accessnow

DIGITAL DICTATORSHIP

AUTHORITARIAN TACTICS AND RESISTANCE IN EASTERN EUROPE AND CENTRAL ASIA

Access Now defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, legal interventions, and convenings such as RightsCon, we fight for human rights in the digital age.

Table of Contents

Acknowledgements

This paper is an Access Now publication, written by Tatsiana Ziniakova from Human Constanta (Belarus), Tetiana Avdieieva from the Centre for Democracy and Rule of Law (Ukraine), Diana Okremova from Media Legal Centre (Kazakhstan), and Anastasiya Zhyrmont and Natalia Krapiva from Access Now.

We would like to thank the Access Now team members who provided support, including Daniel Leufer, Eliška Pírková, Estelle Massé, Felicia Anthonio, Gustaf Bjorksten, Isedua Oribhabor, Javier Pallero, Laura O'Brien, Peter Micek, Raman Jit Singh Chima, Zach Rosson, Rogelio López, Vlad, Leanna Garfield, Sage Cheng, Juliana Castro, Méabh Maguire, and Donna Wentworth.

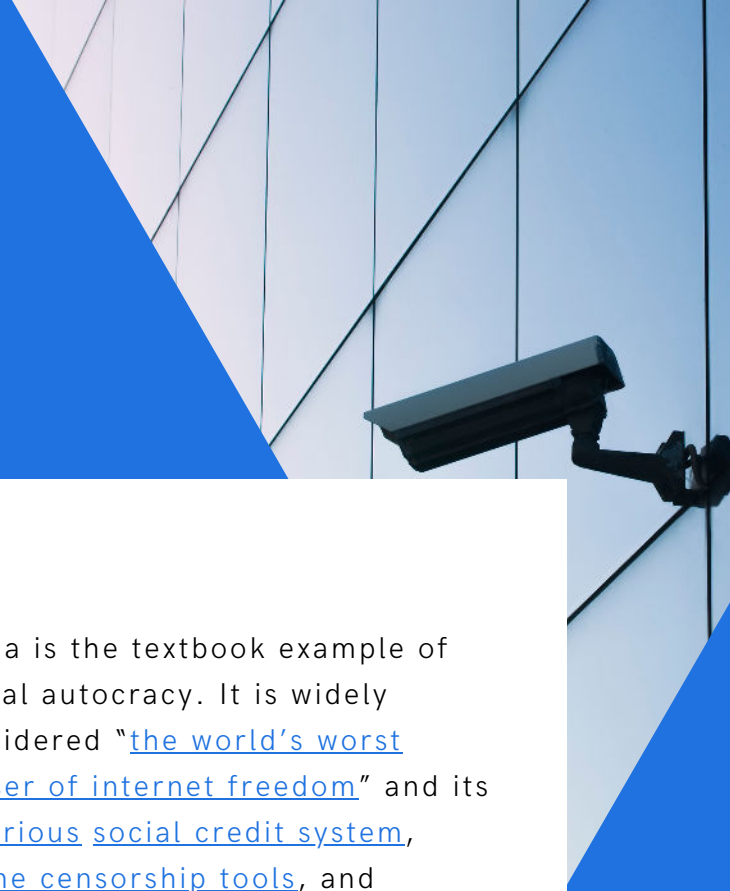
We appreciate the help of all the researchers and activists who provided us with key insights and information for this publication. We look forward to receiving feedback and further input from experts in the field of digital rights, including the rights to freedom of expression, freedom of assembly, and privacy online.

Designed by Ann Marie Carrothers.

