do infrastructural limitations restrict access to the internet or the speed and quality of internet connections?	**4**/6

During the reporting period, damage caused by the Russian military's full-scale invasion continued to interrupt internet access for many, though the government has taken action to restore access in liberated areas. [1]

According to the latest data from the International Telecommunication Union (ITU), as of 2021, Ukraine's internet penetration rate was 79.2 percent, with the fixed- and mobile-broadband penetration rates reaching 18.3 percent and 80.1 percent respectively. [2] As reported by Ukrainian governmental officials, by the end of February 2022, 90 percent of Ukraine was covered by fiber-optic networks and around 89 percent of citizens had access to mobile communication services from at least two operators. [3] According to the research service DataReportal, as of February 2024, some 20.8 percent of Ukrainians remained offline, while the number of internet users increased by 1.1 million (3.7 percent) between 2023 and 2024. [4] Internet availability and ease of access vary by region, and access remained significantly affected by war during the coverage period.

Mobile internet speeds remain poor. The median mobile download speed in May 2024 was 20.99 megabits per second (Mbps), compared to a global average of 52.48 Mbps, according to the network intelligence company Ookla. [5] The median fixed-broadband speed was much faster, per Ookla, at 81.18 Mbps.

Due to emergency blackouts resulting from targeted Russian military air strikes on energy and telecommunications infrastructure, Ukrainians were again periodically disconnected from broadband internet during the coverage period. Under such circumstances, resulting heavy mobile internet usage has overloaded mobile operators' networks, resulting in poor quality service or the total loss of mobile service. Ukrainian internet providers use electricity generators to keep Ukrainians connected. [6] In frontline regions, the critical and social infrastructure facilities have been equipped with compact lithium battery, to bolster power supplies during outages. [7]

Subscribers faced issues accessing the internet for several days in December 2023, when Russian hackers disabled Kyivstar, a large broadband and mobile operator (see C8). [8]

In April 2024, the Ministry of Digital Transformation reported that Russia's full-scale invasion had damaged 30,000 kilometers of fiber optic cables, 4,300 mobile base stations, and a quarter of the country's internet networks. [9] When Ukrainian forces have retaken territories, reestablishing internet connection has been one of their priorities. [10] However, restoring infrastructure has been challenging due to mines, constant shelling, and power outages. While repairs are

ongoing in liberated territories, Ukrainian providers have established makeshift Wi-Fi spots where residents sometimes must queue for hours to connect to the internet for just 15 minutes. [11] In May 2023, the Ministry of Digital Transformation and Nokia signed an agreement to launch a pilot project modernizing networks in front-line settlements and those that had previously been occupied by the Russian military. [12]

As of May 2024, the government had also equipped 730 "invincibility points," specially equipped places where Ukrainians can charge their devices, warm up, and get free internet access. [13]

In 2022, after the full-scale Russian military invasion, Ukraine became one of the countries with the highest rate of SpaceX's Starlink usage (see A4). By the end of 2023, Ukraine had at least 47,000 Starlink receivers, [14] which have been operationalized to provide internet access to individual users and critical infrastructure facilities even during the blackouts and in the areas most heavily affected by war. [15] Ukrainian soldiers have reportedly used the SpaceX-operated systems to coordinate military action and stay in touch with their families. [16] Moreover, after a successful testing, the Ministry of Digital Transformation and Ukrainian Railways announced in 2023 that they plan to equip all high-speed intercity trains with Starlink receivers. [17] The Russian military has tried to target Starlink service on battlefield, leaving Ukrainian military without the only reliable source of connection. [18] In August 2023, Elon Musk, the chief executive of SpaceX, refused to activate Starlink satellites in Russian-occupied Sevastopol, Crimea, at the request of the Ukrainian government, which wanted to use the network in an attack against a Russian fleet there. [19]

The government has also worked with mobile operators to help them launch a national roaming service allowing subscribers to switch between networks in cases where a signal is jammed. [20] In April 2022, 27 mobile operators in the European Union (EU) and Ukraine reached an agreement to provide roaming calls to Ukraine at a free or reduced price. [21] The preferential roaming regime was prolonged until July 2024. [22] By the end of the reporting period, in order to comply with the EU-Ukraine Association Agreement, the Ukrainian parliament had adopted a draft law introducing a single roaming zone in the EU. The president signed it shortly thereafter and it currently awaits follow-up approval by the EU (see A4). [23]

In 2020, three major mobile operators—Kyivstar, Vodafone, and Lifecell—began work on a nationwide program to provide fourth-generation (4G) technology for mobile networks to 90 percent of the population by 2024. [24] By the end of 2021, Kyivstar's 4G network reached 90 percent of Ukraine's population, closely followed by Vodafone Ukraine with 83 percent coverage, [25] and the two networks had covered four international highways with high-quality 4G connection. [26] However, growth of the 4G network was put on hold after the full-sale invasion, with operators' attention shifting to emergency restoration of base stations destroyed by Russian military.

In mid-February 2022, the parliament approved a bill that simplifies the procedure for deployment of 4G base stations by mobile operators, and halves the time required to obtain the necessary permit. [27] As of the end of this reporting period, the parliament was still considering a draft law that would allow mobile operators to obtain land for construction of base stations in 1 to 3 months—twice as fast as is needed currently, according to the Digital Transformation Ministry. [28]

The first government tender for a 5G implementation plan was to be announced in 2021, but it was postponed until February 2022 [29] and then put on hold following the Russian military invasion. In late 2023, the government adopted a radio frequency spectrum usage plan aiming to facilitate 5G implementation, bridge the urban-rural digital divide, and improve e-services quality. The new license terms do not establish any qualification or organizational requirements for licensees. [30] In May 2024, Vodafone and Nokia conducted the first 5G testing in Ukraine. [31]

A2 0-3 pts

Is access to the internet prohibitively expensive or beyond the reach of certain segments of the population for geographical, social, or other reasons?	**2**/3

Internet infrastructure is more developed in urban areas, though inequality along an urban-rural divide has continued to narrow. There has been limited data on disparities in internet access since the Kremlin's full-scale invasion.

With an average monthly wage of 14,308 hryvnia ($363) in 2023, [32] monthly internet subscription rates are fairly affordable for most of the population.

According to 2023 data from the ITU, the average cost of a 5 gigabyte (GB) monthly fixed-broadband subscription was 2.25 percent of gross national income (GNI) per capita, while that of a 2 GB mobile subscription was 1.36 percent of GNI per capita. [33] High competition among operators generally keeps internet subscription prices affordable. As reported by the Ministry of Digital Transformation, during 2023, 540 villages were connected to 4G network for the first time. [34]

In February 2023, Ukrtelecom launched free public Wi-Fi zones in the largest Ukrainian cities—Kyiv, Dnipro, Lviv, Odesa, and Kharkiv—that have a capacity to remain functional for two to four hours during electricity blackouts. [35] The Ministry of Digital Transformation planned to expand the number of such free public Wi-Fi zones by installing Starlink receivers, including in recaptured territories, [36] though no updates on achieved progress were available during the reporting period.

A3 0-6 pts

Does the government exercise technical or legal control over internet infrastructure for the purposes of restricting connectivity?	**4** / 6

Ukraine's diverse and open internet infrastructure poses structural obstacles for any government authority seeking to enact a large-scale connectivity blockage. The backbone connection to the global internet is not centralized, and major ISPs manage their own channels independently. [37] The country has at least 23 internet exchange points (IXPs), [38] 12 of which were operational as of May 2024. [39] Ukraine's largest IXP, UA-IX, allows Ukrainian ISPs to exchange traffic and connect to the global network. Ukraine's internet has proven resilient even during the full-scale war due to availability of numerous exit points with neighboring countries, a well-provisioned network of international connectivity providers, a strong local peering fabric, and well-secured networks to mitigate security issues. [40]

As reported by Access Now, in 2023, Russian military air strikes resulted in at least 8 network disruptions in Ukraine. [41]

Beginning in the spring of 2022, the Russian military compelled ISPs in occupied areas to reroute connections through Russian networks. [42] Individuals connected to these ISPs are unable to access websites that are blocked in Russia, including

Instagram and Facebook. Russian-backed authorities in occupied areas of Ukraine also restrict access to virtual private networks (VPNs), [43] websites, and messaging applications that are not blocked in Russia, including Google, YouTube, and the messaging application Viber (see C4). [44] After the liberation of territory in Kherson in October 2022, local ISPs in those territories stopped rerouting internet traffic through Russia.

