

Flygtningenævnets baggrundsmateriale

Bilagsnr.:	342
Land:	Ukraine
Kilde:	Freedom House
Titel:	Freedom on the Net 2018 – Ukraine
Udgivet:	1. november 2018
Optaget på baggrundsmaterialet:	4. februar 2019



Freedom on the Net 2018 - Ukraine

Publisher [Freedom House](#)

Publication Date 1 November 2018

Cite as Freedom House, *Freedom on the Net 2018 - Ukraine*, 1 November 2018, available at: <https://www.refworld.org/docid/5be16af1a.html> [accessed 3 December 2018]

Disclaimer This is not a UNHCR publication. UNHCR is not responsible for, nor does it necessarily endorse, its content. Any views expressed are solely those of the author or publisher and do not necessarily reflect those of UNHCR, the United Nations or its Member States.

Status: Partly Free
Total Score: 45/100 (0 = Best, 100 = Worst)
Population: 44,831,159
Internet Penetration: 52.5%
Social Media/ICT Apps Blocked: Yes
Political/Social Content Blocked: Yes
Bloggers/ICT Users Arrested: Yes
Freedom in the World Status: Partly Free

Key Developments, June 1, 2017 – May 31, 2018

- The government blocked over 200 websites, and an increasing number of legislative proposals have contained broad provisions for blocking webpages on national security grounds, often without requiring court orders (see Blocking and Filtering).
- Law enforcement officers and the Security Service of Ukraine raided the offices of *Strana* and *Vesti*, two Ukrainian online news outlets with pro-Russian stances (see Intimidation and Violence).
- Ukrainian authorities arrested a number of social media users, while Russian-backed separatist authorities in Luhansk sentenced a blogger to 14 years in prison (see Prosecutions and Detentions for Online Activities).
- In June 2017, Ukraine experienced the devastating 'NotPetya' cyberattack, which has been traced back to Russia (see Technical Attacks).
- In January 2018, some Ukrainian mobile operators received 4G licenses (see Availability and Ease of Access).

Introduction:

Ukraine's online environment remained tense in 2018 after a sharp decline in internet freedom in 2017. Ukrainian authorities increasingly blocked pro-Russian or pro-separatist webpages, while a devastating cyberattack in June 2017 destabilized government ministries, private companies, and vital infrastructure across the country.

The ongoing conflict and information war with Russia pose significant challenges to internet freedom. In late spring and summer of 2014, Russian and pro-Russian forces occupied the Crimean peninsula and later took control of parts of the Donetsk and Luhansk regions. De facto authorities of the self-proclaimed Donetsk People's Republic (DPR) and Luhansk People's Republic (LPR) have sought to disrupt or regulate access to telecommunications, and residents in the region often experience internet disruptions. De facto authorities have also pressed internet service providers (ISPs) to take down or block particular services, such as Ukrainian news websites in Donetsk,^[1] Luhansk,^[2] and Crimea.^[3]

Ukrainian authorities have used the ongoing conflict to justify incursions on internet freedom. Several Russian platforms including Vkontakte and Odnoklassniki have been blocked since May 2017, and state officials blocked over 200 more webpages during this reporting period alone. An increasing number of legislative initiatives have been proposed that would provide more power to the government to block webpages on broad grounds often without court orders. While the draft laws have not been passed, thanks to pressure from local civil society, these efforts showcase the government's increasing determination to control the digital sphere.

Content manipulation by trolls favoring both sides of the dispute have flourished on social media, and dozens of journalists, bloggers, and social media users have been prosecuted by both Ukrainian and de-facto authorities. Online journalists, bloggers and citizen journalists also continue to face digital and physical security threats. In June 2017, Ukraine suffered a massive cyberattack that was "felt around the world."^[4] Russia is believed to be behind that attack. As part of response, Ukrainian MPs passed a new framework law on cybersecurity.

Ukrainian civil society has a vital presence online. Activists used social media for a range of reasons, including to coordinate volunteer support for the military, stay up-to-date on developments in eastern Ukraine, assist internally displaced populations, encourage government oversight, advocate for human rights, and expose biased or manipulated information online.

Obstacles to Access:

Internet penetration continued to grow in 2018. Access to the internet remains affordable for most of the population. The diverse market is no longer dominated by state-owned providers. Inevitably, Ukraine's telecommunications market has suffered due to economic hardships in the country, the crisis following Russia's annexation of Crimea, and the upheaval in eastern Ukraine.

Availability and Ease of Access

The availability and ease of access varies sharply in various regions of Ukraine. De facto authorities in the self-proclaimed DPR and LPR have gradually forced out Ukrainian ISPs. In October 2016, the de facto authorities in Luhansk issued a decree mandating that internet service be supplied only by local "state-owned" providers. The Donetsk office of Ukraine's largest ISP, UkrTelecom, was seized by de facto authorities in March 2017, leaving some 200,000 users without a landline phone connection and mobile internet.^[5] In the absence of Ukrainian ISPs, internet traffic in the occupied territories is now largely routed through Russia.^[6]

Infrastructure is more developed in urban areas, though the urban-rural divide has been narrowing slightly over time. Internet penetration in rural areas rose from 45 percent in 2015 to 52 percent in 2017, according to one estimate.^[7] Most people access the internet from home or work, though many cafes and restaurants provide free Wi-Fi. Access is also common in public libraries, schools, shopping malls, and airports. It has also become available in some public transport, like high-speed trains. Monthly subscriptions are fairly affordable for most of the population, with monthly

fixed-line broadband costing as low as UAH 80-130 (US \$4-5), and monthly mobile broadband costing as low as UAH 40-70 (US \$1.50-\$2.50) in 2017.

Mobile internet use continued to grow in Ukraine, with some data suggesting that 42 percent of Ukrainians used smartphones or mobile phones to access the internet in 2017.^[8] An estimated 35 percent of the population owned a smartphone.^[9] Mobile operators were granted 3G licenses in 2015, greatly facilitating mobile internet use. While speed and coverage remains relatively poor compared to mobile data services in other countries,^[10] the 3G network continued to expand to more towns and cities in 2017.^[11] In January 2018, leading Ukrainian mobile operators received 4G licenses, which is expected to foster better-quality mobile internet connection across the country.^[12]

While there is a lack of reliable information about internet availability and levels of penetration in the so-called DPR and LPR, occasional media reports suggest that some communities have limited access to the internet due to poor infrastructure and slow connection speeds.^[13] Reportedly, the cost of monthly subscriptions is relatively similar in occupied areas, although prices fluctuate depending on company and the quality of service differs greatly.^[14]

Restrictions on Connectivity

Restrictions on connectivity are most common in the occupied LPR and DPR. A number of disruptions were reported during the coverage period, including in October 2017,^[15] which de facto authorities blamed Ukraine for disconnecting channels for data transmission,^[16] and in April 2018.^[17] In January 2018, Vodafone's mobile telecommunications services, a remaining Ukrainian mobile operator functioning in LPR and DPR, were disrupted in the region.^[18] Representatives of the de facto authorities reportedly said that Vodafone would not be allowed to restore connectivity in the region due to political reasons.^[19] While the connection was partially restored in April, the situation remained unsettled.^[20] Some confusion exists surrounding the cause of the initial disruption and reasons for its continuation, particularly on whether the disruption was an infrastructural or political issue.

Internet disruptions remained local in part because Ukraine's diverse internet infrastructure makes it resilient to disconnection. The backbone connection to the international internet in Ukraine is not centralized, and major ISPs each manage their own channels independently, though the formerly state-owned UkrTelecom remains dominant (see ICT Market). Ukraine's backbone internet exchange, UA-IX, allows Ukrainian ISPs to exchange traffic and connect to the wider internet. The country has a well-developed set of at least eight regional internet exchanges, as well as direct connections over diverse physical paths to the major western European exchanges.^[21]

ICT Market

The Ukrainian telecommunications market is fairly liberal and undergoing gradual development. Overall, approximately 6,000 providers and operators of telecommunications operate, according to the National Commission for the State Regulation of Communications and Informatization (NCCIR).^[22]

The state previously owned 93 percent of the largest telecom company and top-tier ISP, UkrTelecom, but the company was privatized in March 2011.^[23] Authorities were investigating alleged irregularities in the privatization agreement, though the company denied involvement. A court case is currently pending.^[24]

UkrTelecom is still the largest ISP in the country. Other telecommunications providers are dependent on leased lines, since UkrTelecom owns the majority of the infrastructure, and many alternative providers lack resources to build their own networks. However, UkrTelecom does not exert any pressure or regulatory control over other ISPs.