October 2022

Digital dictatorship: authoritarian tactics and resistance in Eastern Europe and Central Asia

Note: We began working on this report before Russia's full-scale invasion of Ukraine, which began on February 24, 2022 and continues to claim many innocent lives. Although this report is not focused exclusively on conflict-related aspects of Eastern Europe and Central Asia's digital rights landscape, the trend toward digital authoritarianism is especially dangerous and explosive in wartime, when the aggressor uses any and every excuse to ignore human rights and fundamental freedoms, both online and off. Military aggression and occupation are forms of oppression that heighten the risk of digital authoritarianism. The war in Ukraine is evolving rapidly and Access Now continues to monitor violations of digital rights associated with the war.



Introduction:

DIGITAL AUTHORITARIANISM IN THE EECA REGION

With the rise of digital technology in the late '90s and early 2000s, many believed that the internet could be an unstoppable democratic force — one that would undermine authoritarian regimes across the world. However, despite the positive role technology can play in empowering civil society and toppling dictators, notably during the Arab Spring, the idea that the internet will inevitably bring about "political empowerment" has proved naive, if not utopian. Instead, academic communities and civil society are ringing alarm bells about the rise of digital authoritarianism. The same tools that allow people to self-organize and hold governments accountable are being abused by governments, who fear their people, to repress and suppress democratic dissent.

China is the textbook example of digital autocracy. It is widely considered "the world's worst abuser of internet freedom" and its notorious social credit system, online censorship tools, and omnipresent surveillance technologies do little to reform that reputation. But it is far from being the only country willing to use new technologies to control and repress its own people. Both autocracies and democracies are exploring how they can use technology to advance their interests at the expense of people's freedoms. Artificial intelligence algorithms are used for racial profiling, spyware tools threaten people's privacy, and digital identity programs undermine data protection and enable discrimination. Last year, Freedom House reported that global internet freedom, "the antidote to digital authoritarianism," had consistently declined for 11 consecutive years,

while international media organizations, such as Global Voices, which publishes the Unfreedom Monitor, warn that digital authoritarianism is increasing around the world.

Digital authoritarianism is not a definitive categorization of a country's political systems. It refers rather to a plethora of mechanisms, tools, policies, and specific tech-based solutions, that governments use to exert pressure and exercise pervasive control over people's lives. These tactics and tools increasingly threaten progress toward human rights-centered internet governance, and run counter to governments' obligations to guarantee individuals' right to privacy, freedom of expression, and peaceful assembly. The companies that supply tools to enable human rights violations are likewise failing to meet private-sector obligations as defined in global business and human rights principles.

Both established and aspiring dictators are keen to tighten their grip over people's digital rights.[1] In an examination of the rise of digital authoritarianism,[2] Eastern Europe and Central Asia (EECA) is a region that warrants close inspection. Historically, countries in this region were either part of or were occupied by the Soviet Union, which infringed human rights as a matter of course. The region's nascent democracies are often fragile and vulnerable to malign hybrid influences, while neighboring autocracies are some of the most violent and long-standing in the world. Although EECA states are by no means homogeneous in terms of their development, it's vital that the wider

1. A 2020 *Foreign Affairs* study, The Digital Dictators: How Technology Strengthens Autocracy, found that in a group of 37 dictatorships that lasted more than a year but collapsed between 2000 and 2017 (out of 91 during the same time period), "those that avoided collapse had significantly higher levels of digital repression, on average, than those that fell." It is therefore plausible that regimes wishing to control their populations or to be seen as "competent dictatorships," would seek to accomplish that using both digital and analog means.
2. According to the GSMA Mobile Connectivity Index: 2022, four countries (Belarus, Kazakhstan, Russia, Ukraine) rank as "advanced," five as "transitioner" (Armenia, Azerbaijan, Georgia, Kyrgyzstan, Moldova), and two as "emerging" (Tajikistan and Uzbekistan). (Note: the GSMA index does not includeTurkmenistan.) Freedom House also examined nine out of 12 EECA countries in its Freedom on the Net 2021 Index (it does not cover Moldova, Tajikistan, and Turkmenistan). Among those nine states, only Armenia and Georgia are ranked as "free," while others are characterized as either "partly free" (Kyrgyzstan, Ukraine) or "not free" (Azerbaijan, Belarus, Kazakhstan, Kyrgyzstan, Russia, Uzbekistan). It is no surprise that none of the nine are rule of law champions; according to the World Justice Project Rule of Law 2021 Index, Georgia scores the highest among EECA countries with a dismal 0.61 points, while Russia scores lowest with 0.46.

international community pays attention to their specific needs to prevent set-backs for democratic institutions and processes.