The Russian occupying authorities took a similar approach with mobile operators. The authorities forced people to switch to SIM cards of Kremlin-run mobile operators, which block calls into Ukraine. [45] The Russian military had previously taken similar actions in Crimea, which is outside of this report's scope. [46]

Ukrainian legislation on states of emergency and martial law could be used to restrict connectivity. In December 2020, Parliament passed the Law on Electronic Communications (see C6), which amended the Law on Combatting Terrorism to enable the government to temporarily restrict access to the internet for the sake of antiterrorist operations. The law also allows the restriction of internet access during states of emergency or martial law, [47] when the government may introduce "special rules" concerning "the connection and transmission of information through computer networks." [48] Under martial law (see C1), the military is empowered to prohibit "the transmission of information through computer networks." [49] As of the end of the coverage period the government had refrained from implementing these provisions, even after martial law was declared in response to the Russian invasion. [50]

A4 0-6 pts

Are there legal, regulatory, or economic obstacles that restrict the diversity of service providers?	**5**/6

The Ukrainian information and communications technology (ICT) market is fairly liberal. According to the National Commission for State Regulation of Electronic Communications, Radio Frequency Spectrum and Provision of Postal Services (NCEC), there were 2,091 ISPs in the country at the end of the coverage period. [51] The diversity of ISPs and absence of strict state control over the networks were key factors that enabled Ukraine to avoid a nationwide internet shutdown

during massive and continuous attempts by Russia to destroy telecommunications infrastructure since the beginning of full-scale invasion (see A1).

Because Ukrtelecom, which was 93 percent state-owned prior to its privatization in 2011, owns much of the ICT infrastructure, and some providers lack the resources to build their own networks, [52] there is some dependency on leased lines. However, Ukrtelecom does not exert pressure or regulatory control over other ISPs. During the coverage period, Kyivstar maintained its leadership in the fixed-broadband market, followed by Ukrtelecom, Datagroup-Volia, and Vodafone (having acquired Vega and Freenet). Other major ISPs in Ukraine include Lanet, Triolan, Fregat, and Uarnet. [53] Following the invasion, subscribers regularly shifted between ISPs looking for stable internet connection during electricity blackouts. [54] In November 2023, the Ministry of Digital Transformation, along with the nongovernmental organization LUN Misto, launched a map of internet availability during blackouts, primarily covering ISPs in the city of Kyiv, and sporadically issuing updates on blackouts in the Kyiv, Odesa, and Lviv regions. [55]

As of November 2023, Russia's military has destroyed a quarter of all internet networks across Ukraine, leaving over 90 ISPs on the verge of bankruptcy (see A1). The German government has allocated financial support of €700,000 ($765,000) for 68 Ukrainian ISPs to restore internet connection on de-occupied territories, improve network resilience, and connect remote settlements. [56]

The mobile-broadband market is dominated by three main competitors: Kyivstar (VEON), Lifecell (owned by Turkey's Turkcell), and Vodafone Ukraine (owned by Azerbaijan's BakCell). [57]

An April 2021 decision by the Antimonopoly Committee of Ukraine concluded that there are no significant administrative barriers to entering the ICT market and financial expenses at the startup phase are relatively low. Moreover, major players often allow new providers to access existing infrastructure for nominal fees when they are establishing their operations. Easy entry to the market and the ability of users to change the provider of their choice keep the competition among ISPs high. [58]

In September 2019, the government removed a licensing requirement for telecommunications operators, introducing a simplified notification procedure in

its stead. [59] Additionally, Diia Business, a digital platform launched by the Ministry of Digital Transformation, offers guidelines for those looking to launch an ISP. [60] However, mobile operators must still license the radio frequencies they use to provide cellular services. At the same time, mobile operators received additional frequencies to enhance network capacity during wartime. [61]

A5 0-4 pts

Do national regulatory bodies that oversee service providers and digital technology fail to operate in a free, fair, and independent manner?	**3**/ 4

In February 2022, the previous ICT regulator, the National Commission for the State Regulation of Communications and Informatization (NCCIR), was transformed into the National Commission for State Regulation of Electronic Communications, Radio Frequency Spectrum, and Provision of Postal Services (NCEC). The new body features a more transparent procedure for selection of its members, involving an independent selection commission and final approval by the government. The NCEC has seven members; its chair is selected by members from among themselves for a three-year term. [62] The current members and chair, who were appointed under the NCCIR's presidential decree system, will perform their duties until the end of their terms. [63]

The Ministry of Digital Transformation is responsible for articulating and implementing state policy for online-government efforts and is in charge of efforts to build digital skills among Ukrainians. [64] Zelenskyy's administration has created digital transformation leadership positions in each ministry, regional administration, state company, and state agency. [65] When the Law on Electronic Communications entered into force in January 2022, the Ministry of Digital Transformation assumed powers from the State Service of Special Communications and Information Protection (SSSCIP) related to shaping policy in the field of electronic communications and radio frequency spectrum. [66] In September 2023, the ministry assumed primary responsibilities for restoring internet connection and mobile networks on de-occupied territories, expanding high-speed internet coverage, facilitating a single roaming area with the EU, and simplifying rules in telecom sector. As a result, the SSSCIP is now mostly focused on protection of critical infrastructure. [67]

Several civil society groups provide input on ICT and media regulation in Ukraine, including the Internet Association of Ukraine and the National Union of Journalists of Ukraine, and their recommendations are often implemented.

B. Limits on Content

B1 0-6 pts

Does the state block or filter, or compel service providers to block or filter, internet content, particularly material that is protected by international human rights standards?	**3**/6

The Ukrainian government blocks numerous Russian and pro-Russian websites. Russian-owned web platforms, including Vkontakte (VK), Odnoklassniki (OK), and Mail.ru; a wide variety of websites deemed to contain Russian propaganda; and Russia-affiliated companies like Dr. Web, Kaspersky, and Yandex have been blocked via "sanctions," which have been repeatedly renewed, since 2017. [68] In May 2021, sanctions were levelled against Russian and pro-Russian Crimean media, payment systems, and information technology companies. [69] At different periods, blocking orders also included the online resources of the self-proclaimed governance bodies of the Kremlin-controlled Luhansk People's Republic, as well as those of Rostelecom, RT, National Media Group, All-Russia State Television and Radio Broadcasting Company, Channel One, Information Agency ITAR-TASS, and others. [70] The actual implementation of website blocking has been inconsistent, [71] disputed in the court, [72] and never properly monitored. [73]

After instituting martial law (see C1) in response to the February 2022 invasion, the NCEC asked ISPs to block a massive number of Russian websites that allegedly spread disinformation [74] or facilitated cyberattacks. [75] By March 2022, the NCEC ordered the blocking of more than 48 million Russian IP addresses. The penalty for noncompliance is exclusion from the register of telecom operators and providers, and the regulator is empowered to apply more severe measures. At least one such case has been reported so far. [76]

In March 2023, the National Center for Operational and Technical Management of Telecommunications Networks began deploying a filtration system for phishing domains used for fraudulent purposes in banking and financial sector. The

decision met some resistance from the industry, including from the Ukrainian Internet Association, partially because the measure could lay the ground for future indiscriminate blocking of online resources. [77] Similar measures had previously been applied to fraudulent online casinos. [78]

In September 2023, a group of volunteers launched UABlockList, a website that aims to register online resources that are blocked in Ukraine. According to the register, 5,230 websites are blocked in total. During the reporting period, according to UABlockList, Ukrainian authorities ordered the blocking of 475 Russian websites, out of which 236 were blocked upon the National Security and Defense Council (NSDC) decision, and 238 ordered by the SSSCIP. [79]

According to an August 2023 report from the European Commission, which has also sanctioned Russian websites across the European Union, restrictions introduced by Ukraine since the full-scale invasion are "legitimately rooted in national security concerns. However, the Ukrainian government should provide a clear vision for the reestablishment of rights and freedoms after martial law ends." [80]

The NSDC has also issued sanctions against non-Russian media outlets that adopt a pro-Russian stance. For example, in August 2021, Zelenskyy banned the online news outlet Strana and sanctioned its editor in chief, Ihor Huzhva, and blogger Anatoliy Shariy, on grounds of disseminating pro-Russian propaganda (see C3). [81] Blocking also was ordered for related channels and pages on YouTube, Facebook, Twitter, and Telegram, and affiliated individuals and businesses were also affected. [82] The sanctions against online resources related to Huzhva and Shariy were extended for three and ten years respectively in February 2022 [83] and January 2023. [84] In 2024, the NSDC continued ordering blocking of YouTube channels of sanctioned Russian propagandists. [85]

In January 2024, the SSU ordered the blocking of a Viber channel that was sharing information about locations where representatives of the territorial recruitment centers were handing out draft notices in Lviv region, thus helping Ukrainian men to avoid mobilization. [86] Seven Telegram channels and Viber groups were blocked in the Cherkasy region on similar grounds (see C3). [87]

The authorities occasionally direct ISPs to block websites involved in cybercrime, fraud, illegal gambling, the drug trade, and money laundering. [88] In the past, courts have also blocked websites on grounds that hosting content allegedly violated intellectual property rights. [89]

B2 0-4 pts

Do state or nonstate actors employ legal, administrative, or other means to force publishers, content hosts, or digital platforms to delete content, particularly material that is protected by international human rights standards?	**2**/4

The government sometimes refers content to third parties, seeking its removal. During the coverage period, social media platforms and search engines also removed inauthentic content in response to the Russian military invasion of Ukraine (see B5).

