Ukraine

Key Developments: June 2015 – May 2016

- Pressure from separatist militants resulted in the temporary blocking of dozens of websites within the eastern regions of the country (see Restrictions on Connectivity).

- Ukrainian authorities clamped down on so-called “separatist” and “extremist” expression online, with many users detained, fined, and even imprisoned for such activities (see Prosecutions and Detentions for Online Activities).

- Ukrainian nationalist hackers leaked the personal information of thousands of journalists working in eastern Ukraine, deliberately compromising their privacy and safety (see Intimidation and Violence).
Editor's Note

On March 16, 2014, Russian military forces presided over an illegal referendum in Crimea to justify Russia's annexation of the territory from Ukraine. On March 27, 2014, the General Assembly of the United Nations issued a non-binding resolution calling the referendum invalid and urging member states and international organizations not to recognize any such change in Crimea's status. As of this report, Ukraine and a vast majority of countries recognize neither the Russian-organized referendum nor Crimea as part of the Russian Federation.

Freedom on the Net focuses on internet freedom developments as they pertain to internet users within each of the 65 countries under study. This report focuses primarily on the overall status of internet freedom in Ukraine from June 2015 through May 2016. Due to the ongoing crises in the region, events in Crimea during this time are generally excluded from this report and do not directly affect the analysis, assessment, or score of internet freedom in Ukraine published here. To the extent that Crimea is mentioned in the report, it is to acknowledge and describe the connection between internet freedom developments in Crimea and those elsewhere in Ukraine. Events in parts of the Donbas that are outside of government control are included in the report and do affect the analysis, assessment, and score of internet freedom in Ukraine.

Introduction

Ukraine's internet freedom declined due to increasing arrests against netizens for expressing "separatist" views on social media, while users in the Donbas region were barred from accessing dozens of blocked sites.

While the online media sphere flourished in the wake of the Euromaidan movement of 2014, the ongoing conflict between Ukrainian forces and Russian-backed separatists in eastern Ukraine has undermined user rights online and fostered an environment of self-censorship. Ukrainian authorities have become less tolerant of online expression perceived as critical of Ukraine's position in the conflict, and the government has been especially active this year in sanctioning social media users for "separatist" and "extremist" activities, with many users detained, fined and even imprisoned for such activities. Meanwhile, separatist forces in the east have stepped up efforts to block content online perceived to be in support of Ukrainian government or cultural identity.

Ukrainian internet users continue to face external threats to their digital security and physical wellbeing. Within the coverage period, key infrastructure in Ukraine, including a power plant, was targeted in a series of debilitating cyberattacks which appear to have originated from within Russia. Meanwhile, Ukrainian nationalists targeted journalists working within the conflict zone, leaking the personal details of thousands of accredited journalists online.

Despite the challenges posed by the ongoing conflict and information war, Ukrainian civil society continues to have an important presence online. Activists use social media to organize and promote ideas such as coordinating volunteer support for the military, aiding efforts to assist internally displaced populations, encouraging oversight of government, as well as exposing instances of biased or manipulative information.
Obstacles to Access

Internet penetration continued to grow in 2015-2016, and access to the internet remains affordable for most of the population. The ICT market is diverse, and state-owned providers no longer dominate the market. Inevitably, Ukraine’s telecommunications market has suffered during the reported period due to economic hardships in the country and the crisis following Russia’s annexation of Crimea and later, the upheaval in eastern Ukraine. Other obstacles to access, such as damage to infrastructure in the eastern region, have obstructed internet and mobile access for parts of the country.