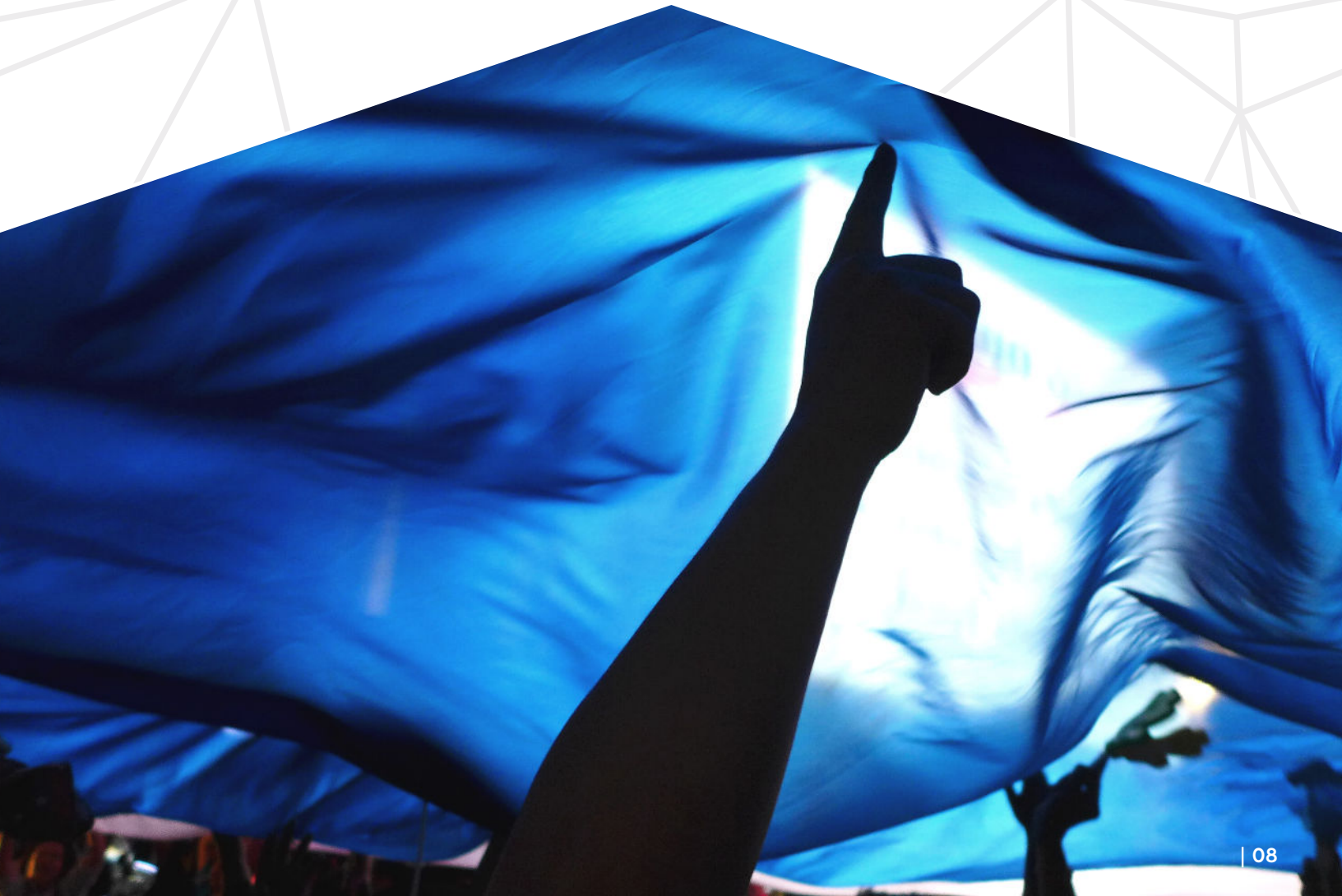
Many of these countries already import surveillance technologies, while others plan to do so. The region is fraught with instability and tension; there are currently both active and frozen conflicts, including between Russia and Ukraine, Russia and Georgia, Russia and Moldova, and Armenia and Azerbaijan. Meanwhile, people in Belarus, Russia, Kazakhstan, and other countries who protest their governments' policies are quickly repressed and silenced. EECA governments consistently cite national security concerns as justification for violating digital rights. To ensure sustainable development and respond to authoritarian abuses of technology, it's vital that we keep a close eye on the evolution of digital freedom in this turbulent region.