In the first half of 2023, Meta restricted access to 137 items of content based on Ukrainian government requests for "alleged violation of local laws." In the last six months of 2023, Meta restricted access in Ukraine to 107 items of such content. These numbers demonstrated a sharp decrease compared to 2022. [90] In the first half of 2023, Google received 28 requests from the government covering 133 items and removed 22.5 percent of items for legal and policy reasons. In the second half of 2023, Google received 40 requests regarding 382 items, removing 5.2 percent of them on legal and policy ground. Most of the requests related to defamation and national security. [91] X did not produce a transparency report covering the reporting period.

Several Ukrainian social media pages that have shared information about the war or tried to organize support for the Ukrainian army have also had their pages removed, or otherwise limited since the start of the full-scale invasion. For example, in July 2023, a commemoration post for a Ukrainian writer killed in a Russian missile attack was marked by Facebook as hate speech. [92] Meta has also deleted and later restored the Instagram account of a memorial project commemorating people killed by the Russian military. [93] In October 2023, YouTube blocked a Ukrainian version of a documentary about environmental damage caused by the Kremlin's full-scale invasion, which was published by the Ukrainian Armed Forces Strategic Communications Department; however the

English version remains available. [94] The platform has also been deleting links to charity foundation Come Back Alive, allegedly for obscene pictures. Reportedly some content was restored after users' complaints. [95]

Since December 2023, Ukrainian media can challenge their accounts' restrictions on TikTok, Instagram, and Facebook via the Tech and Journalism Crisis and Emergency Mechanism platform, [96] which was launched by the Global Forum for Media Development.

In April 2024, without any prior notification, Telegram temporarily blocked some official chatbots, including those of the SSU, the Ministry of Digital Transformation, and Defense Intelligence. [97] Shortly before the blocking, Telegram founder Pavel Durov stated that the company allegedly received a request from Apple to block certain news and propaganda channels for iPhone users with Ukrainian SIM cards, and that Telegram would take action to comply. [98]

The same month, the NSDC Center for Countering Disinformation (CCD) announced official cooperation with TikTok to block, within Ukraine, Russian propaganda channels according to a previously submitted list of 83 such channels. [99] However, by the end of the reporting period the negotiations had not progressed significantly. [100] Similarly, the CCD and the SSU Cybersecurity Department have released a list of 66 X accounts that reportedly promulgate Russian disinformation, [101] but no action was taken against them.

In April 2024, Telegram began considering an SSU request to block 26 pro-Russian channels, [102] while the CCD has reported blocking of YouTube channels associated with sanctioned television channels NewsOne, and Nash. [103] In early March 2024, a Telegram representative confirmed that the company has received from the Ukrainian authorities a list of "problematic" channels spreading Russian propaganda and will consider undertaking actions based on the terms of service. [104]

In March 2024, the television channel Espreso reported that its representatives had been approached by an intermediary who offered a payment for removing an article alleging unethical lobbying by Olena Shuliak, the head of the Servant of the People Party, and Oledsandr Kubarov, the deputy prime minister. [105]

The Cyber Police, a law enforcement department charged with fighting cyber crime, has collaborated with volunteers to develop the Mriya project, which allows Ukrainians to flag Russian propagandistic websites and channels for further investigation. The project had led to over 22,000 removals by the end of 2023. [106] In March 2024, the Cyber Police rebranded Mriya into the Brama project, which has expanded its aims to include improving media literacy and safe behavior online. [107]

B3 0-4 pts

Do restrictions on the internet and digital content lack transparency, proportionality to the stated aims, or an independent appeals process?	**2** / 4

During wartime, certain laws provide government agencies with the authority to restrict content. Legislation also permits the government to restrict child sexual abuse imagery. [108]

The sanctions against Russian web platforms and websites prohibit "internet providers" from allowing access to the sanctioned resources, even though this term has not been defined in domestic law. (The Law on Telecommunications, for instance, regulates "operators and providers of telecommunications.") Further, the Law on the National Security and Defense Council implies that sanctions are only binding upon state bodies—and not upon "internet providers" or "operators or providers of telecommunications." [109] These inconsistencies have gone unaddressed when authorities have extended the sanctions.

In March 2024, the parliament registered a draft law that would subject "information-sharing platforms" to Ukrainian laws on ownership and funding transparency. The draft law mostly targeted Telegram, which, unlike many other widely used social media platforms and messengers, has not been designated as a Very Large Online Platform (VLOP) under the EU's Digital Services Act. [110] Thus, Telegram is the main platform in Ukraine that would be subject to the law. The draft law would recognize providers of information-sharing platforms as stand-alone actors in the media sphere and compel these platforms to appoint an official legal representative in Ukraine, unless they are registered or have a representative in the EU. When requested by the regulator, providers of information-sharing platforms would be required to disclose their ownership

structure and funding sources. Inability to do so would lead to the recognition of provider's ownership structure as "nontransparent." Existing legislation prohibits state and local self-government authorities, civil servants, and providers of financial services from using platforms that have nontransparent ownership structures, with similar restrictions to be considered for armed forces. [111]

In September 2024, after the coverage period, the Ukrainian government banned the use of Telegram by government officials. [112]

The Law on Media (see B6), which came into force in March 2023, enables the National Council on Television and Radio Broadcasting to issue fines, order the removal of content in violation of the law, and block websites in cases of noncompliance**.** The law classifies the dissemination of information that denies or justifies criminal nature of the 1917–91 communist totalitarian regime and Nazi totalitarian regime, or creates positive image of their leaders; contains any symbols of these regimes, or humiliates or insults Ukrainian language as significant offenses. Additionally, the law prohibits incitement to discrimination based on sexual or gender identity. [113]

In the conditions of a full-scale war, there are further regulations that apply from the moment a state is recognized by the Ukrainian parliament as an aggressor state and until five years after this status is canceled, subject to annual revision of the necessity to sustain limitations. Among them, media, including online outlets, are prohibited from disseminating information that presents armed aggression against Ukraine as an internal conflict or civil war; or inaccurate information about armed aggression and actions of an aggressor state with the aim to fuel hatred, forcefully change the constitutional order, or violate the territorial inviolability—all of which constitute "severe" offenses. They are also prohibited from disseminating materials, except for informational and analytical ones, from participants who have been included in the list of persons that present a danger to national security; that violation constitutes a "significant" offense. [114]

Online media outlets found guilty of violations are subject to fines, and repeated violations can lead to suspensions by the National Council on Television and Radio Broadcasting or bans by the courts. [115] ISPs will have three days to restrict access to websites of fully or temporarily banned online media. National groups, including the Independent Media Trade Union of Ukraine, and international

organizations, including the Committee to Protect Journalists (CPJ) have criticized the law for giving the National Council too much power to ban outlets and block websites. [116]

The Law on Media also allows the National Council to request providers of information-sharing platforms and representatives of search engines to restrict and exclude from search results material that is in violation of the law. [117]

A year since the Law on Media came into force, the National Council on Television and Radio Broadcasting had registered 290 online media, which include 229 websites, 21 YouTube channels, 13 Facebook pages, 12 Telegram channels, 8 Instagram pages, 4 TikTok accounts, 1 X account, 1 channel in Viber, and 2 channel in WhatsApp. For online media registration is voluntary but if completed provides official media status. [118]