Other major ISPs in Ukraine include Volia, Triolan, Fregat, Datagroup, Lanet, and Vega.^[25] Kyivstar (owned by Dutch VimpelCom Ltd) is the second largest ISP,^[26] and one of three major players in the mobile communications market, along with Vodafone Ukraine and "lifecell" (formerly "life"), owned by Astelit, whose main shareholders are the Turkish company Turkcell and Ukrainian System Capital Management. Together, these companies hold 94.6 percent of the mobile communications market.^[27]

Ukrchastotnagliad, the Ukrainian frequencies supervisory center, reports that 86 operators have licenses to provide satellite communication services in Ukraine. Companies providing internet access using satellite technologies in Ukraine include Ukrsat, Infocom-SK, Spacegate, Adamant, LuckyNet, Ukrnet, and Itelsat. With the exception of Infocom-SK,^[28] all of these companies are privately owned.^[29]

There are dozens of local ISPs in the occupied areas, according to available reports. Intertelecom is reportedly the only Ukrainian ISP still operating in some parts of the occupied areas.^[30] Other Ukrainian ISPs were forced out of the region, and then some local providers took over remaining infrastructure and assets. For example, Komtel took over Ukrtelecom's assets in Donetsk,^[31] while Fenix operates on Kyivstar's network and infrastructure.

There are no direct barriers to entry into the ICT market, but any new business venture faces obstacles including bureaucracy and corruption, as well as the legal and tax hurdles common to the Ukrainian business environment. In particular, the Ukrainian ICT market has been criticized for its difficult licensing procedures for operators – under the 2003 Law on Communications, operators are required to have a license before beginning their activities. Regional ISPs are usually smaller local businesses, and regional dominance largely depends on business and other connections in a specific region, making the market prone to corruption.

Regulatory Bodies

The ICT sector is regulated by the NCCIR, which is subordinate to the president and accountable to the parliament.^[32] The president also appoints NCCIR members. Current members include former government officials and professionals with backgrounds in engineering, security, and communications. The 2003 Law on Communications outlines that the president approves NCCIR regulations, thus threatening the commission's independence. Critics are also concerned that the commission lacks transparency in its decisions and operations. The lack of transparency surrounding appointments has also raised concern in light of widespread corruption in the political system and the lucrative nature of business in the ICT sector.^[33]

Limits on Content:

The conflict with Russian-backed separatists in eastern Ukraine has driven authorities to censor online content perceived to undermine Ukraine's standing in the conflict. Many Russian online platforms and websites are blocked as the Ukrainian government increasingly proposes legislation that would codify its blocking power into law. Despite the restrictions, the internet remains relatively diverse. Though pro-Russian trolls are active online, locals actively track and expose online manipulation attempts.

Blocking and Filtering

Authorities on both sides of the conflict engage in online censorship beyond the limits of international norms. The Ukrainian government – which rarely blocked content in the past – now prevents access to several Russian-owned platforms and services, as well as websites deemed to contain Russian propaganda, while de facto authorities in LPR and DPR block Ukrainian news sources and other websites.^[34] Over the past two years, the government has been proposing an increasing number of laws that would provide more blocking power, signaling its efforts to further control online information.

Social media platforms VKontakte and Odnoklassniki are blocked, as well as Yandex, the Russian-speaking world's most popular search engine, and mail.ru, a popular email service. ISPs were ordered to block them as part of a national security decree issued by President Petro Poroshenko in May 2017, which imposed sanctions against Russian companies.^[35] President Poroshenko claimed the measures were necessary to protect against cyberattacks and data collection by Russian authorities.^[36] A year later in May 2018, President Poroshenko implemented more sanctions that required ISPs to block 192 websites, including Russian and separatist online media outlets.^[37] Despite the ongoing blockings, Russian social media platforms remain popular due to the availability and increased use of VPNs to circumvent government censorship. Survey data from February 2018 suggested that VKontakte, Odnoklassniki, and Yandex were among the top 10 most popular websites in Ukraine.^[38] Other international platforms such as Facebook and Twitter remain freely available and gained significantly more users following the Revolution of Dignity in 2014 (see Digital Activism).

In July 2017, the Security Service of Ukraine (SBU) stated that it blocked 10 unnamed websites for allegedly spreading anti-Ukrainian propaganda as part of a "hybrid war" against Ukraine.^[39] In December 2017, SBU also reportedly instructed some ISPs to block access to 58 websites for spreading anti-Ukrainian and pro-separatist content.^[40]

The Ministry of Information Policy has also asked the SBU to block websites. In May 2018, the Ministry requested that 21 websites be blocked for a range of reasons, including inciting inter-ethnic enmity and calling for violence.^[41] Another list of 20 websites were provided to the SBU in June 2017 for similar reasons. Many of the websites listed were publishing content sympathetic to de facto authorities in the occupied Donbas region.^[42] Some websites listed by the Ministry have reportedly been blocked by ISPs, although there has been no formal blocking order.^[43] Some copyright-infringing material is also blocked by a cyberpolice unit established in 2015.

The government's ability to block websites still remains largely ungrounded in legislation. However, a number of legislative proposals could codify this ability into law. In July 2017, Ukrainian MPs submitted two bills both addressing national security that contained broad provisions for blocking websites by a range of state officials, including the ability to block websites that threaten security without a court order for a 48-hour period.^[44] If ISPs fail to block the webpages, fines could be imposed. The bills were heavily criticized by local civil society.^[45] In June 2018, after the coverage period of this report, the parliament's Committee on Security and Defense approved one of the bills, registered as #6688, thus putting it up for discussion in the Ukrainian Parliament.^[46] There has been harsh criticism and pressure from local civil society, and activists have remained alert in the face of recurring attempts to push through the bill.^[47]

In February 2018, the NCCIR approved a resolution that identified how ISPs can block webpages and established a technical mechanism for government and law enforcement officials to monitor whether websites were successfully blocked.^[48] The provision was developed by the State Service of Special Communication and Information Protection of Ukraine, which is part of the intelligence services. A joint statement by Ukrainian civil society organizations urged authorities to withdraw

the provision, arguing that it provides too much power to state officials and threatens a free internet.^[49]

In February 2017, decrees on cybersecurity and information security were introduced, which called for the development of legal mechanisms to block, monitor, and remove content deemed threatening to the state.^[50] Also in the spring of 2017, the National Police drafted legislation that would implement the 2011 Budapest Convention on Cybercrimes in domestic Ukrainian law. However, rather than solely addressing computer-related fraud and violations of network security, the bill goes beyond the scope of the convention by including provisions on blocking websites.^[51]

Meanwhile, in May 2015, de facto authorities in the DPR instituted an official blacklist of websites banned on its territory, including Ukrainian news websites,^[52] though the list is not public and it is unclear to what extent DPR officials have been able to enforce it.^[53] De facto authorities in the LPR blocked access to over 100 media websites in May 2015 by pressuring local ISPs to implement censorship orders.^[54]

Content Removal

The Ukrainian government sometimes forces third parties to remove politically sensitive content. The SBU targeted web-hosting company NIC after the company failed to comply with a request to remove five allegedly anti-Ukrainian websites in April 2015. SBU officers subsequently seized hosting servers at four NIC data centers in Kyiv, causing 30,000 unrelated Ukrainian websites to go offline temporarily.^[55] No similar incidents were publicly reported during the period of coverage.

In April 2017, the Ukrainian parliament enacted the law "On State Support of Cinematography in Ukraine" that will require hosting service providers to limit access to webpages containing unauthorized reproductions of certain categories of copyrighted material on the request of the copyright owner, if the webpage has been notified of the infringing content and failed to remove it. The hosting provider can hide the page without a court order, but court approval is required within ten days. Providers risk liability for noncompliance.^[56] The law was intended to support the Ukrainian cinema industry.^[57]

Ukraine's criminal code currently mandates punishments for "unsanctioned actions with information stored on computer devices or networks."^[58] ISPs could be obligated to remove or block the offensive or illegal content within 24 hours.

Media, Diversity, and Content Manipulation

Online media in Ukraine is generally less constrained by economic pressure and owner interests than the mainstream media. The ubiquitous use of social networks, particularly Facebook, by journalists, politicians, and activists facilitates diversity and pluralism online. However, online journalists, commentators, and internet users have been pressured to self-censor, especially on topics related to separatism, terrorism, patriotism, and the Russian-backed insurgency in the east. Self-censorship has been more prevalent in Crimea and the parts of eastern Ukraine occupied by pro-Russian forces, where internet users and journalists have faced attacks,^[59] abuse, and intimidation for expressing pro-Ukrainian positions.