How much EECA governments are willing or able to develop, export, and implement digital authoritarianism tools and methods varies widely from country to country. Russia has a comprehensive model that is both comparable to and distinguishable from its Chinese counterpart. Azerbaijan is notorious for using digital surveillance to target regime opponents. Yet democracies such as Ukraine, Georgia, and Moldova seem less inclined to weaponize digital technologies in order to maintain control and power. Other EECA countries are keen to exert tighter control over their populations, but lack the tech-savviness to do so effectively via digital means. Such states do not qualify as current "digital dictators," but should rather be considered aspiring digital dictators, or "wannabees." While they may not yet have reached the same scale or impact of digital authoritarianism as a country like China, their enthusiasm and intent to encroach on digital rights in the future warrants equal attention.

The goal of this report is not to definitively label EECA countries as dictatorships or autocracies, but rather to examine how these countries may be moving farther away from, rather than closer to, democracy — at least in the digital sphere.

We have taken a closer look in particular at how authoritarian tactics deployed online intersect and interact with conventional "offline" repression; what characterizes and

contributes to a country expanding its use of authoritarian digital tools; and which specific technologies are preferred by digital autocrats as a means to establishing and maintaining nondemocratic regimes. Finally, we look at some digital tools and resources that civil society and individuals can use to resist established or aspiring digital dictators.



INSIDE THE TOOLKIT FOR CONTROL

States in the EECA region use a broad range of tactics and technologies — a toolkit — for control. Note: the absence of certain digital repression tools in this infographic does not necessarily indicate they are not used, but we may not have sufficient data on their prevalence.

Online Censorship

Disproportionate restrictions of speech in digital spaces, blocking of independent media and NGO websites, intimidation and coercion of targets to self-censor

Internet Shutdowns

Deliberate network disruption and interference with internet access, blocking of communications platforms

Disinformation and Hate Speech

State-sponsored propaganda and disinformation campaigns, failure to address hate speech online, and/or active participation in inciting hatred against specific targets or communities

Surveillance

Mass and targeted surveillance, including the use of spyware against government critics or other targets, mass collection and retention of personal data, and use of systems for biometric surveillance, such as video cameras and facial recognition technology

COUNTRIES USING THE TOOLS OF CONTROL

Surveillance

Armenia, Azerbaijan, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Russia,Tajikistan, Turkmenistan,Ukraine,* Uzbekistan

Disinformation and Hate Speech

Armenia, Azerbaijan, Belarus, Georgia, Russia, Tajikistan, Uzbekistan

Internet Shutdowns

Azerbaijan, Belarus, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, Turkmenistan, Uzbekistan

Online Censorship

Azerbaijan, Belarus, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, Turkmenistan, Uzbekistan

*The current situation with digital rights in Ukraine cannot be fully assessed according to peacetime metrics. On March 1, 2022, Ukraine notified the United Nations Secretary General of the derogation from some of its human rights obligations, in accordance with Article 4 of the International Covenant on Civil and Political Rights (ICCPR) and Article 15 of The European Convention on Human Rights (ECHR), for the duration of the martial law introduced on February 24. Nothing in this report should be used to justify Russia's illegal aggression against Ukraine.