In March 2023, following the ratification of the Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism, the Ukrainian parliament amended the Law on Sanctions to allow for the blocking of online resources that promote terrorist groups. [119]

The 2017 Law on State Support of Cinematography in Ukraine requires website hosts to limit access to pages containing unauthorized reproductions of certain categories of copyrighted materials upon a request from a copyright owner, if the owners of the pages fail to remove said materials. The website host can hide pages without a court order for up to 10 days. Hosting providers risk liability for noncompliance. [120]

B4 0-4 pts

Do online journalists, commentators, and ordinary users practice self-censorship?	**3**/4

Online journalists and ordinary internet users have faced pressure to self-censor, especially on topics related to separatism, collaborationism, terrorism, and Russia. Self-censorship in Ukrainian media also results from outlets' financial dependence on their owners, pressure on journalists, and impunity for perpetrators of many attacks on media or journalists. According to a May 2023 survey conducted by the Ilko Kucheriv Democratic Initiatives Foundation and Human Rights Centre ZMINA,

which covers the challenges journalists have faced since the beginning of the full-scale invasion, 78 percent of respondents said the Russian invasion has led to more self-censorship cases. [121] Likewise, IREX's 2024 Vibrant Information Barometer report notes that "journalists exercise self-censorship when covering defense issues" and "tend to refrain from criticizing the government or investigating misconduct" over fear that they might "ignite public outrage." [122]

Following the Russian military's invasion in February 2022, journalists avoided disclosing information about the location of Ukrainian military units, losses among Ukrainian soldiers, and specific places hit by Russian airstrikes, as doing so could have provided the Russian military with details about Ukrainian defenses. [123] Such disclosures may also have been prohibited by the implementation of martial law (see C1), which limits the topics journalists can cover.

B5 0-4 pts

Are online sources of information controlled or manipulated by the government or other powerful actors to advance a particular political interest?	**2** / 4

Domestic and foreign dis- and misinformation, particularly from Russia, [124] increased significantly following the 2022 full-scale invasion. Beyond social media manipulation, the online media landscape is highly polarized and frequently distorted. Media outlets tend to promote the political sympathies of their owners. [125]

Online news outlets and social media accounts affiliated with the Russian state have created fabricated content, including doctored videos and images, to intentionally mislead online audiences. [126] The SSU has also accused Russian actors of creating Telegram channels that mimic Ukraine government officials' channels and using them to spread disinformation. [127] In same way, Russian actors have mimicked fact-checking resources to spread false information about the war. [128]

Fabricated or intentionally misleading information disseminated by actors linked to the Russian government and presenting Kremlin-friendly narratives are regularly circulated in online articles that mainly target Ukrainians in areas occupied by the Russian military. [129] A February 2024 *Washington Post* report

revealed that in January 2023 Sergei Kiriyenko, the first deputy chief of staff of the Russian president, assembled a team to attempt to "destabilize" Ukraine through the spread of false or trumped-up narratives that aim to refute Ukrainian government talking points, emphasize splits between Ukrainian officials and other public figures, confuse residents of Ukraine, and "demoralize" the military. [130] Journalists in occupied territories have been forced to cooperate with occupying authorities and obtain approval from the Russian military before publishing. In occupied territories, people who have shared information that challenges the Russian military's narrative have been arrested, tortured, and killed on the spot. [131]

Additionally, as the Russian military continued its assault on Kharkiv throughout the coverage period, those who live in the city have received fake text messages, which are purportedly sent by government employees, instructing them to flee. The Russian military has used drones that "imitate cellular base stations," an unnamed Ukrainian security official told Reuters news agency, to spread these messages, which are often accompanied by similar campaigns on social media. [132]

To circumvent blocking in Ukraine, Russian actors spreading false information largely operate on social media platforms, such as Facebook and Instagram, and messenger apps, including Telegram and Viber, with Facebook and Telegram becoming the most popular channels of Kremlin supporters. [133]

Throughout the coverage period, social media platforms routinely removed networks spreading disinformation among Ukrainian users (see B2). In Meta's Adversarial Threat Report for the fourth quarter of 2023, the company said it had removed a network of 1,020 Facebook accounts, 711 Instagram accounts, 5 Facebook Pages, and 2 Facebook groups, that engaged in coordinated inauthentic behavior to post in support of Ukrainian politician Viktor Razvadovskyi. The Ukraine-based network was also active in promoting the current Kazakh government and criticizing the political opposition in comments on Kazakh news accounts. Meta also observed that Russian government-linked actors' targeting of Ukraine with disinformation narratives has been "particularly aggressive and persistent." [134] In Meta's Adversarial Threat Report for the second quarter of 2024, the company noted it removed a network of 12 Facebook accounts, 32 pages, 5 groups, and 3 Instagram accounts, originating from Russia but operated by a firm in Sri Lanka, that criticized the Ukrainian government. The network

established Facebook pages mirroring Ukrainian organizations and others that posed as influential figures in "the West." Meta removed several other operations that targeted the EU, and the United States and other countries in an effort to shift public opinion on the full-scale invasion of Ukraine. [135]

Between July and December 2023, TikTok removed six distinct covert influence operations' networks composed of 15,624 accounts, which primarily operated from Russia, though some operated from Ukraine, and aimed to influence public opinion about the war across the European Union. The company also removed 6,304 videos for violation of misinformation policy when reporting on the invasion of Ukraine, and continued removing livestream videos originating in Russia and Ukraine from the For You feed of users located in the EU to minimize risk of harmful content. As of December 2023, TikTok had tagged 114,218 videos with the state affiliated media label for Russia, Belarus, and Ukraine. [136]

Between the beginning of full-scale invasion and August 2024, the SSU reported that it shut down 86 bot farms, including over three million fake accounts, for spreading false information. [137]

The reporting period was also marked by a scandal around the largest state online news agency, Ukrinform. Leaked material posted online indicated that director general Oleksiy Matsuka, who had been expeditiously appointed in November 2023, had been following the instructions from president's office, on what topics and individuals should receive news coverage and which should be avoided. The six months of Matsuka's leadership were also marked by numerous dismissals of journalists who have been working in Ukrinform for many years, as well as unjustified salary bonuses for those loyal to new leadership and its managerial style. The revelations led to Matsuka's resignation in May 2024. Appointment of the new Ukrinform's director general Serhiy Cherevatyy also raised some concerns in the journalistic community who worry that his military background might impact the unprejudiced news coverage. [138]

In early 2024, several online media outlets and popular Telegram channels falsely claimed that a number of anticorruption activists were avoiding mobilization (see C7). [139]

Several Ukrainian groups work to identify content manipulation (see B7).

The Center for Strategic Communications and Information Security, part of the Ministry of Culture and Information Policy, has a mandate of countering disinformation. [140] In late November 2023, the center, along with few journalistic organizations, created a working group to develop recommendations addressed towards YouTube aimed at combatting the impact of Russian propagandistic channels. The group is also working on voluntary recommendations for establishing quality and transparency standards for Ukrainian YouTube channels and bloggers. [141] The National Security and Defense Council (NSDC) also has its own Center for Countering Disinformation. [142]

B6 0-3 pts

Are there economic or regulatory constraints that negatively affect users' ability to publish content online?	**2**/3

Online media in Ukraine are generally less constrained by economic pressures and owner interests than print and broadcast media. Lower production costs and generally liberal regulations have also contributed to the development of a vibrant online media landscape. There are no obligatory registration requirements for online media, though the Law on Media establishes a system of voluntary registration, which affords registered outlets more protections.

In 2022, at least 217 Ukrainian media outlets shuttered their operations due to loss of subscribers and advertisers, problems acquiring electronic and other supplies, lack of staff, and financial losses resulting from destruction, according to a February 2023 report from the Institute of Mass Information (IMI) and Reporters Without Borders (RSF). [143] However, during 2023, the internet advertising market in Ukraine increased by 78 percent, recovering to prewar levels. [144]

Prior to the war, many online media outlets already struggled to remain financially viable in a market deeply distorted by consolidated media conglomerates whose backers are willing to lose money in order to maintain the political influence afforded to them through media ownership. Independent online outlets rely mainly on advertising for funding, though some generate revenue by publishing *jeansa*—paid commercial or political materials disguised as journalistic content. [145] The amount of jeansa in Ukrainian online media sharply decreased at the

beginning of the war, but in early 2024 political jeansa was on the rise again, according to a report from the IMI. [146]

In May 2022, the so-called Oligarchs' Law, aimed at preventing threats to national security related to the excessive influence of oligarchs, entered into force. Significant influence on media is listed among criteria defining a person as oligarch. According to the law, oligarchs are banned from funding political parties and campaigns and must submit an income e-declaration. In June 2022, the president approved the NSDC decision to create the oligarchs' register, the launch of which was postponed until three months after the end of martial law in Ukraine. The Ministry of Justice was appointed in charge of the register instead of the NSDC. [147] According to initial NSDC estimates, 86 individuals might qualify as oligarchs. [148] However, the creation of the register was postponed.