Availability and Ease of Access

Internet penetration in Ukraine continues to grow steadily, due in part to diminishing costs and the increasing ease of access, particularly to mobile internet. According to the International Telecommunication Union (ITU), Ukraine had an internet penetration rate of 49 percent in 2015; compared to 43 percent in 2014, and 41 percent in 2013. At the same time, local research indicates that the share of regular Internet users among Ukrainian adults has reached the 62 percent mark. According to the Pew Research Center, 53 percent of Ukrainian adults accessed the internet at least occasionally or owned a smartphone as of 2015. The Pew Research Center also found that 73 percent of Ukrainian adults who do have access to the internet use it on a daily basis. For fixed-line broadband subscriptions, the penetration rate was approximately 11.8 percent at the end of 2015, while mobile broadband had a penetration rate of 7.5 percent. Meanwhile, according to Akamai, the average broadband connection speed in Ukraine was 11.2 Mbps in the fourth quarter of 2015 (compared to 9.3 Mbps in the fourth quarter of 2014), and access to broadband internet in Ukraine is fairly affordable. A monthly unlimited data plan with a 1 Mbps broadband channel costs UAH 80–120 (US$3.20-4.80), while the average monthly wage in the country was UAH 4,920 (US$196) in March 2016.

The level of infrastructure differs between urban and rural areas, contributing to an urban-rural divide. Most people access the internet from home or work, though many middle- and higher-end cafes and restaurants also provide free Wi-Fi. Access is also common in public libraries, schools, shopping malls and airports. Internet cafes still exist but are gradually losing popularity.

---

According to the World Bank, mobile phone penetration reached 144 percent in 2015. Use of mobile internet is gaining in popularity, with 5.6 million Ukrainians accessing the internet on their smartphones or mobile phones. Cost continues to be the main barrier to higher mobile internet use. In February 2015, mobile operators finally gained access to the military’s share of third-generation (3G) mobile phone frequencies. All three companies started commercial use of the frequencies in the summer of 2015 and 3G mobile internet access is currently priced at 100-150 UAH ($4.50-7) for 2-3 GB of traffic per month.

Restrictions on Connectivity

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. Along with gaining political control, those forces also attempted to disrupt or regulate access to telecommunications. While some disruptions in internet and mobile connectivity were caused by military activity, especially in eastern Ukraine (for example, cell towers or internet cables damaged by explosions), in some cases there was direct pressure on internet service providers (ISPs) from rebel militias and Russian-supported authorities, causing them to take down or block particular services, such as city web cameras in Luhansk, or Ukrainian news websites in Donetsk, and Crimea (see “Blocking and Filtering”). As of May 2015, none of the Ukrainian mobile providers are operating in Crimea.

The backbone connection to the international internet is not centralized, and major ISPs each manage their own channels independently. Ukraine’s backbone internet exchange, UA-IX, allows for traffic exchange and connection to the wider internet for Ukrainian ISPs. Ukraine’s internet infrastructure is diverse, with more than 200 domestic autonomous systems purchasing direct international transit service (out of a total of more than 1,650 domestic autonomous system numbers). 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.

---

11 Oleh Dmytrenko, “5,6 млн українців заходять в інтернет через смартфон або мобільний телефон,” [5.6 million Ukrainians access the internet through a smartphone or mobile phone], Watcher, November 2, 2015, http://watcher.com.ua/2015/11/02/5-6-mln-ukrajintsv-zahodyat-v-internet-cherez-smartfon-abo-mobilnyy-telefon/
ICT Market

The Ukrainian telecommunications market is fairly liberal and undergoing gradual development. The state previously owned 93 percent of the largest telecom company and top-tier ISP, Ukrtelecom, but the company was privatized in March 2011. Though no longer state-owned, Ukrtelecom is still the largest ISP in the country and possesses Ukraine’s primary network, trunk, and zone telecom lines. Other telecommunications providers are dependent on leased lines, since Ukrtelecom owns the majority of the infrastructure, and many alternative providers do not have sufficient 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, Vega, and Datagroup; however, major mobile service providers, like Kyivstar and MTS, also provide broadband internet access. There are about 400 ISPs in Ukraine, according to the National Commission for the State Regulation of Communications and Informatization (NCCIR). 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.

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, all of these companies are privately owned. The three major players in the mobile communications market are Kyivstar (owned by Dutch VimpelCom Ltd.), MTS Ukraine (owned by Russian AFK Sistema) which since October 2016 has been operating under the Vodafone brand as part of a partnership agreement, 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.

There are no obvious restrictions or barriers to entry into the ICT market, but any new business venture, whether an ISP or an internet cafe, 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.