II. The tools of digital authoritarianism deployed in the EECA region

Digital authoritarianism should be viewed as a toolbox made up of various instruments used to restrict personal freedoms and to constrain society online. These include invasive new technologies, such as artificial intelligence or facial recognition, as well as legislative means of criminalizing online dissent and policy changes that foster intimidation or encourage self-censorship.

EECA countries are not "technological powerhouses." But this does not lessen the threat their efforts pose to democracy, human rights, and civil society voices. Shutting down the internet or spreading disinformation online is often "enough to silence critics and control the narrative," and offline modes of repression are complemented with digital authoritarianism tools.

Some of the most common digital authoritarianism tools include:

1 Internet shutdowns during elections, protests, and in conflict zones

In recent years, internet shutdowns have been a major threat to digital freedoms in the EECA region and beyond. The #KeepItOn coalition, which unites over 280 organizations globally, is tasked with fighting internet shutdowns across the world. The coalition has historically defined an internet shutdown as the "intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information." They may include "blanket" shutdowns (cutting off access entirely), slowing access ("throttling"), and blocking communications platforms such as messaging apps. This is distinct from online censorship, which can include the blocking of sites that are not used primarily for two-way communications, such as independent news sites. In 2021, Access Now and the #KeepItOn coalition documented at least 182 internet shutdowns in 34 countries.

Clément Voule, the United Nations Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association, noted in his report, *Ending Internet shutdowns: a path forward*, that "shutdowns have been observed in long-established democracies and more recent democracies alike, in line with broader trends of democratic recession across the world." The report was based on information gathered and submitted by civil society groups, including members of the #KeepItOn coalition, and it identified six major trends:

- The number of governments imposing internet shutdowns during mass demonstrations continues to grow;
- Shutdowns are increasing in length, scale, and sophistication;
- Bandwidth throttling – or deliberately reducing internet speeds – is becoming increasingly common;
- Most shutdowns target applications and services used by protesters;
- Shutdowns are used as pre-emptive tools against peaceful assemblies, especially in the context of elections; and
- Marginalized and at-risk populations are especially targeted.

The Office of the United Nations High Commissioner for Human Rights also issued a report on the global impact of internet shutdowns in May 2022, based on input from a diverse range of stakeholders. Its findings include:

- "Over the past decade, shutdowns have tended to occur in particular contexts, including during periods of conflict or heightened political tensions, such as the periods surrounding elections or during large-scale protests";
- Shutdowns are implemented with limited transparency – "when implementing shutdowns, governments often fail to acknowledge them or provide minimal or no explanation for the measures, including their legal basis and underlying grounds";
- "When shutdowns are based on legal orders, they generally rely on vaguely formulated laws that offer a large scope of discretion to authorities";
- Shutdowns increasingly impact economic activities – they often "lead to the disruption of financial transactions, commerce, industry, labor markets and the availability of platforms for the delivery of services. Moreover, shutdowns create a climate of uncertainty for investment"; and
- Shutdowns increasingly impact access to education, health and humanitarian assistance – "delays and impediments provoked by shutdowns compromise the effectiveness of health-care and public health policies" and interfere with education planning.

These trends can be widely seen in the EECA region, particularly around elections and during conflicts.