The Law on Media, which entered into force in March 2023 (see B3), defines online media as "media that regularly disseminates digital information in textual, audio, audiovisual, or any other form via internet on its own website, except for media that are classified as audiovisual media." Bloggers are not considered online media unless they register under the law. The law also covers providers of video-sharing platforms, but only includes those that are not registered in EU member states and have either parent or subsidiary companies registered in Ukraine. [149] In mid-May 2023, to comply with the Law on Media, the regulator adopted procedure for registration of online media. [150] Additionally, the law includes transparency requirements and forbids ownership and funding of media in Ukraine by individuals and legal entities based in Russia. [151]

Press freedom organizations, including the Committee to Protect Journalists, have criticized the SSU's efforts to influence journalists covering the Ukrainian military, prevent them from covering certain operations, or withhold accreditation for journalists. [152]

Since January 2022, foreign technology companies providing services to users in Ukraine are obliged to pay a 20 percent value added tax (VAT) if the cost of the services they provide exceeds 1 million hryvnia ($25,300). Companies that fail to pay could be fined 195,000 hryvnia ($4,900). [153] Companies, like Adobe, Amazon, Meta, and Google, added the tax to customers' fees. In 2023, the state budget of Ukraine received 8 billion hryvnia ($202 million) from the tax. [154] In 2023, the tax

authorities began monitoring to identify the companies that still have not registered as taxpayers, [155] with PornHub having become the first one to pay fine in the amount of $5,543. [156]

B7 0-4 pts

Does the online information landscape lack diversity and reliability?	3 / 4

The online media landscape in Ukraine is generally pluralistic and diverse. Although the media sector in Ukraine faces challenges due to politicization (see B5 and B6), many online publications continue to publish quality reporting, including investigative journalism. At the same time, Ukrainian media face certain fact-checking and attribution challenge when reporting on developments where Russian media are the original source of information. [157] According to a 2023 study from the Institute of Mass Information, 68 percent of the top 50 online media outlets meet the Institute's transparency standards, which assesses publicly available data on staff, ownership, and funding, compared to 38 percent in 2022. [158] Although many television news channels have online presences, most are owned by oligarchs. And, while social media has been beneficial to the growth of independent media outlets, it has also facilitated the spread of Russian disinformation. [159]

The invasion created difficulties for independent media. Many outlets face financial struggles, and even major outlets have had to reduce salaries, shift to remote modes of work, ask for donations, and launch crowdfunding campaigns. Journalists must also contend with threats to their physical security (see C7) and psychological distress. In some cases, news outlets were unable to continue operations under occupation, and journalists evacuated. Nevertheless, local media play a critical role in documenting the Russian military's war crimes [160] and delivering news to people living in cities under Russian occupation, even as disrupted internet connectivity has made this coverage difficult. [161] To avoid broadcasting Russian propaganda, some local media outlets in cities under Russian siege closed their operations.

Journalists, politicians, and activists use social media, particularly Facebook and Telegram. Russian social media platforms remain available through VPNs and via

some ISPs that did not comply with sanctions orders, but their use among Ukrainians is low. [162]

According to a 2023 study by the Internews media support program in Ukraine, social media platforms have become the main source of news for many Ukrainians, with messengers gaining momentum during the war. Out of all platforms and messengers, 72 percent of Ukrainians use Telegram to consume news, while 15 percent use Viber for this purpose. Facebook and YouTube serve as a source of news for 19 and 16 percent of Ukrainians, respectively. News consumption on Instagram, TikTok and X were the lowest. [163]

Several Ukrainian groups work to identify content manipulation (see B5), such as TrollessUA, which identifies and flags suspicious accounts on Facebook, [164] and the Feykogryz project, which is a browser extension designed to identify disinformation, misinformation, and propaganda. [165] Following the full-scale Russian invasion, the independent analytical platform VoxUkraine launched a "Propaganda Diary," which logs Russian propaganda in Italian and German media, identifying those countries as among those intensively targeted by Russian disinformation. [166] Ukrainian Radio has also launched an "anti-fake program" to debunk Russian disinformation. [167] #DisinfoChronicle, started by the online portal Detector Media, collects and documents disinformation about the Russian invasion in real time. [168] Many Ukrainian media outlets also focus efforts on uncovering Russian mis- and disinformation related to the war. In 2022, Meta provided Ukrainian fact-checking partners StopFake and Vox with emergency funding to support their teams' safety and sustain their work during war time. [169] In February 2024, StopFake launched a Telegram bot for automated fact-checking of text, audio, and video content. [170]

As of May 2024, Tor, a browser that allows anonymous use, identified Ukraine as sixth on the list of countries in which users access Tor daily through relays. [171]

B8 0-6 pts

Do conditions impede users' ability to mobilize, form communities, and campaign, particularly on political and social issues?	**5**/6

The Ukrainian social media sphere is an important space for debate about politics, reforms, and civil society. Telegram channels are growing rapidly and are largely

focused on political issues. [172] However, in territories occupied by the Russian military, authorities prohibit public officials from using Telegram, Viber, and WhatsApp, when they are connected to Ukrainian mobile numbers. This effectively forces those users to register email addresses in the .ru domain. [173]

Ukrainians and Ukrainian government officials actively use e-petitions and online resources to publicize their activities and advocate for social and political issues. Since 2014, investigative journalists and activists have worked to maintain a digital database of officials' tax declarations. [174]

Ukrainians have launched several online campaigns to highlight the devastating impact of the war and rally international support. The global campaign #SuspendKremlin urged major social media platforms to ban Russian government officials from their platforms, in an effort to combat the spread of Russian state-sponsored disinformation. [175] Another group of volunteers created a website called Post to Stop War, which showcases key messages about the invasion in over 30 languages to audiences abroad. [176] Multiple online fundraising campaigns run by volunteers across the country have helped to collect funds to provide ammunition and equipment to Ukrainian soldiers. [177] Ukrainians have been actively using hashtags on social media to draw attention to the war and its consequences (e.g. #SaveUkraine, #StopWar, #PeaceforUkraine, and #RussiaIsATerroristState). [178] Dedicated online campaigns have been launched to collect evidence of Russian war crimes in Ukraine [179] and to track the damage inflicted by the Russian military. [180] In May 2022, President Zelenskyy launched UNITED 24, billed as "the official fundraising platform" to help Ukraine, [181] which had raised $658.8 million by June 2024. [182] However, critics have noted the funds are distributed in a centralized manner. [183]

Marginalized and underrepresented groups actively use online platforms to advocate for their rights. LGBT+ people in Ukraine regularly use social media tools to organize offline events, such as Kyiv Pride. However, they sometimes face resistance, also organized online, by far-right groups. [184]

C. Violations of User Rights

C1 0-6 pts

Do the constitution or other laws fail to protect rights such as freedom of expression, access to information, and press freedom, including on the internet, and are they enforced by a judiciary that lacks independence?	**3**/6

The right to free speech is granted to all citizens of Ukraine under Article 34 of the constitution, but the state can restrict this right in the interests of national security or public order, and it is sometimes restricted in practice. Article 15 of the constitution prohibits censorship. [185] Martial law has been in effect since February 2022, when the full-scale Russian invasion began, and some restrictions limiting speech have been enforced.