Paid-for commentators and trolls have proliferated online.^[60] Some investigative reports suggest that Ukrainian political actors widely use companies, often officially non-existing, that propose social media management activities, including the whitewashing of political actors or conducting online attacks of opponents and critics. Such activities are usually conducted through networks of

fake accounts and bots. One of the reports, for example, found that a group of Facebook accounts, which had traits common to 'fake' accounts, demonstrated unusually high activity on certain Facebook pages, including pages of the Ministry of Information Policy and other politicians.^[61] Analysis of those accounts' activities showed that they often liked and shared the same content from Facebook users and pages that were not directly connected, which could suggest that the same network of fake accounts is used in multiple online campaigns.

Available evidence suggests that these companies, and the services they provide, are quite diverse, and that a range of both local and national political actors employ these practices.^[62] Much is unknown about the operation of these campaigns, and their impact on public debate and opinion is questioned.

The Ukrainian online information landscape is also subject to manipulation by actors appearing to represent Russian interests. Fabricated or intentionally misleading information presenting Kremlin-friendly narratives is regularly circulated in online news articles targeting Russian-speaking audiences, including Ukrainians. StopFake, a local platform created to debunk fake news and propaganda online, regularly identifies examples of Russian language fake news on topics concerning Ukraine. The articles follow a similar pattern, presenting false information purporting to highlight various failures attributed to the Ukrainian government,^[63] Ukraine's failing relationship with the EU,^[64] as well as false information purporting to highlight Ukrainians' and Crimeans' acceptance of Russia's annexation of Crimea.^[65] The articles often first appear on Russian outlets, including state media outlets, and sometimes reappear on Ukrainian online news websites.^[66]

Kremlin-aligned trolls actively target Ukrainian audiences on social media. In December 2017, the *Washington Post* reported Russia's disinformation efforts to influence Ukrainian citizens prior to the 2014 incursion in Crimea.^[67] A classified report from Russia's intelligence service detailed how Russian actors targeted Facebook and VK with fake accounts purporting to be disappointed with Western-leaning Ukrainians.

Trolls have also been observed posing as enthusiastic Ukrainian patriots in the past few years, attempting to sow distrust within society. Observers noted that the troll accounts operated in intricate networks, and were often highly active in Ukrainian patriot groups on social media, sometimes even acting as page administrators. The trolls used symbolic Ukrainian images in profile pictures, and typically sought to depict the government as failing their citizens, often calling for them to be violently overthrown. Observers have noted that their target audience appears to be patriotic Ukrainians engaged with political affairs.^[68]

More traditional forms of pro-Russian manipulation continue to occur, including mass commenting and paid posts on social media and fake websites.^[69] The Ukrainian Ministry of Information has attempted to respond in kind to the organized Russian information manipulation efforts by creating its own "internet army," but its actions have not received much praise from Ukrainian internet users.^[70]

Digital Activism

The Ukrainian social media sphere, which expanded dramatically following the Revolution of Dignity, continued growing in 2018. Facebook in particular has become a crucial platform for debate about Ukrainian politics, reforms, and civil society. In January 2018, there were 11 million Facebook users in Ukraine, a 67 percent increase from the beginning of 2017.^[71] There was also a notable increase in Instagram users in the country, from 3.6 million in 2016 to 7.3 million by the end of 2017.^[72] However, Russian social networks VKontakte and Odnoklassniki remained

blocked during the reporting period, inhibiting the potential for mobilizing on these popular platforms (see Blocking and Filtering).

Websites and social media platforms have been crucial for providing Ukrainians with up-to-date information on developments in eastern Ukraine. One online platform, LetMyPeopleGo, provides regular information about Ukrainian citizens held captive or being prosecuted by Russian forces. It also campaigns for their release.^[73] A separate social media campaign in March 2017 advocated for the release of Ukrainian university professor Igor Kozlovsky, who was imprisoned in Donetsk on charges of spying and weapons manufacture.^[74] In December 2017, Kozlovsky was released along with 72 other Ukrainian captives during the largest prisoner exchange between Ukraine and DPR and LPR.^[75] In 2015, citizen journalists used open-source tools and data to track the presence of Russian troops and military equipment in Ukraine.^[76]

Social media is also actively used for various online initiatives such as advocating for people with disabilities,^[77] women's rights, and anti-corruption efforts.^[78] Povaha, an online platform launched in 2016, seeks to elevate professional women through online advocacy campaigns and the creation of an online database of Ukrainian women experts. The database is available to local and international media outlets seeking expert input for media segments.^[79] Another online campaign, #ЯНеБоюСказати (I Am Not Afraid To Say It), was made popular in July 2016 by activist Anastasiya Melnychenko after she shared personal stories of sexual harassment and abuse. Thousands of women from Ukraine and Russia mobilized to share similar stories using the hashtag, with the aim of shifting cultural attitudes in countries which often dismiss or blame women for inviting sexual violence.^[80]

Many officials in the Ukrainian government use Facebook and Twitter heavily to report on their actions and reforms. Officials regularly engage with comments in attempts to take into account public opinion, helping to increase accountability.^[81]

Violations of User Rights:

Authorities have cracked down on social media users in attempts to curb anti-Ukrainian rhetoric online, imprisoning users for so-called "separatist" or "extremist" expression. Physical violence remains a concern since the murder of renowned journalist Pavel Sheremet in Kyiv. Cyberattacks, predominantly initiated by foreign agents, have targeted various state agencies, infrastructure, and state registries, with the devastating 'NotPetya' hitting Ukraine in June 2017.

Legal Environment

The right to free speech is granted to all citizens of Ukraine under Article 34 of the constitution, although the state may restrict this right in the interest of national security or public order, and in practice it is frequently violated. Part 3 of Article 15 of the constitution forbids state censorship.

There is no specific law mandating criminal penalties or civil liability for ICT activities, but other laws, such as those penalizing extremist activity, terrorism, or calls to separatism, apply to online activity. Article 109(2)-(3) of the Ukraine Criminal Code outlines jail terms of three to five years for public calls for violent overthrow of constitutional order and seizure of power.^[82] Article 110 of the Criminal Code criminalizes public appeals for the infringement of Ukraine's territorial integrity, including any made online, with maximum penalties of up to five years in prison.

Ukraine's law on State of Emergency contains broad provisions that allow for the introduction of "special rules" concerning the connection and transmission of information through computer

networks during a state of emergency.^[83] It is unclear what this provision could mean in practice, though it is likely to allow for some limitation in access to the internet.

A cyberpolice unit within the Ministry of Interior was created in 2015 as part of a broader police reform that was largely welcomed.^[84] The unit was tasked with battling internet crime, including international money laundering schemes and digital piracy.

As Ukraine remains a target for cyberattacks (see Technical Attacks), a new cybersecurity law was passed in October 2017 and came into effect in May 2018. The law outlines protection for "critical infrastructure" and communication infrastructure the government uses. It also introduces criminal liability for crimes conducted in cyberspace, which was previously not clearly regulated in domestic law.^[85] Additional legislation that will clarify certain measures in the cybersecurity law is expected in the coming years.

Prosecutions and Detentions for Online Activities

Multiple internet users in Ukraine were fined, detained, or sentenced to prison for up to five years in recent years.^[86] Separately, separatist administrations controlling territories in the east sentenced a blogger to 14 years in prison in July 2017.