1.1 Shutdowns around elections

Internet shutdowns in Belarus in 2020, extensively documented by the Belarusian Internet Observatory initiative, were widely believed to be a tool of "dissuading protesters from going out into the streets, organizing, and sharing critical information" and one of the key digital authoritarianism tools in the country. On the day of the presidential election in 2020, the government kicked off by blocking YouTube, WhatsApp, Telegram, Viber, Vkontakte, and other social media platforms, as well as Virtual Private Network (VPN) providers, Tor network, and app stores including Google Play. Authorities followed this with a full three-day internet blackout on August 9-11 (the day of the election and two days directly

following). After that, the internet was throttled every Sunday during major protests, adding up to a total of 121 days of internet shutdowns in 2020. Notably, the shutdowns were implemented using deep packet inspection (DPI) equipment purchased from Sandvine, a company with roots in Canada and the United States. Several states stood with the people of Belarus, publishing a joint statement condemning these massive, anti-democratic violations of free expression.

Russia also has a history of shutting down the internet around elections. In 2019, the authorities shut down mobile internet in Moscow during protests over the Russian electoral commission's refusal to register opposition candidates for local elections.

As the #KeepItOn coalition highlights, internet shutdowns make it harder to fully engage in the electoral process. They undermine the ability of candidates, especially opposition candidates, to campaign and exchange ideas. They also prevent voters from accessing election-related information and engaging in political discourse online. Furthermore, they make it much harder for journalists, election observer groups, and other stakeholders to closely monitor the electoral process. All of this undermines the public's trust in the elections and obstructs any effort to document election-related irregularities.

1.2 Shutdowns in conflict zones

EECA governments also use internet shutdowns in the context of armed conflicts. During the 2020 spike in Nagorno-Karabakh conflict, Azerbaijan shut down the internet and demonstrated exactly how life-threatening restricting access to online information and communication flows can be. The Azerbaijani government attempted to justify the shutdown on the pretext of "[preventing] large-scale provocations and cyber incidents committed by the Republic of Armenia," as well as preventing "unwanted, unverified, war-related content on social networks." At the same time, officials confirmed that authorities were "uncertain about the duration of the government-imposed internet limitations," setting a dangerous precedent by being vague about when and for how long they will impose wide, unrestricted shutdowns. Interestingly, Sandvine – the company that provided technology for the Belarusian shutdowns – reportedly supplied the Azerbaijani authorities with similar

equipment. In Russia, during the 2022 full-scale invasion of Ukraine, authorities are imposing social media shutdowns at home, blocking access to Twitter, Facebook, and Instagram, as well as to major VPNs and Tor browser. They are also blocking or otherwise silencing major independent media and human rights organizations. These actions have prevented Russians from accessing accurate information about the war and the associated human rights violations committed in Ukraine and Russia. It has also allowed Russian state war propaganda to flourish unchallenged, including in the Russia-occupied territories. Rerouting internet traffic to Russian networks, blocking YouTube, Viber, and Instagram in the Ukrainian city of Kherson, and deliberately attacking TV and cell towers are all part of Russia's strategy to seize complete informational control. Russia's Sovereign Internet infrastructure, which relies on DPI technologies, makes such shutdowns more effective and targeted than before.

1.3 Shutdowns during protests and social unrest

Beyond these instances, internet shutdowns have a significant impact during protests and other situations of social unrest and political instability. They disrupt activism, journalism, education, health, and business, and disproportionately affect already vulnerable groups, who may not know how to circumvent the restrictions safely.

Russia has a history of throttling mobile internet during protests. Accordingly, between 2018 and 2019, the local government in Ingushetia shut down the mobile internet during peaceful protests against the border agreement with the neighboring Chechnya. Ingush activist Murad Khazbiev challenged the shutdown in court, but the judges sided with the government and declared the shutdowns lawful. Khazbiev is now appealing the court decision at the European Court of Human Rights.

Internet shutdowns in Central Asia – notably in Kazakhstan, Kyrgyzstan, Turkmenistan, Tajikistan, and Uzbekistan – are emblematic of a "persistent trend of … not being afraid to use any means necessary to restrict people's rights to freedom of expression and peaceful assembly online and [offline]." There is evidence that authorities in Tajikistan and Turkmenistan have blocked essential communication services that have become especially important since the COVID-19 pandemic began, such as Zoom, the video-

conference provider.