Ukrainian courts still feature corruption and political interference, which at times undermines their ability to uphold fundamental rights. [186] However, steps have been made during the reporting period to improve transparency and efficiency of the judicial system to align legislation and enforcement with EU requirements. Notably, in August 2023, the Ukrainian government enacted legislation that enabled it to appoint judges to vacant posts on the Constitutional Court based on a transparent procedure. In May 2024, the parliament approved the candidacy of the first judge selected through the new procedure via the Advisory Group of Experts. [187] Additionally, the High Qualification Commission of Judges and the High Council of Justice were reestablished and able to begin filling more than 2,000 open judicial posts. [188]

In May 2024, the parliament adopted in the first hearing a draft law that would limit access to court decisions concerning national security, state secrets, the inviolability of state borders, conscription and mobilization processes, and established order of military service under martial law.1 The draft law would also apply retroactively to all decisions since February 24, 2022, when martial law was introduced for the first time. The access is suggested to be renewed one year after the cancelation of martial law. [189] Human rights activists and journalists expressed concern that the draft measure could negatively influence both the freedom of speech environment and the transparency of judicial processes. [190]

Following the Russian military's full-scale invasion of Ukraine in February 2022, the Ukrainian government imposed martial law, which, according to the constitution, enables the government to restrict some rights, including the right to freedom of

expression. [191] Specifically, martial law gives the government the right to "control the media," prohibits "public demonstrations and other mass gatherings," and transforms civilian authorities into military administrations. [192] The law has been repeatedly extended and the ban on mass gatherings have occasionally been enforced. In April 2024, Ukraine has submitted to the Council of Europe an updated list of derogation measures, some of which are permitted by the Convention for the Protection of Human Rights and Fundamental Freedoms during martial law. [193]

C2 0-4 pts

Are there laws that assign criminal penalties or civil liability for online activities, particularly those that are protected under international human rights standards?	**2** / 4

Some laws criminalize online activities, while others do not explicitly criminalize them, but have been used to penalize individuals for their online activities. The criminal code penalizes extremism, separatism, and terrorism, including through online activities. Article 109(2) of the criminal code prescribes prison sentences of three to five years for public calls to violently overthrow the constitutional order. Article 110 criminalizes public calls for the infringement of Ukraine's territorial integrity, including those made online, with a maximum penalty of five years in prison. Article 161 prohibits "inciting national, racial, or religious enmity and hatred" and assigns a maximum penalty of five years in prison. [194] Neither defamation nor insult are criminally penalized. [195]

In March 2022, following the Russian military's full-scale invasion of Ukraine, the parliament adopted amendments to the Law on Political Parties and the Law on Civic Associations. The amendments allowed courts to ban political parties, and prohibited the creation of civic associations that undertake actions or aim to liquidate the independence of Ukraine, make violent attempts to change constitutional order, undermine sovereignty and territorial integrity, disseminate war propaganda, propagate communist or Nazi totalitarian regimes and their symbols, or disseminate information containing justification, legitimization, or denial of the armed aggression of the Russian Federation against Ukraine. In the same month, the parliament adopted amendments to the criminal code specifying punishments for justification, legitimization, or denial of the armed aggression of

the Russian Federation against Ukraine launched in 2014, including by calling it internal civil conflict, as well as of temporary occupation of some parts of Ukraine's territory. [196] Under Article 436-2, which criminalizes justification, recognition as legitimate, or denial of the armed aggression of the Russian Federation against Ukraine violators can face up to eight years in prison if the offenses are committed on mass media or by a public official.

In the same month, the parliament criminalized collaborationism with the Russian government under article 111 of the criminal code in the form of public denial of the armed aggression against Ukraine; supporting the occupation of Ukrainian territory; or public calls by a citizen of Ukraine for cooperation with the aggressor state, its armed formations, or occupation administrations. The law, which applies to online speech, also criminalized denying Ukrainian sovereignty over the occupied territories. Individuals found guilty can be deprived of the right to hold certain positions or engage in certain activities for a period of 10 to 15 years. Certain nonspeech related offenses under the amendments carry heavier punishments. [197] A December 2022 coalition of Ukrainian civil society organizations criticized the breadth and vagueness of some of the measures included in the amendments. [198]

In June 2022, the president signed a law prohibiting "propaganda of the Russian neo-Nazi totalitarian regime and the act of aggression against Ukraine." Among other things, the law envisages a ban on the usage of symbols associated with the Russian military invasion in Ukraine, including in online advertising and social media publications. However, there are a few exceptions when such usage is considered legal, including media reporting on false narratives, publications condemning the Russian regime, museum exhibitions, research activities, and school textbooks. [199]

Article 173-1 of the code of administrative offenses prescribes fines for spreading false rumors that sow panic; the law was periodically invoked during the COVID-19 pandemic. [200] Since January 2019, the code of administrative offenses penalizes bullying, including via electronic communication, punishable by fines or community service. Individuals who fail to report bullying can also be penalized. [201]

C3 0-6 pts

Are individuals penalized for online activities, particularly those that are protected under international human rights standards?	3/6

Since the start of the Russian military's full-scale invasion, several individuals have been charged under criminal code articles 109, which criminalizes actions aimed at the violent change or overthrow of the constitutional order or at the seizure of state power; 110, which prohibits public calls for the infringement of Ukraine's territorial integrity; 111-1, which criminalizes collaborationism or high treason; and 436-2, which criminalizes justification, recognition as legitimate, or denial of the armed aggression of the Russian Federation against Ukraine. These charges sometimes solely concern online activities, while other charges include material collaboration with the Russian military or intelligence agencies. Proceedings opened under Article 436-2 were commonplace throughout the coverage period. [202] Russian authorities in occupied territories have also detained individuals who criticize Russia or promote a free Ukraine (see C7).

The SSU has frequently invoked criminal code Articles 109 and 110 against alleged Russian agents for various forms of speech online. [203]

In March 2024, a first instance court in Khmelnytskyi found a local resident guilty of collaborationism under Article 111-1 for Odnoklassniki posts in support of Russia's invasion and imposed a 10-year ban on occupying civil servant positions. [204] In February, the same court found another individual guilty under Article 111-1 and issued a 10-year ban preventing them from holding managerial and administrative positions. [205]

In December 2023, the SSU charged an ISP owner, who provided internet services in the temporarily occupied areas of Luhansk region and cooperated with occupation authorities to broadcast sanctioned Russian channels, under Article 111-1 in Kyiv. [206] The SSU also invoked Article 111-1 to charge a former civil servant, who the SSU alleged was an FSB agent, calling for the Russian annexation of eastern Ukraine on social media. [207] In December 2023, a Vinnytsia court found a freelance journalist, who was working for a pro-Russian propagandistic online media, guilty of high treason and sentenced him to 14 years in prison with property confiscation. [208] However, the decision was appealed and sent back to the first-instance court for a new hearing in May 2024. The new decision was still

pending as of the end of the coverage period. [209] In July 2023, an Odesa court ruled that calls by a blogger to bomb Ukraine were collaborationism and imposed a 10-year ban on working for the state. [210]

In 2024, the courts started invoking Article 114-1 of the criminal code on obstruction of legitimate activity of the armed forces against users who shared information about where draft summonses were being issued. In March, the court in Lutsk sentenced a woman to five years in prison for administering a Telegram channel that notified residents about the places in the city where draft notices are handed out. The imprisonment was substituted with a two years' probation period, and the Telegram channel was shut down. [211] In May 2024, a court in the Cherkasy sentenced a man who had administered a similar Viber group to five years of imprisonment with one year of probation period. [212] In January 2024, three administrators of Telegram channels and Viber groups in Cherkasy Region also had their channels shut down for similar activity. [213] In April 2024, the SSU detained a TikTok blogger and confiscated his mobile phone, laptop, and memory drives with video materials for sharing online military checkpoints' location in his city. [214]

In February 2024, the authorities charged or sentenced several individuals under Article 436-2, the article about justifying Russian military aggression against Ukraine, which was also increasingly used during the coverage period, For instance, a Poltava resident was sentenced to five years in prison, which was substituted with two years' probation, under Article 436-2 for Odnoklassniki posts denying Russia's war against Ukraine. [215] The SSU also charged a blogger in Kyiv, who had allegedly used his YouTube channel and social media accounts to deny Russian aggression, discredit the armed forces leadership, and share disinformation about the social and political situation in Ukraine, under Article 436-2 of the criminal code. The man faces 8 years in prison with property confiscation. [216] Also in February, another woman was charged under Articles 109, 110 and 436-2 for coordinating propagandistic messages of former prime minister Mykola Azarov in Azarov's Telegram channel and on social media, as well as setting up anti-Ukrainian interviews and commentaries for Russian media. The case was in the court as of the end of the coverage period, and the accused woman remained in custody. [217] In February 2024, the SSU charged a man in Poltava under Article 111 and 436-2 for drafting over 60 publications for Russian

online media, which were financially supported by Russian intelligence agencies, that justified shelling of civilian infrastructure and aimed to discredit Ukrainian military and its leadership. [218] In April 2024, he was sentenced to 15 years in prison. [219]