The Ukrainian authorities punish activity on social media pages and accounts they consider to contain "calls to extremism or separatism" or otherwise threatens the territorial integrity of Ukraine. Since there is no public register for criminal investigations, the exact number of criminal charges for online activity is unclear. One SBU report identified 72 criminal cases, 60 of which led to convictions, between 2015 and 2017 for anti-Ukrainian content on Russian social media platforms.^[87] In October 2017, the SBU reported that in 2017 alone there were approximately 37 convictions from 40 criminal cases against administrators of anti-Ukrainian social media groups and pages.^[88] Another report from *Deutsche Welle* identified over 30 sentences between June 2014 and 2017 by Ukrainian courts for charges relating to online activity that called for violence against the state, such as overthrow of constitutional order.^[89]

- In May 2018, Kyrylo Vychynski, a journalist for Russian state media *RIA Novosti Ukraine*, was detained and charged with treason for "subversive" reporting on Crimea and working with separatist groups.^[90] The SBU pointed to opinion pieces published on *RIA Novosti Ukraine's* webpage as evidence for the charges. The office of *RIA Novosti* was also raided by the SBU (see Media, Diversity, and Content Manipulation).
- In February 2018, the SBU searched the home of a Chernihiv resident for allegedly posting anti-Ukrainian content on Russian social media platforms. Authorities seized his computer and phone, and later charged him under Article 109 of Ukraine's criminal code. According to security services, the man shared content on several groups and pages with over 20,000 followers.^[91]
- In November 2017, a man from the Khmelnytsky region was sentenced to a two-year probation period under part 3 of Article 109 and part 1 of Article 110 of the criminal code. The man posted content on VKontakte calling for the overthrow of the Ukrainian government and for changing Ukrainian borders.^[92]
- In October 2017, a Kyiv man was sentenced to a one year conditional sentence for sharing an article by Aleksandr Dugin, a controversial Russian geopolitical strategist advocating for Russia's assertive imperialist foreign policy, on a VKontakte community page with over 15,000 followers. The post called for territorial disintegration of Ukraine.^[93]

- In August 2017, Zhytomyr-based freelance journalist Vasily Muravitsky was arrested for allegedly committing treason, threatening Ukraine's territory, supporting terrorist groups, and inciting hatred.^[94] The SBU reported that Muravitsky published anti-Ukrainian content on six Russian news websites and was an "information mercenary" for the Russian government. The SBU pointed to his contract with the Russian state news agency Rossiya Segodnya as evidence for the arrest. Muravitsky, who faced a maximum sentence of 15 years in prison, was reportedly released in July 2018 on house arrest.

Authorities in the separatist controlled territories of Donetsk and Luhansk also prosecuted online journalists and bloggers.

- In July 2017, de-facto authorities in LPR sentenced Ukrainian blogger Eduard Nedelyaev, who wrote about daily life in Luhansk, to 14 years in prison for espionage and treason.^[95] He was originally detained in November 2016 and accused of defaming LPR residents, inciting hatred against Russia, and threatening national security by cooperating with Ukrainian security services.^[96]
- In June 2017, DPR's de facto authorities detained Stanyslav Aseyev and reportedly charged him with espionage, which includes a potential 14-year prison sentence.^[97] Aseyev is a local journalist who has contributed to the Ukrainian service of *RFE/RL* under the name Stanyslav Vasin.

Surveillance, Privacy, and Anonymity

There is little information publicly available about surveillance or communication interception. Generally, there is a lack of comprehensive legislative regulation to protect privacy and prevent abuse. The security services can initiate criminal investigations and use wiretapping devices on communications technology, but existing legislation, such as the Law on Operative Investigative Activity,^[98] does not specify the circumstances that justify these measures or the timeframe or scope of their implementation.

In December 2013 the NCCIR released a new edition of "Rules for Activities in the Sphere of Telecommunications," which included a problematic paragraph about ISPs and telecom providers having to "install at their own cost in their telecommunications networks all technical means necessary for performing operative and investigative activities by institutions with powers to do so."^[99] There is no information available on the extent to which these provisions have been implemented.^[100]

From 2002 to 2006, mechanisms for internet monitoring were in place under the State Committee on Communications' Order No. 122, which required ISPs to install so-called "black-box" monitoring systems. This was ostensibly done to monitor the unsanctioned transmission of state secrets. Caving to pressure from public protests and complaints raised by the Internet Association of Ukraine and the Ukrainian Helsinki Human Rights Union, the Ministry of Justice abolished this order in August 2006.

There is currently no obligatory registration for either internet users or prepaid mobile phone subscribers, and users can purchase prepaid SIM-cards anonymously, as well as comment anonymously on websites where the website owner does not require registration. However, in July 2017, the State Service of Special Communication and Information Protection of Ukraine published a draft bill that would require mobile phone subscribers to register and mandate telecom providers to collect data on subscribers.^[101] After its release, the public criticized the bill, and parliament has yet to consider it.

Intimidation and Violence

The ongoing conflict in eastern Ukraine continues to expose online activists and journalists to threats, and political instability has contributed to a tense environment in the country. The National Union of Journalists of Ukraine noted 90 incidents of physical aggression against journalists in 2017, many of whom represented online outlets.^[102]

Ukrainian authorities sometimes intimidate online outlets perceived to be pro-Russian. Between June and August 2017, law enforcement officers and the SBU raided the offices of *Strana* and *Vesti*, two Ukrainian online news outlets with pro-Russian stances. The SBU stated that the searches were part of an investigation into the alleged disclosure of state secrets, though *Strana* denied being involved in such activity. Observers have speculated that the raids were an attempt to pressure and intimidate the outlets. Both websites remain accessible.^[103] In February 2018, chief editor of *Strana* Igor Guzhva reported that he left Ukraine for Austria after receiving death threats and serious intimidation from government officials.^[104] In May 2018, the SBU also raided the office of Russian-state news agency *RIA Novosti* and charged a *Ria Novosti* journalist with treason (see Prosecutions and Detentions for Online Activities).^[105]

In November 2017, journalist Mykhaylo Tkach and his film crew were physically attacked by security guards while working for an investigative program called Schemes, a joint project of *Radio Svoboda (RFE/RL)* and UA:First TV Channel.^[106] The guards worked for Ukrainian politician Viktor Medvedchuk, who is known for his close ties with Russian president Vladimir Putin.

On July 20, 2016, Pavel Sheremet, a veteran Belarusian journalist working for Ukraine's *Ukrayinska Pravda* website, was killed in a car bomb explosion in Kyiv.^[107] Sheremet covered state corruption and the conflict in the east for the website, among other topics; he had endured state pressure and jail time during a career that spanned Belarus, Russia, and Ukraine. Sheremet's colleagues at *Ukrayinska Pravda* believe he was murdered in retribution for his professional activity.^[108] The case remained unsolved in early 2018.

Politically sensitive events such as protests are also particularly dangerous for online journalists and citizens reporting on developments. On March 3, 2018, several journalists were targeted by the police during anti-government protests.^[109] Sergey Nuzhnenko, an *RFE/RL* correspondent, was attacked by police using a gas cartridge while taking photos and videos.^[110]

Journalists reporting on the conflict face retaliation from both Ukrainian nationalist partisan forces and Russian-backed separatists. Both sides used the tactic known as doxing, deliberately publishing the target's personal information to encourage harassment. In August 2016, a group of Ukrainian nationalist activists calling themselves *Myrotvorets* (Peacemaker) updated a public list containing the leaked contact details of thousands of journalists who were accredited to report in the self-proclaimed Donetsk People's Republic,^[111] labelling them as "accomplices of terrorists."^[112] Journalists on the list said the exposure obstructed their efforts to report objectively on the conflict, and several received threats.^[113] The doxing caused widespread consternation among the international media community,^[114] but met with little criticism from Ukrainian officials. Some, including Minister of Internal Affairs Arsen Avakov, applauded the move. Prosecutors in Kyiv investigated the leaks, though no progress was reported, and the list remained available online in early 2018.

Other vulnerable groups have been subject to online abuse. LGBTI (lesbian, gay, bisexual, transgender, or intersex) people have been baited on social media and lured to in-person meetings where they were beaten. The attackers have been known to post video footage of the incidents

online, forcing victims to state their name, address, and other personal details. Entire groups on social media platform VKontakte are devoted to "exposing" LGBTI people. Participants in the groups tend to conflate LGBTI people and pedophiles, justifying the harm they inflict.^[115]

Technical Attacks

Ukrainian business, government websites, and national infrastructure frequently face cyberattacks. In June 2017 the country suffered from a massive cyberattack that affected dozens of state agencies and companies. In June 2018, the Ukrainian government warned of another large-scale attack from Russian hackers.

Ukraine was significantly disrupted by a ransomware attack in June 2017. The malicious software, dubbed NotPetya, encrypted entire hard drives and requested payment in order to restore access.^[116] The virus spread across the country on June 27, the eve of the anniversary of the adoption of Ukraine's constitution, destabilizing telecommunications companies, government ministries, banks, and other vital infrastructure. Radiation-measuring systems at the site of the Chernobyl nuclear disaster were also temporarily inhibited before the attack was contained on June 28.^[117] Observers speculated that the intention of the attack may have been political rather than financial. Ukrainian security services said that the software lacked an effective mechanism for securing ransom funds, indicating that the real purpose was to destroy data and disrupt institutions across Ukraine, a goal they attributed to Russia.^[118] The U.S. Central Intelligence Agency reported to have concluded that Russia was behind the massive cyberattack as well.^[119]

In June 2018, Serhiy Demedyuk, Ukraine's cyber police chief, claimed of another upcoming large-scale cyberattack after learning that Russian hackers were infecting Ukrainian companies with malware to install backdoors.^[120] Those reportedly targeted include banks, energy firms, and other Ukrainian companies. The Russian government has denied any involvement.