In January 2022, authorities in Kazakhstan responded to protests by imposing five days of internet blackouts, demonstrating that internet shutdowns are among the tools in its "authoritarian rulebook." The Kazakh Law on Communications allows the General Prosecutor to order an internet shutdown without a court order, if there are calls for people to "participate in unauthorized public gatherings, calls for terrorism, extremism, and mass riots." Reportedly, the scale and impact of the shutdown was unprecedented, as the authorities had to manually hit the kill switch after unsuccessfully trying to force the telecom operators to block the internet with DPI equipment made by Israeli firm Allot. The shutdowns adversely affected the country's residents and its businesses; disruptions in mobile payments services and the functioning of debit card machines caused cash and food shortages.

In Tajikistan, frequent government-ordered internet disruptions in Gorno-Badakhshan impact the proper functioning of the healthcare and education systems, and force the residents to travel to other regions to withdraw or transfer cash and conduct other basic transactions, an expensive undertaking.

Uzbekistan also uses internet shutdowns to suppress protests. After Uzbek President Shavkat Mirziyoyev proposed amendments to the constitution that would curtail the autonomy of the Karakalpakstan republic, which angered the Karakalpak people, the Uzbek authorities responded with internet shutdowns. At first, the authorities implemented mobile internet shutdowns on June 26, 2022, hoping to prevent mass-scale protests. However, internet shutdowns often have the opposite effect, as they are associated with an increase in protests and violence. The government then reacted to the mass-scale protests that erupted on July 1 with a shutdown of fixed-line internet, making it difficult for the Karakalpaks to locate their loved ones amidst state violence, or likewise to find the missing journalists who had been documenting the events. Similar to the situation in Kazakhstan, the shutdowns stopped ATMs and payment services from functioning, putting people at an additional risk.

Internet shutdowns can exacerbate democratic backsliding, which is already a problem in the EECA region. Authoritarian states' ability to easily acquire dual-use filtering equipment from foreign corporate

actors, who typically escape meaningful national or international accountability, is cause for alarm, particularly because it runs counter to the U.N. business and human rights principles that companies must adhere to in order to demonstrate respect for human rights.

2 Beyond shutdowns: online censorship through legislative and other means

A digital dictator need not resort to internet shutdowns to threaten democracy and freedom of expression. Online censorship, whether achieved by blocking independent media and NGO websites or tightening online speech regulations, is a key weapon in the arsenal. It comes in different forms, from government bans on certain content, to labeling organizations "extremist," to placing disproportionate burdens on expressing opinions online, and more.

States that want to control the narrative in order to preserve their power have responded to the ease with which online communications platforms enable people to express themselves and exchange information by cracking down on social media. This pressure on platforms results in a narrowed space for open public dialogue, and it allows authorities to create what is essentially an informational "echo chamber" online to avoid dealing with dissent and criticism.

2.1 Censorship through legislative means (e.g. anti-extremism, national security, "fake news," and child protection laws)

According to Timur Toktonaliev, the Central Asia editor of the Institute for War and Peace Reporting, "most of the methods that are used to regulate the internet in Central Asia are authoritative and promote censorship."

In September 2021, members of the Kazakh parliament proposed amending the Law on the Rights of the Child in order to fight cyberbullying. In particular, parliamentarians suggested mandating that the largest social networks establish representative offices in Kazakhstan or face being blocked. Human rights activists and journalists criticized the amendments

as a move toward censorship, publishing a petition signed by more than 18,000 people. This fortunately led to the government rolling back some of the amendments. However, Kazakhstan's national security laws and decrees still allow the government to block any websites that do not remove "illegal material," including alleged cyberbullying.