In January, authorities in Mykolaiv invoked Article 110 to charge a woman for creating and sharing anti-Ukrainian posts in pro-Russian Telegram channels. [220] In December 2023, a Khmelnytskyi resident was sentenced to five years in prison, which was substituted with 18 months' probation period, for a similar offense. [221]

In July 2023, a court in Poltava Region imposed a fine of approximately $1,300 on the administrator of an online media outlet who published Russian ads and accepted payments via a banned payment system. [222]

In late 2020, the SSU charged politician and pro-Kremlin blogger Anatoliy Shariy under Articles 111 and 161 (infringing upon citizens' equality) of the criminal code for posting a map of Ukraine on his YouTube channel that excluded the occupied territories of Crimea and Donbas. The SSU put Shariy—who lives in Spain, where he had received asylum—on its wanted list. [223] In May 2022, Spanish authorities detained Shariy, [224] and later released him to house arrest pending extradition. [225] Reportedly, in October 2022, the Spanish court closed the case after Ukrainian officials failed for a second time to file extradition paperwork. [226] In July 2023, the SSU charged him with committing high treason at the behest of the Russian security services, namely for editing and disseminating videos about the torture of Ukrainian war prisoners. [227]

In the occupied city of Berdyansk in the Zaporizhzhia Region, the Russian occupying authorities have conducted random checks of Ukrainian citizens' mobile phones with the aim to identify whether they follow "propagandistic resources of the Kyiv regime." If found guilty, a person first gets a warning, which then can be followed by fine and criminal liability according to Russian law. [228]

C4 0-4 pts

Does the government place restrictions on anonymous communication or encryption?	**3**/ 4

There is no obligatory registration for internet users or prepaid mobile device subscribers. Users can purchase prepaid SIM cards anonymously and may comment anonymously on many websites. The Law on Electronic Communications (see A3 and C6) preserves the right to use communication services anonymously.

There are no restrictions related to encryption tools in government-controlled territory, though the commercial provision of these tools is subject to licensing. [229] VPNs are widely used in Ukraine.

However, in occupied areas of Kherson and Zaporizhzhia Regions, users reportedly experienced issues accessing VPNs. In March 2024, the authorities in the Russian-occupied territories banned the "promotion" of VPNs, mirroring a recently passed Russian law. [230] The occupying authorities also prohibit residents from using Ukrainian mobile numbers and force employees of public institutions to register email addresses in .ru domain. [231] In occupied settlements of the Zaporizhzhia Region, payment for utilities, internet, and mobile credit is conditioned upon obtaining a Russian passport. [232]

C5 0-6 pts

Does state surveillance of internet activities infringe on users' right to privacy?	**3**/6

Little information about surveillance or communications interception in Ukraine is publicly available. The SSU and police can initiate criminal investigations and use wiretapping devices on communication technologies, but existing legislation, such as the Law on Operative Investigative Activity, [233] does not specify the circumstances that justify these measures or set limits on the time frame or scope of their implementation. However, during the coverage period investigative journalists alleged that an SSU unit wiretapped their phones (see C7). [234]

Previous governments had purchased equipment compliant with the Russian-designed System for Operational Investigative Measures (SORM) surveillance architecture. [235] Some analysts believe that Ukrainian law enforcement and intelligence services make use of an analogous architecture, requiring operators to install equipment that facilitates the lawful interception of user data. [236]

Deep packet inspection (DPI) technology can be used to filter internet traffic and surveil users. Authorities have repeatedly tried to oblige providers to install DPI for these purposes, but their efforts have been unsuccessful. Mobile operators Kyivstar and Vodafone use DPI systems, ostensibly to allocate resources more effectively, analyze subscribers' preferences, and enhance targeted advertisements. Kyivstar claims its system handles depersonalized data. Lifecell has not disclosed whether it has a DPI system. [237]

In March 2024, given the intensified shelling of Kyiv by Russia's military, city authorities announced new security measures that including monitoring social media for disinformation and provocative content aimed to destabilize the situation in the Ukrainian capital. There is no clear evidence how this measure was (if at all) enforced. [238]

C6 0-6 pts

Does monitoring and collection of user data by service providers and other technology companies infringe on users' right to privacy?	**3**/6

Previously, ISPs were not legally required to aid the government in monitoring the communications of their users in the absence of a court order, but recent laws on Electronic Communications and Intelligence have provided the government with ways to circumvent a court order.

The Law on Electronic Communications obliges providers of electronic communication services to retain users' personal data, location data, and data-transfer routes. This data can be shared with the government only when the law is violated and when an investigating judge or court has issued a request. The law stipulates that electronic communications services must give the state the technical ability to access communications; the state may do so autonomously. The law also envisages that operators must ensure the integrity of their subscribers' data, which can only be disclosed after subscribers have given explicit consent or if they have violated the law. [239] In March 2022, the parliament amended the law to allow prosecutors, along with courts and investigative judges to gain access to subscribers' information and metadata. [240]

The Law on Intelligence enables the intelligence authorities to autonomously intercept information from telecommunications networks. According to the law,

interception can begin up to 72 hours before a court order is issued. Moreover, court orders (both approving and denying interception) are not subject to being recorded in a unified register. Civil society claims that the law was adopted without proper public consultation and contains significant contradictions to the country's constitution and the European Convention on Human Rights. [241]

C7 0-5 pts

Are individuals subject to extralegal intimidation or physical violence by state authorities or any other actor in relation to their online activities?	**1** / 5

Following the full-scale Russian invasion, journalists in Ukraine have faced extreme danger due to Russian attacks while conducting their work. According to human rights experts at the United Nations, journalists have been "targeted, tortured, kidnapped, attacked, and killed, or refused safe passage" [242] from cities and regions under Russian siege. Reporters Without Borders (RSF) filed eight war crimes complaints with the International Criminal Court and Ukraine's prosecutor general covering 53 total acts of violence and abuse involving 121 journalists by May 2023. [243] A May 2024 report from IMI found that during 27 months of war, Russian forces had committed 599 crimes against both online and offline journalists and media in Ukraine, including the forced disappearance of administrators of two pro-Ukrainian Telegram channels, and the seizure of 20 editorial offices of Ukrainian media for dissemination of propaganda in occupied territories. The report also notes that 80 journalists have been killed, 10 of whom were performing editorial assignments. [244]

In 2023, the IMI recorded 150 "violations of freedom of speech" against both online and offline journalists (almost a fourfold decrease compared to 2022) out of which 67 were attributed to Russia. The number of violations committed by Ukrainian private and public actors dropped from 97 to 83 during the same period, with 29 recorded violations involving obstruction of legitimate journalistic activity. [245] In 2023, law enforcement opened 77 criminal cases involving violations of journalists' rights, out of which seven have been sent to courts with the charges classified under Articles 171 (obstruction of legitimate journalistic activity) and 345-1 (threat or violence against a journalist). However, the number of investigated crimes against journalists still demonstrates a 74 percent decrease compared to prewar period. [246] In the first quarter of 2024, 22 additional criminal

proceedings were registered, out of which six were closed and one sent to the court. [247]

Human rights groups have reported that Russian soldiers have forced Ukrainians in occupied cities and towns to turn over their cell phones and have killed people who refused to comply. [248] The Russian occupying authorities in Zaporizhzhia have also detained those who operate critical Telegram channels. In August 2023, the Russian military captured Oleksandr Malyshev, Heorhiy Levchenko, Maksym Rupchov, Yana Suvorova, Mark Kaliush, and Kostiantyn Zinovkin, who ran the "RIA Melitopol South" and the "Melitopol Is Ukraine" Telegram channels. The Russian occupying authorities announced their detention two months later in October, and that they faced between 12 and 20 years in prison for treason. [249] Anastasia Glukhovskaya, who worked for the online news outlet RIA Melitopol prior to the invasion, was also captured in August. In May 2024, the Russian occupying authorities announced they had detained Vladyslav Herson, who also contributed to the Melitopol is Ukraine Telegram channel. [250] In May 2023, the Russian occupying authorities captured retired journalist Iryna Levchenko and her husband in Melitopol. In August 2023, Victoria Roschyna, a freelancer working for Ukrainian Pravda, was taken captive in Berdiansk and her family was informed that she was held prisoner in Russia in May 2024. [251]