---

24 “Во 2 квартале количество абонентов провайдеров Интернет увеличилось на 6,4%,” [In Second Quarter Number Of Subscribers Of Internet Providers Grew By 6.4%] Delo, July 26, 2007, http://bit.ly/1BA2el4
26 OpenNet Initiative, “Ukraine,” https://opennet.net/research/profiles/ukraine
Regulatory Bodies

The ICT sector is regulated by the National Commission for the State Regulation of Communications and Informatization (NCCIR). Members of the NCCIR are appointed by the president of Ukraine.\(^{28}\) Due to widespread corruption in the political system and the lucrative nature of business in the ICT sector, appointments to the commission have lacked transparency. The NCCIR’s work has often been obstructed by claims of nontransparent decisions and operations. Furthermore, the 2003 Law on Communications does not guarantee the independence of the NCCIR. However, the newly appointed head of the NCCIR has vowed to reform the regulator in 2015, and is working on a bill that will guarantee both the financial independence of the NCCIR and its independence from the executive branch of state power.\(^ {29}\)

Limits on Content

Unlike traditional media, access to online content in government-controlled Ukraine remains largely unaffected by the Russian occupation of Crimea and Russian involvement in the conflict in parts of eastern Ukraine, though dozens of Ukrainian websites have been censored in the rebel controlled Donetsk and Luhansk regions. Furthermore, online discussion forums and social media continued to be impacted by partisan voices from both sides, Russian-paid commenting, and self-censorship out of fear.

Blocking and Filtering

The Ukrainian government does not engage in blocking websites or filtering online content, although separatist authorities in the eastern regions of Donetsk and Luhansk did restrict access to news sites over the coverage period. YouTube, Facebook, Twitter, and blog-hosting services such as WordPress and LiveJournal are freely available and have gained significantly more users since the Euromaidan protests in 2013-2014.\(^ {30}\)

Russian-backed separatist militants in eastern Ukraine have been more proactive in blocking Ukrainian resources, and have cracked down on Ukrainian news websites in Donetsk.\(^ {31}\) In May 2015, the self-proclaimed “Donetsk People’s Republic” followed Russia’s example in instituting an official blacklist of websites banned on its territory, though the list is not public and it is unclear to what extent DPR officials would be able to enforce it.\(^ {32}\) In January 2016, separatist authorities in the neighboring “Luhansk People’s Republic” blocked access to over 100 news and media websites by pressuring local ISPs to implement censorship orders.\(^ {33}\)


Since the start of the crisis in eastern Ukraine, Ukrainian authorities have attempted to pressure ISPs to introduce selective blocking of websites containing “separatist” or “terrorist” content, but ISPs have refused wholesale blocking, and insist that court orders must be provided in each case in order for a website to be blocked or taken down. However, individuals have faced legal repercussions for allegedly sharing alleged calls to “separatism” or “extremism” (see “Prosecutions and Detentions for Online Activities”). In October 2015, with the announcement of a new cyberpolice unit, the Interior Minister Arsen Avakov also announced plans to create a banned websites registry that would register and block websites and webpages containing “forbidden content” such as child pornography, malware, and content that violates copyright.

Content Removal

In April 2015, in an attempt to block five allegedly anti-Ukrainian websites, the Ukrainian Security Service officers seized hosting servers at four data centers in Kyiv of the web-hosting company NIC.ua, also the largest domain registrar in Ukraine. As a result, 30,000 Ukrainian websites that had nothing to do with the targeted websites were also taken offline. It turned out that all but one of the five websites suspected of separatism only used NIC.ua as a registrar, and hosted their content on servers in Russia. The Security Service claimed that it had officially requested that NIC.ua block the targeted websites, but the company did not comply. NIC.ua denied the fact that they received any official requests and noted that it is illegal in Ukraine to block websites based on a scanned request or warrant, and that proper procedure would require original court documents. Within a few weeks, over 90 percent of the websites had been restored.