Hacker collectives like the pro-Russian Cyber Berkut and the nationalist Ukrainian Cyber Forces continued their activities, including defacing websites and leaking information to discredit their perceived foes. In March 2017, the Ukrainian Cyber Forces claimed that it had taken 173 separatist websites offline in three years, though it remains unclear what methods the group used.^[121]

President Poroshenko had previously accused Russia of running a covert cyberwar against Ukraine. In December 2016, Poroshenko claimed that Russia had launched at least six thousand cyberattacks against Ukrainian state websites in the span of two months.^[122] The websites of the Ministry of Finance and the state Treasury were reportedly among those affected. Ukrainian infrastructure has been consistently targeted by cyberattacks in the past, including the railway service,^[123] the state aviation service,^[124] and state registries.^[125] Poroshenko established a National Cybersecurity Coordination Centre within the National Security and Defense Council to counter external threats in early 2016.^[126]

Notes:

1 "В "ДНР" ввели цензуру в интернете," ["DNR" Introduces Internet Censorship] ZN.ua, May 30, 2015, <http://bit.ly/1PQ7yO3>

2 Tetyana Lokot, "Ukrainian Separatists Block 100+ News Websites in 'Lugansk People's Republic'," *Global Voices*, January 14, 2016. <https://globalvoices.org/2016/01/14/ukrainian-separatists-block-100-news-websites-in-lugansk-peoples-republic/>.

3 <http://khpg.org/en/index.php?id=1501768045>; <http://qha.com.ua/en/society/eight-more-mass-media-to-be-blocked-in-crimea-that-are-absent-on-lists-of-roskomnadzor/143975/>

4 <https://www.zdnet.com/article/notpetya-malware-attack-chaos-but-not-cyber-warfare/>; <https://www.wired.com/story/white-house-russia-notpetya-attribution/>

5 "Укртелеком" Ахметова в ОРЛДО припиняє роботу через захоплення", [Akhmetov's Ukrtelekom stops operating in the occupied territories of Luhansk and Donetsk regions] *Ekonomichna Pravda*, March 1, 2017, <https://www.epravda.com.ua/news/2017/03/1/622149/>.

6 "Д" "Укртелеком" Ахметова в ОРЛДО припиняє роботу через захоплення," ["DNR" completely switched to Russian internet traffic] *Strana.ua*, March 7, 2017, <http://bit.ly/2qM200A>.

7 KIIS, "Укртелеком" Ахметова в ОРЛДО припиняє роботу через захоплення," [Dynamics of internet use in Ukraine: May 2017, press release], <http://www.kiis.com.ua/?lang=ukr&cat=reports&id=705&page=2>

8 Olha Minchenko, "Вже більше половини жителів сіл в Україні користуються інтернетом," [More than a half of rural residents in Ukraine use internet] *Watcher*, January 17, 2018, <http://watcher.com.ua/2018/01/17/vzhe-bilshe-polovyny-zhyteliv-sil-v-ukrayini-korystuyutsya-internetom/>

9 "Користувачі смартфонів є 35% українців - дослідження," (35 per cent of Ukrainians own smartphones – study) *RBC Ukraine*, September 12, 2016, accessed on April 4, 2017, <https://www.rbc.ua/ukr/lnews/polzovatelyami-smartfonov-vlyayutsya-35-ukraintsev-1473682956.html>

10 "В Україні мобільний інтернет один із найгірших у світі - OpenSignal" (In Ukraine, mobile internet one of the worst in the world – OpenSignal) *Hromadske*, August 17, 2016, accessed on April 4, 2017, <https://hromadske.ua/posts/v-ukraini-mobilnyi-internet-odyn-iz-naihirshykh-u-sviti-opensignal>

11 Pavel Krasnomovets, "Lifecell, "Київстар" и Vodafone запустили 3G в Черкассах - одном из последних областных центров без нового стандарт", (Lifecell, Kyivstar and Vodafone launched 3G in Cherkasy – one of the last oblast centers without a new standard) *AIN*, March 16, 2017, <https://ain.ua/2017/03/16/3g-v-cherkassax>

12 Olga Karpenko, "«Київстар», «Vodafone Україна» и lifecell получили лицензии на 4G в диапазоне 2600 МГц," [Kyivstar, Vodafone Ukraine and lifecell received 4G licenses for frequency range 2600 MHz] *AIN*, January 31, 2018, <https://ain.ua/2018/01/31/licenzii-na-4g>

13 "Интернета в Донецке нет? Что предлагают местные операторы «ДНР»," [No internet in Donetsk? What do local "DPR" ISPs offer] *Novosti Donbassa*, October 21, 2017, <https://bit.ly/2Laq2gx>; "Интернета в Донецке нет? Что предлагают местные операторы «ДНР»," [The last thread of connection: how to make calls to the occupied territories of Donbas?] *Donbas Realii*, <https://bit.ly/2zHjVPB>.

14 "Интернета в Донецке нет? Что предлагают местные операторы «ДНР»," [No internet in Donetsk? What do local "DPR" ISPs offer] *Novosti Donbassa*, October 21, 2017, <https://bit.ly/2Laq2gx>.

15 "Интернета в Донецке нет? Что предлагают местные операторы «ДНР»," [Disruptions of internet connection lasting for two days on the territory of the "DPR"] *Strana.ua*, October 10, 2017, <https://strana.ua/news/97850-na-territorii-dnr-uzhe-dvoe-sutok-pereboi-s-internetom.html>

16 "В "ДНР" признали, что Интернет получали из Украины, а теперь вдруг каналы отключили," ["DPR" representatives recognized that received internet from Ukraine, while now the channels were suddenly cut off] *Ostrov*, October 10, 2017, <http://bit.ly/2Fm53Z5>.

17 "В ДНР пропали интернет и мобильная связь", [Internet and mobile connection disrupted in DPR] *Korrespondent*, April 14, 2018, <https://bit.ly/2uzBdrT>.

18 "В ДНР пропали интернет и мобильная связь," [Vodafone connection disrupted in the occupied Donbas] *Liga Biznes*, January 11, 2018, <http://biz.liga.net/ekonomika/telekom/novosti/3723864-v-okkupirovannom-donbasse-propala-svyaz-vodafone.htm>

19 "В ДНР отказ от связи Vodafone назвали "политическим решением",," [DPR representatives said their refusal from Vodafone connection is a 'political decision'] *Korrespondent*, February 23, 2018, <http://bit.ly/2Ia7LP3>.

20 Mikhail Popov, "В ДНР отказ от связи Vodafone назвали "политическим решением",," [Vodafone in "DPR": once again ready to leave?] *Donetskiye Novosti*, June 4, 2018, <https://bit.ly/2uzyiiU>.

21 Jim Cowie, "Syria, Venezuela, Ukraine: Internet Under Fire," *Dyn Research*, February 26, 2014, <http://www.renesys.com/2014/02/internetunderfire/>.

22 National Commission for the State Regulation of Communications and Informatization, <http://nkrzi.gov.ua/index.php?r=site/index&pg=55&language=uk>

23 92.8 percent of shares sold to ESU, a Ukrainian subsidiary of the Austrian company EPIC. See "Укртелеком продан," [Ukrtelecom Sold] *Dengi.Ua*, March 11, 2011, <http://bit.ly/1Vq9ALT>. ESU was acquired by Ukrainian firm System Capital Management in 2013. <http://en.interfax.com.ua/news/economic/404675.html>.

24 "Укртелеком продан," [The court sent the case on Ukrtelecom's reprivatisation for retrial], *Liga Biznes*, July 5, 2018, <https://bit.ly/2NQIQUN>.

25 Serhey Kulesh, "Укртелеком продан," [Ranking of Ukrainian ISPs in 2016: Ukrtelekom, Kyivstar and Volia are leaders by the number of subscribers, Fregat and Lanet – by the general assessment] *ITC.ua*, April 6, 2017, <http://bit.ly/2D8hn9l>

26 Ibid.

27 Olga Karpenko, "В Украине почти 55 млн абонентов мобильной связи,," [Ukraine has almost 55 million mobile subscribers] *AIN*, July 31, 2012, <http://bit.ly/1FKMuIE>.