Nonphysical acts of harassment and doxing remain a problem. [252] In January 2024, reports indicated that key anticorruption activists faced a coordinated harassment campaign by some online media and Telegram channels accusing them of avoiding mobilization (see B5). [253] Later in April, following a search of the chairman of the board of Kharkiv Anticorruption Center, civil society activists issued a demand towards the president and other respective authorities to stop the persecution of anticorruption activists and investigative journalists. [254]

In May 2024, the police opened criminal proceedings in the case of Mykhailo Tkach, lead investigative reporter at the online media outlet Ukrainska Pravda, who became a target of anonymous online threats after publishing an investigation about the travels of wealthy Ukrainians. His fellow colleagues received similarly threatening emails. [255]

In April 2024, the SSU attempted to issue a military summons to a journalist of the investigative agency Slidstvo.Info in retaliation for his reporting about luxury

properties of the head of the SSU cybersecurity department. [256] After the case went public, the commander in chief of the Ukrainian Armed Forces ordered an internal investigation, [257] which immediately resulted in the suspension of the head of the respective territorial mobilization center. [258] Subsequently, the head of the cybersecurity department was fired by presidential decree. [259]

In January 2024, investigative media outlet Bihus.Info reported that the 30 individuals in the SSU's Department for the Protection of National Statehood had surveilled their team for months, including by attending a party in December where they filmed employees ordering illegal drugs. The outlet also claimed that their team members' phones had been wiretapped for around a year (see C5). [260] At the end of the month, Roman Semenchenko, the head of the SSU Department for the Protection of National Statehood was fired by Zelenskyy. In the wake of the scandal, the SSU launched an investigation into the potentially illegal use of "technical means" to surveil the outlet. [261]

The intimidation of marginalized groups online is common. LGBT+ individuals frequently face online harassment. [262] In March 2024, the National Council on Television and Radio Broadcasting issued an order to a nongovernmental organization for publishing on its website an article that incited hatred and discrimination towards LGBT+ individuals. [263] Earlier in July 2023, a regional online media outlet in Sumy was harassed and its employees doxed for their coverage of LGBT+ issues on YouTube and their website. [264]

In July 2020, the prosecutor general filed charges against Vladislav Manger and Oleksiy Levin, two officials from Kherson, of ordering the 2018 murder of journalist Kateryna Handziuk, who used social media platforms and the local citizen journalism website MOST to expose corruption. Five people found guilty for carrying out the acid attack were jailed in 2019. [265] During the coverage period, the court sentenced Manger and Levin to 10 years each in prison, inclusive of time spent in the pretrial custody. [266] The civil lawsuit for compensation of moral damages was satisfied, with around $380,000 paid to Handziuk's parents and husband. [267] Both convicted have challenged decision in the appellate court, and the hearings were ongoing at the end of the reporting period. [268]

Investigations and prosecutions for the 2016 murder of Pavel Sheremet, a journalist with the online newspaper Ukrainska Pravda, have been characterized by

delays and mismanagement. [269] In September 2021, the judge leading Sheremet's case was found dead. [270] In June 2023, after three years of hearings, the composition of the jury was changed, and as a result the case will be heard again from the scratch. [271] In January 2024, the court hearings were suspended as two out of three suspects are serving in the military. [272]

C8 0-3 pts

Are websites, governmental and private entities, service providers, or individual users subject to widespread hacking and other forms of cyberattack?	**1** / 3

Cyberattacks, including distributed denial of service (DDoS) attacks, from Russian-aligned actors intensified significantly during Kremlin's full-scale invasion of Ukraine, though Ukrainian government agencies have worked to mitigate the impact of these attacks. While online media outlets, journalists, and human rights defenders, are frequently subject to cyberattacks, there is no indication that the Ukrainian state is involved in these attacks.

In 2023, the SSU reported that it had neutralized over 4,000 cyberattacks on public authorities' databases and informational resources, and objects of critical infrastructure. [273] In 2023, the Computer Emergency Response Team of Ukraine (CERT-UA) processed 2,543 cyber incidents, a 15.9 percent increase from 2022. CERT-UA classified 367 of these attacks as "serious," representing a 65 percent decline compared to 2022. I February 2024, the SSSCIBP reported that cyberattacks by Russian hackers against Ukrainian information systems had intensified in comparison to 2023. [274]

In December 2023, the leading Ukrainian mobile operator Kyivstar suffered a massive attack by Russian hackers, resulting in partial destruction of company's IT infrastructure and loss of mobile connectivity and internet by users (see A1). The services were gradually restored throughout the next several days. During this period, the national roaming system allowing users to switch between mobile operators was disabled to avoid network overload. [275] Subsequently, Kyivstar has allocated $90 million to repair damage, strengthen the system and fund a client-loyalty program. [276] In April 2024, CERT-UA announced it successfully identified an attempt by Sandworm hacking group, which is linked to Kremlin intelligence

services, to disrupt information and communication systems of over two dozens of critical infrastructure providers across 10 regions in Ukraine. [277]

Between February 2022 and May 2024, IMI recorded 86 cyberattacks on websites and social media channels of Ukrainian online media. Moreover, some local media's websites are periodically suffered distributed denial-of-service (DDoS) attacks following publications unfavorable towards the local authorities and public persons. [278] Russian hackers have regularly disrupted broadcasting of Ukraine's television channels [279] and online media. [280] Hackers have also targeted news outlets' social media accounts; for instance, in February 2024, Ukrainian Pravda's X account was hacked to display pro-Russia messages. [281] In late February 2024, the parliament's website was hacked to display a link to a fake Telegram channel. [282] In November 2023 and May 2024, Hromadske Radio suffered massive DDoS attacks, rendering its website unavailable. [283]

Russia-aligned actors have also sent phishing emails, [284] offered Ukrainian regional media to purchase their websites, [285] hacked computer systems of law enforcement agencies [286] and tablets used by Ukrainian military to plan combat operations, [287] the websites of ministries, [288] Kyiv Regional Council, [289] the leading gas supply provider, [290] the Kyiv city train, [291] and the Coordination Headquarters for the Treatment of Prisoners of War [292], as well as mimicked legitimate media resources [293] and created fake Telegram channels, such as those of Ukrainian military brigades and battalions. [294]

According to the CERT-UA report, in the second half of 2023, the Russian hackers increasingly targeted the mobile phones of Ukrainian military, actively using messengers, mostly Telegram and Signal, to disseminate malicious software. [295] Similar attacks via Signal targeted civil servants, military, and defense sector employees. [296]

In January 2024, the SSU issued a warning of a massive email campaign offering monetary rewards for collaborating with Russian intelligence services. The campaign targeted both ordinary citizens and employees of state authorities and private companies. [297]

Note on sources: The reports cited in footnotes 121 and 245 produced by Human Rights Centre ZMINA and the Institute of Mass Information were funded in part of

or in full by Freedom House.

Footnotes

1. International Telecommunication Union (ITU), "Interim assessment on damages to telecommunication infrastructure and resilience of the ICT ecosystem in Ukraine," December 2022, https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Interim.
2. International Telecommunication Union (ITU), "Country ICT Data (Latest available data)," accessed April 2024, https://datahub.itu.int/data/?e=UKR&u=
3. George Ingram and Priya Vora, "Ukraine Digital Resilience In A Time of War," Center for Sustainable Development at Brookings, January 2024, https://www.brookings.edu/wp-content/uploads/2024/01/Digital-resilience...
4. Simon Kemp, "Digital 2024: Ukraine," DataReportal, February 23, 2024, https://datareportal.com/reports/digital-2024-ukraine?rq=ukraine
5. Speedtest Global Index, "Median Country Speeds – May 2023," https://www.speedtest.net/global-index/ukraine.

More footnotes

On Ukraine

See all data, scores & information on this country or territory.

See More ›

Country Facts

Population

38,000,000

Global Freedom Score

49 /100 **Partly Free**

Internet Freedom Score

59 /100 **Partly Free**

Freedom in the World Status

Partly Free

Networks Restricted

No

Social Media Blocked

Yes

Websites Blocked

Yes

Pro-government Commentators

Yes

Users Arrested

Yes

In Other Reports

Freedom in the World 2024

Other Years

2023

Be the first to know what's happening.

Join the Freedom House weekly newsletter

Subscribe

ADDRESS

1850 M St. NW Floor 11
Washington, DC 20036
(202) 296-5101

GENERAL INQUIRIES

info@freedomhouse.org

PRESS & MEDIA

press@freedomhouse.org