Ukraine’s criminal code currently mandates punishments for “unsanctioned actions with information stored on computer devices or networks.” In some cases, such laws obligate ISPs to remove or block the offensive or illegal content within 24 hours or, if such content is found to be hosted outside of Ukraine, ISPs would have to limit Ukrainian users’ access to such content, effectively introducing a practice of filtering content.

Media, Diversity, and Content Manipulation

Online media in Ukraine is generally less constrained by economic pressure and owner interests than traditional media, and the ubiquitous use of social networks such as Facebook and VKontakte by journalists, politicians and activists for disseminating opinions and promoting media stories further levels the playing field. However, amid the conflict in eastern Ukraine, online journalists, commentators and internet users have been pressured to self-censor, especially on topics directly related to the Russia-backed insurgency in the east, and on the themes of separatism, terrorism and patriotism. Self-censorship has been more pronounced in the parts of eastern Ukraine occupied by

---

pro-Russian forces and in Crimea, where internet users and journalists have faced attacks,\textsuperscript{38} abuse, and intimidation for their pro-Ukrainian positions. However, the media landscape remains varied, and different viewpoints are readily available to users online, especially on social media.

Journalists continued to experience challenges reporting on the conflict as access to occupied parts of eastern Ukraine remained limited. Online media outlets such as Luhansk’s Realnaya Gazeta,\textsuperscript{39} as well as blogs\textsuperscript{40} and social media accounts\textsuperscript{41} of users living in occupied territories, provided important framing and information about the state of human rights and freedom of speech in eastern Ukraine, with local users often risking their safety to provide up-to-date reports.

Attempts to manipulate the online landscape have mostly been external, emanating from Russia, in the form of mass commenting and paid posts on social media,\textsuperscript{42} as well as fake websites,\textsuperscript{43} and social media groups and networks run by pro-Russian internet users.\textsuperscript{44} The Ukrainian Ministry of Information has attempted to respond in kind to the organized Russian information manipulation efforts by creating its own “internet army,”\textsuperscript{45} but its actions have not received much praise from Ukrainian internet users. Grassroots initiatives to debunk fake news and propaganda from Russia and elsewhere, such as StopFake,\textsuperscript{46} have operated consistently on the Ukrainian internet for the past several years.

A new Ministry of Information Policy was created in December 2014,\textsuperscript{47} which aims to promote information security, regulate information policy, and protect Ukraine in the information war with Russia, including online. Although the concrete regulatory powers of the new ministry remain unclear, media advocates and journalists have branded the department “Orwellian,”\textsuperscript{48} and have expressed concern that the agency will only hinder freedom of speech and set a dangerous precedent in granting the new government a greater measure of control over Ukrainian media.

**Digital Activism**

The Ukrainian social media sphere, which expanded dramatically during the Euromaidan protests, continued to thrive and Facebook and Twitter played host to lively debates about Ukrainian politics,
reforms, and civil society. By the end of 2015, the Facebook audience in Ukraine grew by 30 percent (1.2 million users) and reached 5 million users for the first time. 49

With the annexation of Crimea and the start of the conflict in eastern Ukraine, activists and volunteers mobilized during Euromaidan 50 and found new uses for online platforms and their networks, 51 switching their efforts over to help fundraise for the needs of the military and volunteer battalions, provide information and assistance to refugees, and help to those kidnapped by the pro-Russian militias. Citizen journalists also used open-source tools and data to track the presence of Russian troops 52 and military equipment in Ukraine. 53 More recently, projects such as LetMyPeopleGo 54 have campaigned online for the release of Ukrainian citizens held captive illegally in Russia and annexed Crimea, while activists with a new online initiative Dostupno.UA 55 have used social media to break the pervasive stereotypes about people with disabilities and integrate them into society. Many officials in the new Ukrainian government use Facebook and Twitter heavily to report on their actions and reforms, and regularly engage with comments and take into account public opinion in their work, helping to increase accountability. 56

Social media has also been used to bring taboo topics into public discussion. After the coverage period, in July 2016, Anastasiya Melnychenko launched the hashtag, #яНебоюсьСказати (#IAmNotAfraidToSayIt), sharing stories of the pervasive sexual harassment and abuse she experienced throughout her life. The hashtag was widely shared across social media, with thousands of women from Ukraine and Russia mobilizing to share their own stories, with the aim of shifting cultural attitudes in their countries which often dismiss or blame women for inviting sexual violence. 57