28 Infocom-SK was founded in 1991 jointly by state-owned Ukrtelecom and Controlware, a German telecommunications company. Infocom, "History," accessed on June 15, 2012, <http://bit.ly/1FIrp1N>.

29 OpenNet Initiative, "Ukraine," <https://opennet.net/research/profiles/ukraine>

30 "В Украине почти 55 млн абонентов мобильной связи,," [Ukrainian mobile operator Intertelekom available in "DPR"] *Novosti Donbassa*, <https://dnews.dn.ua/news/663085>

31 "В Украине почти 55 млн абонентов мобильной связи,," [No internet in Donetsk? What do local "DPR" ISPs offer] *Novosti Donbassa*, October 21, 2017, <https://bit.ly/2Laq2gx>.

[32](#) National Commission on Regulation of Communications and Informatization, accessed on April 5, 2017, <http://bit.ly/1OaChbb>.

[33](#) Stas Yurasov, "В Украине почти 55 млн абонентов мобильной связи,," [A call from the past. The court started restoring members of telecom regulator from Yanukovich's times in their official roles] *Ekonomichna Pravda*, July 22, 2015, <https://bit.ly/2Lc8MuC>.

[34](#) "Д" "В Украине почти 55 млн абонентов мобильной связи,," ["DNR" Introduces Internet Censorship] ZN.ua, May 30, 2015, <http://bit.ly/1PQ7yO3>; Tetyana Lokot, "Ukrainian Separatists Block 100+ News Websites in 'Lugansk People's Republic'," *Global Voices*, January 14, 2016. <https://globalvoices.org/2016/01/14/ukrainian-separatists-block-100-news-websites-in-lugansk-peoples-republic/>; <http://khp.org/en/index.php?id=1501768045>; <http://qha.com.ua/en/society/eight-more-mass-media-to-be-blocked-in-crimea-that-are-absent-on-lists-of-roskomnadzor/143975/>

[35](#) "In new sanctions list, Ukraine blocks Russian social media sites," *Washington Post*, May 16, 2017, <http://wapo.st/2htxHN4>.

[36](#) "In new sanctions list, Ukraine blocks Russian social media sites," *Washington Post*, May 16, 2017, <http://wapo.st/2htxHN4>.

[37](#) "Указом про санкції президент незаконно зобов'язав провайдерів блокувати 192 нових сайти – «Лабораторія цифрової безпеки»,," [President illegally obliged ISPs to block 192 new websites with his decree on sanctions – Laboratory of digital security] *Detector Media*, May 25, 2018, <https://bit.ly/2upjPH4>.

[38](#) "Указом про санкції президент незаконно зобов'язав провайдерів блокувати 192 нових сайти – «Лабораторія цифрової безпеки»,," [Three Russian websites appeared among the most popular ones in Ukraine] *Liga Biznes*, February 15, 2018, <http://bit.ly/2tv4Nl6>

[39](#) Security Service of Ukraine, <https://ssu.gov.ua/ua/news/1/category/2/view/3685#.2veayF96.dpbs>; Net Freedom, "SBU blocks 10 sites for anti-Ukrainian propaganda" July 12, 2017, <http://netfreedom.org.ua/sbu-zablokovano-10-sajtiv-z-antyukrainskoju-propagandoju/>.

[40](#) "З'явився перелік сайтів, до яких СБУ рекомендує провайдерам обмежити доступ. Позасудово," [A list of websites recommended for blocking by SBU published. Without court decisions] *Netfreedom.org.ua*, December 11, 2017, <https://netfreedom.org.ua/zjavyvsia-perelik-sajtiv-do-jakych-sbu-rekomenduje-provajderam-obmezhyty-dostup/>.

[41](#) "З'явився перелік сайтів, до яких СБУ рекомендує провайдерам обмежити доступ. Позасудово," [Ministry of Information Policy proposes banning 21 websites in Ukraine] *Detector Media*, March 12, 2018, <http://bit.ly/2DntT4Y>

[42](#) Ministry for Information Policy, Ukraine, "List of prohibited websites," accessed November 1, 2017, <http://mip.gov.ua/files/pdf/perelik-sajtiv.pdf>.

[43](#) "МІП планує на початку року розширити перелік сайтів, які слід блокувати," [MIP plans to extend the list of websites to be blocked early next year] *Detector Media*, December 29, 2017, <http://bit.ly/2GcQdkL>.

[44](#) <https://medium.com/@cyberlabukraine/legal-analysis-of-the-draft-law-on-amending-certain-laws-of-ukraine-on-counteracting-threats-to-39b3738d97cf>; Maryana Zakusylo, "МІП планує на

початку року розширити перелік сайтів, які слід блокувати," [MPs want to legalize extra-judicial blocking of internet resources] *Detector Media*, July 12, 2017, <http://bit.ly/2oZHVEK>

[45](#) "Медійники вимагають від депутатів не вносити до порядку денного законопроекти щодо обмежень в інтернеті (ДОПОВНЕНО)," [Media professionals urge MPs to not consider bills that contain restrictions in internet (ADDED) *Detector Media*, September 5, 2017, <http://bit.ly/2yqCkON>

[46](#) <https://www.kyivpost.com/ukraine-politics/parliament-committee-okays-bill-critics-say-will-block-websites-end-internet-anonymity.html>;
<https://europeanjournalists.org/blog/2018/07/06/ukraine-draft-bill-to-allow-blocking-of-internet-sites-without-a-court-order/>

[47](#) E.g. <http://khpg.org/index.php?id=1529815121>,
<http://detector.media/infospace/article/139000/2018-07-02-zakonoproekt-6688-mozhe-prizvesti-do-povnogo-pripinennya-diyalnosti-deyakikh-informresursiv-koalitsiya-za-vilnii-internet/>

[48](#) "И грянул гром: власти наконец решили, как блокировать россайты,," [Thunder broke out: the authorities finally decided how they are going to block Russian websites] *Liga Biznes*, February 22, 2018, <http://bit.ly/2p4IBsn>

[49](#) "И грянул гром: власти наконец решили, как блокировать россайты,," [NGOs call instalment of technical equipment for surveillance of ISPs unacceptable] *Net Freedom*, February 27, 2018, <http://netfreedom.org.ua/gromadski-organizatsii-zajavliayut-pro-neprypustymist-vstanovlennia/>

[50](#) Yuliya Zabelina, "И грянул гром: власти наконец решили, как блокировать россайты,," (Fight with unwelcome or Russia: what is behind the information security doctrine) *Detector Media*, March 1, 2017, <http://bit.ly/2nYm9AB>.

[51](#) "Нацполиция предлагает блокировать сайты, ссылаясь на европейские нормы. Что с этим не так," [National Police proposes blocking websites, referring to European norms. Here's what's wrong with that] *AIN*, February 28, 2018, <http://bit.ly/2oZ4sIT>

[52](#) "Нацполиция предлагает блокировать сайты, ссылаясь на европейские нормы. Что с этим не так," ["DNR" fighters block internet websites speaking against terrorism and separatism] *CRiME*, September 30, 2014, <http://crime.in.ua/node/6462>.

[53](#) "Нацполиция предлагает блокировать сайты, ссылаясь на европейские нормы. Что с этим не так," ["DNR" Introduces Internet Censorship] *ZN.ua*, May 30, 2015, <http://bit.ly/1PQ7yO3>.

[54](#) Tetyana Lokot, "Ukrainian Separatists Block 100+ News Websites in 'Lugansk People's Republic'," *Global Voices*, January 14, 2016. <https://globalvoices.org/2016/01/14/ukrainian-separatists-block-100-news-websites-in-lugansk-peoples-republic/>.

[55](#) Anna Poludenko-Young, "Ukraine's Security Service Takes Down 30,000 Websites to Fight 'Pro-Russian Propaganda'," *Global Voices*, April 28, 2015, <http://bit.ly/1M47yqs>.

[56](#) Baker McKenzie, Intermediaries Now Liable for Third Party Online Copyright Infringements in Ukraine, <http://www.bakermckenzie.com/en/insight/publications/2017/05/intermediaries-online-copyright-infringements/>.

[57](#) "Між захистом і цензурою. В Україні регулюють інтернет-піратство досудовим методом," (Between protection and censorship. Internet piracy is to be regulated by pre-court procedure in Ukraine) Net Freedom, April 3, 2017, <http://netfreedom.org.ua/mizh-zakhystom-i-cenzuroju-v-ukrajini/>.