Violations of User Rights

Authorities have increasingly cracked down on social media in an attempt to curb anti-Ukrainian rhetoric online, imprisoning users for so-called “separatist” or “extremist” expression. While physical violence against online commentators has declined overall, a number of troubling instances of violence occurred, including the murder of a renowned independent journalist after the coverage period in July 2016. Furthermore, the security of thousands of journalists was compromised in a leak of a database containing the personal information of accredited journalists reporting in eastern Ukraine. Key infrastructure in Ukraine, including Kiev’s international airport, has also been targeted by cyberattacks initiated by foreign agents.


Legal Environment

The right to free speech is granted to all citizens of Ukraine under Article 34 of the constitution, although the article also specifies that the state may restrict this right in the interest of national security or public order. Part 3 of Article 15 of the constitution forbids state censorship. In practice, however, these rights have been frequently violated. Especially grave violations were observed in occupied parts of eastern Ukraine, where journalists and regular internet users faced attacks, kidnappings and extralegal intimidation for their reporting or for demonstrating pro-Ukrainian views.

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 threats to the territorial integrity and sovereignty of Ukraine.58

In October 2015, Ukrainian authorities announced the creation of a cyberpolice unit within the Ministry of Interior as part of a broader police reform.59 The new unit has been tasked with neutralizing threats in the field of information and communication technologies and battling internet crime, including international money laundering schemes and digital piracy.

Prosecutions and Detentions for Online Activities

In 2015-2016, multiple internet users in Ukraine have been detained,60 fined61 and even imprisoned for up to five years for creating, running and moderating social media pages and accounts that the Ukrainian authorities found contained “calls to extremism or separatism” or otherwise threatened the territorial integrity of Ukraine. For example, a Ukrainian user in Chernihiv was sentenced in March 2016 to five years in prison for disseminating “materials calling for change of Ukrainian territory or state borders” online.62

In May 2016, journalist Ruslan Kotsaba was convicted of obstructing the activities of Ukraine’s armed forces and sentenced to 3 years and 6 months in prison.63 He had been arrested in February 2015 by Ukraine’s Security Service on charges of treason (which were eventually changed) after he posted a YouTube video calling viewers to boycott the military mobilization in Ukraine.64 Kostaba’s arrest sparked heated debates about the balance between information security and freedom of

63 “Коцабу не визнали зрадником, але дали 3,5 року в’язниці” [Kotsaba not pronounced a traitor, but gets 3.5 years in jail], Ukrainska Pravda, May 12, 2016, http://www.pravda.com.ua/news/2016/05/12/7108218/.
speech online during an armed conflict. Kotsaba was released from prison on July 14, 2016, when his conviction was overturned in court, after 18 months in detention.

Surveillance, Privacy, and Anonymity

The pervasiveness and legality of surveillance is unclear as very little information on this is openly available, and there is generally a lack of comprehensive legislative regulation of communication interception and surveillance. The Security Service of Ukraine can initiate criminal investigations and use wiretapping devices on communications, but existing legislation (for example, the Law on Operative Investigative Activity) does not specify the circumstances that justify interception of information from communication channels nor the time limits of any such interception.

A proposal announced in April 2015 by the State Service on Special Communications and Information Security mandates that all mobile phone users, including those using prepaid packages, would have to register and disclose their personal data (such as their passport number) to mobile providers. The committee that is working on the legal framework for the proposal claims it has received pressure from law enforcement to institute the measure, given the terrorist and security threats Ukraine currently faces. So far, only a draft of the proposal has been published on the government website, though it has already caused widespread criticism from the industry and free speech advocates. 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.

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 that would provide access to state institutions. 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. Since the revocation of Order No. 122, the service has acted within the limits prescribed by the Law on Operative Investigative Activity.