[58](#) Articles 361, 362, 363 of Ukraine's Criminal Code, <http://zakon1.rada.gov.ua/laws/show/2341-14/>, page 11.

[59](#) "Між захистом і цензурою. В Україні регулюють інтернет-піратство досудовим методом," [In Luhansk, separatists kidnap journalist, rob internet website office] *Radio Svoboda*, July 16, 2014, <http://bit.ly/1MKcSSA>.

[60](#) Maria Zhdanova and Dariya Orlova, (2017) Computational Propaganda in Ukraine: Caught Between External Threats and Internal Challenges. *Working Paper*. <http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Comprop-Ukraine.pdf>

[61](#) Gala Skliarevskaya, "Минстеть, Арбузов і Ляшко: что общего у политиков в соцсетях," [Minstets, Arbuzov and Lyashko: what is common for politicians in social networks] *Detector Media*, March 19, 2018, <https://bit.ly/2L1mJvY>.

[62](#) Maria Zhdanova and Dariya Orlova, (2017) Computational Propaganda in Ukraine: Caught Between External Threats and Internal Challenges. *Working Paper*. <http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Comprop-Ukraine.pdf>

[63](#) For example: <http://www.stopfake.org/en/fake-ukraine-to-introduce-food-ration-cards/>

[64](#) For example: <http://www.stopfake.org/en/fake-most-ukrainians-not-interested-in-visa-free-travel-to-eu/>.

[65](#) For example: <http://www.stopfake.org/en/fake-crimea-benefits-economically-from-reunification-with-russia/>.

[66](#) For example: <http://www.stopfake.org/en/fake-most-ukrainians-not-interested-in-visa-free-travel-to-eu/>.

[67](#) Ellen Nakashima, "Inside a Russian disinformation campaign in Ukraine in 2014," *Washington Post*, December 25, 2017. <http://wapo.st/2FzTjHP>

[68](#) "The troll network," *Texty*, October 4, 2016, http://texty.org.ua/d/fb-trolls/index_eng.html.

[69](#) Aric Toler, "Inside the Kremlin Troll Army Machine: Templates, Guidelines, and Paid Posts," *Global Voices*, March 14, 2015, <http://bit.ly/1j3kMNw>; Aric Toler, "Fake 'Ukrainian' News Websites Run by Russian 'Troll Army' Offshoots," *Global Voices*, November 19, 2014, <http://bit.ly/1P7EkfB>.

[70](#) Tetyana Lokot, "Ministry of Truth' Recruits Ukrainians for 'Internet Army,'" *Global Voices*, February 25, 2015, <http://bit.ly/1OJEyua>.

[71](#) Olga Minchenko, "У Facebook вже 11 млн українців," [There are 11 mln Ukrainians on Facebook already] *Watcher*, January 23, 2018, <http://bit.ly/2GbKImp>

[72](#) Olga Minchenko, "У Facebook вже 11 млн українців," [There are 11 mln Ukrainians on Facebook already] *Watcher*, January 23, 2018, <http://bit.ly/2GbKImp>

- [73](#) LetMyPeopleGo, <https://www.facebook.com/LetMyPeopleGoUkraine.en/>. Accessed on August 1, 2016.
- [74](#) "#FreeKozlovskyu. У соцмережі флешмоб із закликом визволити вченого з полону "ДНР", (#FreeKozlovskyu. A flashmob in social media to call for release of scholar from the captivity in "DPR") *Ukrayinska Pravda. Zhyttia*, March 15, 2017, <http://bit.ly/2nrKmlC>; <https://www.hrw.org/news/2016/07/21/they-do-exist>
- [75](#) "UPDATED: Ukraine Holds Prisoner Exchange with Russia-Led Separatists," *Hromadske*, December 27, 2017, <http://bit.ly/2FFnJTd>
- [76](#) Tetyana Bohdanova, "Outing the Russian Military in Eastern Ukraine," *Global Voices*, March 19, 2015, <http://bit.ly/1O5Tp0r>; Aric Toler, "Fact Checking the Conflict in Eastern Ukraine," *Global Voices*, March 3, 2015, <http://bit.ly/1YRnKVo>.
- [77](#) Dostupno.UA, <https://www.facebook.com/ДоступноUA-1617803701799770/>. Accessed on August 1, 2016; "Користувачі соцмереж у різних шкарпетках підтримують людей із синдромом Дауна," (Users of social networks support people with Down syndrome by wearing different socks) *Ukrayinska Pravda. Zhyttia*, March 21, 2017, <http://bit.ly/2nrILfL>.
- [78](#) "У листопаді стартує комунікаційна кампанія #ЯнеДаю проти корупції (ВІДЕО)," [Communication campaign #Idon'tbribe against corruption to be launched in November (VIDEO)] Detector Media, November 6, 2017, <http://bit.ly/2tCqoYN>.
- [79](#) "Women and digital advocacy in post Euromaidan Ukraine," *Global Voices*, January 1, 2016, <https://rising.globalvoices.org/exchange/2016/01/27/women-and-digital-advocacy-in-post-euromaidan-ukraine/>.
- [80](#) Anastasiya Melnychenko, "The woman who wasn't afraid to say it," *Meduza*, July 8, 2016, <https://meduza.io/en/feature/2016/07/08/the-woman-who-wasn-t-afraid-to-say-it>.
- [81](#) "ТОП-50 лідерів думок у соцмережах," [TOP-50 opinion leaders in social media] *Novoe Vremya*, November 17, 2016, <https://magazine.nv.ua/ukr/journal/2597-journal-no-43/geroi-facebook.html>
- [82](#) Criminal Code of Ukraine (2001, Amended 2016), <http://bit.ly/2fzpeqb>.
- [83](#) Legislation of Ukraine, State of Emergency <http://zakon3.rada.gov.ua/laws/show/1550-14>.
- [84](#) Tetyana Lokot, "Watch Out, Internet! Ukraine Is Getting Its Own Cyberpolice," *Global Voices*, October 12, 2015. <https://globalvoices.org/2015/10/12/watch-out-internet-ukraine-is-getting-its-own-cyberpolice/>.
- [85](#) "Кого і як має захистити в Україні закон про кібербезпеку," [Whom and how a new law on cybersecurity will protect in Ukraine] *Deutsche Welle*, October 6, 2017, <http://bit.ly/2tERnTL>; <https://finance.yahoo.com/news/ukraine-adopts-stringent-cybersecurity-law-150027854.html>
- [86](#) Isaac Webb, "Ukrainian Social Media Users Get Five Years in Prison For 'Supporting Separatism'," *Global Voices*, February 7, 2017, <http://bit.ly/2oNREAt>.
- [87](#) "72 criminal proceedings of "anti-Ukraine" propaganda cases registered in 2015-2017", NetFreedom, October 23, 2017, <http://bit.ly/2Inu301>
- [88](#) "Понад 30 власників та адміністраторів антиукраїнських спільнот у соцмережах отримали вирoki суду – СБУ," [More , [More than 30 owners and admins of anti-Ukrainian

communities in social media were sentenced by court – Security Service of Ukraine] *Detector Media*, October 28, 2018, <http://bit.ly/2HoPZq4>

89 "За які пости в інтернеті в Україні можуть засудити," [What kinds of online posts can cause court sentences in Ukraine] *Deutsche Welle*, June 23, 2017, <http://bit.ly/2p5dm1a>

90 <https://rsf.org/en/news/journalist-held-treason-charge-ukraine>;
<https://www.dw.com/en/ukraine-charges-russian-journalist-with-treason/a-43816675>

91 "Проти чернівчанина відкрито справу за адміністрування антиукраїнських пабліків у соцмережах," [A criminal case is launched against a resident of Chernihiv for administering anti-Ukrainian communities in social media] *Detector Media*, February 23, 2018, <http://bit.ly/2paRVfx>

92 "Мешканця Хмельниччини засудили за антиукраїнські заклики в соцмережі," [A resident of Khmelnytsky region sentenced for anti-ukrainian calls in social media] *Ye*, November 23, 2017, <http://bit.ly/2tG1Der>

93 "Мешканця Хмельниччини засудили за антиукраїнські заклики в соцмережі," [The court sentenced a Kyiv resident to one year of conditional period for posting a call for "Novorosiya" secession from Ukraine] *Detector Media*, October 11, 2017, <http://bit.ly/2DmMXQV>

94 CPJ, "Ukrainian journalist in custody on anti-state charges," August 2017, <https://cpj.org/2017/08/ukrainian-journalist-in-custody-on-anti-state-char.php>; RSF "Two more victims in Ukraine's information war," <https://rsf.org/en/news/two-more-victims-information-war-ukraine>.

95 CPJ, "Separatists in east Ukraine 'sentence' blogger to 14 years in captivity," September 2017, <https://cpj.org/2017/09/separatists-in-east-ukraine-sentence-blogger-to-14.php>

96 RSF "Two more victims in Ukraine's information war," <https://rsf.org/en/news/two-more-victims-information-war-ukraine>; "В окупованому Луганську затримали блогера, який відкрито підтримував Україну," (Blogger who openly supported Ukraine was detained in occupied Luhansk) *I12*, November 30, 2016, <http://bit.ly/2pfenld>.

97 CPJ, "Russia-backed separatists holding Ukrainian journalist, accuse him of espionage," July 2017, <https://cpj.org/2017/07/russia-backed-separatists-holding-ukrainian-journalist.php>

98 Law of Ukraine on Operative Investigative Activity, <http://zakon5.rada.gov.ua/laws/show/2135-12>. Accessed on August 1, 2016.

99 NCCI, Rules for Activities in the Sphere of Telecommunications.

100 Oleg Shynkarenko, Зашморг на інтернет, [A Noose on the Internet], *INSIDER*, January 8, 2014, <http://www.theinsider.ua/business/52bac42dd8f4d/>.

101 "Зашморг на інтернет," (Connection by passports. Mobile phone subscribers are expected to be registered) *Liga Biznes*, August 9, 2017, <http://bit.ly/2Hwt5x6>

102 National Union of Journalists of Ukraine, "Зашморг на інтернет," (90 cases of physical aggression against journalists noted in 2017), January 4, 2018, <http://nsju.org/index.php/article/6822>

103 Net Freedom, "New searches of Strana.ua and Vesti," August 11, 2017, <http://netfreedom.org.ua/novi-obshuky-strana-ua-ta-lypnevi-obshuky-vestej-chomu-sylovyky-neefektyvni/>.

104 "Editor flees Ukraine after receiving death threats", Committee to Protect Journalists, February 1, 2018, <https://cpj.org/2018/02/editor-flees-ukraine-after-receiving-death-threats.php>; <https://strana.ua/news/121242-obrashchenie-ihorja-huzhvy-k-chitateljam-internert-hazety-strana.html>

105 "Ukraine charges Russian journalist with treason," *Deutsche Welle*, May 16, 2018, <https://www.dw.com/en/ukraine-charges-russian-journalist-with-treason/a-43816675>.

106 "Охоронці Медведчука скоїли напад на знімальну групу програми «Схеми» біля аеропорту в «Жулянах» – журналіст," (Medvedchuk's security guards attacked a crew of "Schemes" program near airport in Zhulyany – journalist) *Radio Svoboda*, November 7, 2017, <https://www.radiosvoboda.org/a/news-schemes/28840852.html>

107 Christopher Miller, "Prominent Belarusian-Born Journalist Pavel Sheremet Killed In Kyiv Car Blast," *Radio Liberty*, July 20, 2016, <http://www.rferl.org/a/ukraine-journalist-pavel-sheremet-killed-car-bomb/27868777.html>.

108 Alec Luhn, "Car bomb kills pioneering journalist Pavel Sheremet in Kiev," *The Guardian*, July 20, 2016, <https://www.theguardian.com/world/2016/jul/20/ukraine-journalist-pavel-sheremet-killed-kiev-car-bombing>.

109 "ІМІ вимагає негайно розслідувати та покарати силовиків, які атакували журналістів," (IMI demands immediate investigation and punishment for police officers that attacked journalists) *Detector Media*, March 3, 2018, <http://bit.ly/2pcj8xw>

110 "A police officer used a gas cartridge against a journalist from Radio Liberty," *Radio Free Europe/Radio Liberty*, March 3, 2018, <https://www.radiosvoboda.org/a/news/29076340.html>

111 ІМІ вимагає негайно розслідувати та покарати силовиків, які атакували журналістів," ("Myrotvorets" published a new list of journalists), *Detector Media*, August 20, 2016, <http://bit.ly/2phJ7lF>.

112 Aric Toler, Tetyana Lokot, "Ukrainian Activists Leak Personal Information of Thousands of War Reporters in the Donbas," *Global Voices*, May 11, 2016, <https://globalvoices.org/2016/05/11/ukrainian-activists-leak-personal-information-of-thousands-of-war-reporters-in-the-donbas/>.

113 Halya Coynash, "Ukrainian journalist who twice confronted Putin targeted by Myrotvorets Centre vigilantes," *Human Rights in Ukraine*, May 25, 2016, <http://www.khpg.org/en/index.php?id=1464127138>.

114 "Journalists fight back against Ukrainian activists who doxed thousands of war correspondents in the Donbas," *Meduza*, May 11, 2016, <https://meduza.io/en/news/2016/05/11/open-letter-demands-ukrainian-action-over-publication-of-undercover-journalists-information>.

115 « Diversity interrupted: anti-gay crusades mar Ukraine's tolerant façade," *Global Voices*, May 12, 2017, <https://globalvoices.org/2017/05/12/diversity-interrupted-anti-gay-crusades-mar-ukraines-tolerant-facade/>.

116 "Cyber attack hits Ukraine then spreads internationally," June 27, 2016, https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html?mcubz=1&_r=0.

[117](#) "Cyber attacks on Ukrainian government and corporate networks halter," *Ukrinform*, June 28, 2017, <https://www.ukrinform.net/rubric-politics/2255698-cyber-attack-on-ukrainian-government-and-corporate-networks-halted.html>.

[118](#) "Ukraine points finger at Russian security services in recent cyber attack," *Reuters*, July 1, 2017, <https://www.reuters.com/article/us-cyber-attack-ukraine/ukraine-points-finger-at-russian-security-services-in-recent-cyber-attack-idUSKBN19M39P>

[119](#) Ellen Nakashima, "Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes" *Washington Post*, January 12, 2018, <http://wapo.st/2FGXCI8>

[120](#) <https://www.reuters.com/article/us-ukraine-cyber-exclusive/exclusive-ukraine-says-russian-hackers-preparing-massive-strike-idUSKBN1JM225>; <https://www.independent.co.uk/news/world/europe/ukraine-russian-hackers-constitution-day-notpetya-malware-a8418596.html>; <https://www.businessinsider.com/ukraine-cyberattack-russia-notpetya-2018-6>

[121](#) "Українські кібер війська" за три роки заблокували 173 сайти терористів,, (Ukrainian cyber forces blocked 173 websites of terrorists over the course of three years), *Detector Media*, March 10, 2017, <http://bit.ly/2ofBooQ>.

[122](#) "Українські кібер війська" за три роки заблокували 173 сайти терористів,, (Russia launched a cyberwar against Ukraine – Poroshenko), *TSN*, December 29, 2016, <http://bit.ly/2oW7UMJ>.

[123](#) Roman Hankevych, "Мінінфраструктури назвало організаторів хакерської атаки на інформаційну мережу "Укрзалізниці", (Ministry of Infrastructure named organizers of hacking attack on information network of "Ukrzaliznytsia"), *Zaxid.net*, December 15, 2016, <http://bit.ly/2ofS51A>.

[124](#) Yuliya Polikovska, "Мінінфраструктури назвало організаторів хакерської атаки на інформаційну мережу "Укрзалізниці", (Websites of the Ministry of Infrastructure and State Aviation Service do not work), *Zaxid.net*, December 16, 2016, <http://bit.ly/2nvi4GI>.

[125](#) "Мінінфраструктури назвало організаторів хакерської атаки на інформаційну мережу "Укрзалізниці", (None of the DDoS-attacks on state registries was successful and didn't affect the data), *Interfax Ukraine*, February 13, 2017, <http://ua.interfax.com.ua/news/general/402947.html>.

[126](#) Maya Yarovaia, "Мінінфраструктури назвало організаторів хакерської атаки на інформаційну мережу "Укрзалізниці"" [Poroshenko finalizes Ukraine's cybersecurity strategy and creation of coordination center for cybersecurity within NSDC], *AIN*, March 17, 2016, <http://ain.ua/2016/03/17/638654>.

Copyright notice: © Freedom House, Inc. · All Rights Reserved

Search Refworld

by keyword

and / or country

[Advanced Search](#) | [Search Tips](#)

Countries

- [Ukraine](#)

Topics

- [Freedom of expression](#)
- [Freedom of information](#)