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.” Some human rights groups and internet associations were concerned that this step will aid the Security Services and the government in restricting internet freedoms by creating additional means

---

69 NCCI, Rules for Activities in the Sphere of Telecommunications.
of pressure that the government can exert over ISPs, however there is no information available on the extent to which these provisions have been implemented.\textsuperscript{70}

### Intimidation and Violence

The simmering conflict in eastern Ukraine continues to be a source of pressure and threats against online activists and journalists, with a number of troubling instances of violence occurring during the coverage period, and the murder of a renowned independent journalist in July 2016 shocking the media community. Activists, bloggers, and regular internet users are still targeted for their work or pro-Ukrainian views by Russian-backed militants. Ukrainian and international journalists reporting on the conflict have also faced intimidation from Ukrainian nationalist partisan forces.

- Luhansk online journalist and activist Maria Varfolomeeva, who was being held by separatists since January 2015, was released in a prisoner swap with the Ukrainian authorities in March 2016.\textsuperscript{71}

- In January 2016, the car of online investigative reporter Svetlana Kryukova (of Strana.ua website) was smashed and its tires cut in a parking lot near her office.\textsuperscript{72} Kryukova connected the attack to her investigative work on Ukrainian politician Gennady Korban.

- In May 2016, Ukrainian nationalist activist website “Mirotvorets” (Peacemaker) published a leaked list of names and contact details of thousands of journalists who have received accreditation to report in the self-proclaimed “Donetsk People’s Republic,” branding them “accomplices of terrorists.”\textsuperscript{73} The doxing caused widespread consternation among the international media community,\textsuperscript{74} but was met with little criticism among Ukrainian officials, some of whom, including Minister of Internal Affairs Arsen Avakov, applauded the partisan move. Several of the journalists from the list have received threats\textsuperscript{75} and noted that the leak obstructed their efforts to report objectively on the conflict in eastern Ukraine. Kyiv Prosecutor’s Office in Ukraine has opened a criminal investigation into the website’s actions.

- In May 2016, Anatoliy Ostapenko, a journalist affiliated with independent online TV outlet Hromadske Zaporizhzhya, was assaulted in the eastern city of Zaporizhzhya. Ostapenko had reportedly been working on investigations linking local authorities to corruption.\textsuperscript{76}

- On July 20, 2016, Pavel Sheremet, a veteran Belarusian journalist working for Ukraine’s

\textsuperscript{70} Oleg Shynkarenko, Зашморг на інтернет [A Noose on the Internet], INSIDER, January 8, 2014, http://www.theinsider.ua/business/52bac42dd8d4d/.


Ukrainska Pravda website, was killed in a car bomb explosion in the Ukrainian capital Kyiv. Sheremet, who had worked in Belarus, Russia and Ukraine, had previously endured state pressure and jail time for his reporting, which was often critical of political leaders. Although the investigation into his death is still ongoing, Sheremet's colleagues at Ukrainska Pravda believe his murder was retribution for his professional activity.

Technical Attacks

A new wave of cyberattacks in Ukraine signifies the continued battle between pro-Russian and Ukrainian nationalist partisans. Hacker collectives like the pro-Russian “Cyber-Berkut,” and the nationalist “Ukrainian Cyber Forces” continued to deface websites and leak information belonging to their perceived foes.

There were also several hacking attacks on Ukrainian infrastructure, targeting power systems and transportation systems in the country. In December 2015, an attack on a powerplant owned by the electric company Prykarpattyaoblenergo in Ukraine’s western Ivano-Frankivsk region led to a power blackout affecting about 80,000 citizens. Both Ukraine’s state security service and independent Western researchers have blamed Russian hackers for the attack, although it was not clear if the hackers were working at the behest of the Russian government. A January 2016 malware attack targeting the air traffic control system of Kyiv’s main Boryspil airport was also said to have originated from a server within Russia, with connections to the same hacker group.

In March 2016, President Petro Poroshenko established a National Cybersecurity Coordination Centre within the National Security and Defense Council as part of the country’s new cybersecurity strategy shaped by external threats, many of them coming from Russia.

---

81 Мая Яговуя, “Порошенко утвердил стратегию кибербезопасности Украины и создание координационного центра кибербезопасности при СНБО” [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.