In Uzbekistan, changes in the criminal code announced in 2021 criminalize insulting the president online – a rule that is widespread in EECA countries.[3] The definition of an "insult" is left to the discretion of the authorities. Bloggers Otabek Sattoriy and Miraziz Bazarov were each severely punished for speaking critically about public interest issues online: Sattoriy was sentenced to six and a half years in prison and Bazarov was attacked and held under house arrest. These examples of persecution show that authorities in Uzbekistan will not tolerate any unfavorable speech.

Belarus and Russia are among the world's worst offenders when it comes to internet censorship. In Belarus, blocking online resources goes hand-in-hand with labeling such resources and the people who create and distribute them as "extremist." The Belarusian regime deliberately amended its laws and codes to expand the definition of extremism disproportionately, to mandate harsher punishments for spreading "extremist material," and to make it easier to label groups and individuals as "extremist formations." In Russia, anti-extremism laws are also used to criminalize and censor undesirable media outlets, organizations, and platforms; Meta and its two platforms, Facebook and Instagram, have been declared "extremist" and blocked.

Some have suggested that while Central Asian countries may buy repressive technologies from China, they borrow the legal means of digital repression from Russia. The latter's so-called Sovereign Internet project is inspiring governments in the region and around the world to censor the internet and otherwise legislate in authoritarian ways. Russian authorities routinely use extremely vague and overly broad laws to punish and discourage online speech. The country's censorship body,

3. See Criminal Code of Kazakhstan:Article 373 (public insult or other encroachment on the honor and dignity of the first president, desecration of his images), Article 374 (infringement of inviolability of the first president), Article 375 (encroachment on the honor and dignity of the president of the Republic of Kazakhstan and interference with activity of the president); Criminal Code of the Republic of Belarus: Article 368 (insult of the president of the Republic of Belarus); Criminal Code of the Russian Federation: Article 319 (insult of the representative of authority); and Criminal Code of Azerbaijan: Article 323 (defaming or humiliating the honor and dignity of the head of the Azerbaijani state, the president of the Republic of Azerbaijan, in a public speech, publicly displayed work, mass media or on an internet resource by way of mass distribution).

Roskomnadzor, and law enforcement authorites use the foreign agent law, gay propaganda law, undesirable organizations law, terrorist and extremist laws, criminal defamation laws, and legislation combating "fake news" to block, shut down, silence, and prosecute independent media, NGOs, activists, oppositon figures, and social media platforms. The most recent example is Russia's law on false information about the Russian army, which punishes discussion of the war in Ukraine with up to 15 years in jail. Russia also uses the law on proxy avoidance tools to block VPNs and the Tor network.

2.2 Censorship through coercion, intimidation, DDoS attacks, and self-censorship

Taking down or blocking allegedly "undesirable" web content, whether partially or wholly, often lacks a clear legislative basis. Instead, authorities try to prevent individuals or platforms from posting the content in the first place, or if they do post it, encourage them to remove it or make it otherwise inaccessible.

During Russia's 2021 parliamentary elections, authorities used such brute-force methods to coerce Apple and Google to take down the "Smart Voting" app created by associates of opposition leader Alexey Navalny, which was designed to help Russian voters identify candidates not in the ruling party that were most likely to win. Russian agents reportedly threatened Google's local staff with jail unless the company removed the app within 24 hours. The "Smart Voting" website and Telegram were later subjected to Distributed Denial of Service (DDoS) attacks[4] that further limited user access.

Tajikistan authorities, who used DDoS attacks to block two domains of Asia Plus independent media (news.tj and asiaplus.tj) in November 2018, are very familiar with this technique. Despite the attacks, readers were able to access the resources by using VPNs. However, in August 2019, people were once again cut off from the Asia Plus websites through what seems to have been a deliberate domain name misconfiguration. The state body responsible for fixing this kind of error did not respond to requests, suggesting state

4. While this kind of attack is listed as a censorship measure in the present paper, it may also qualify as a form of cyberattack.

authorities were likely behind the change. The apparent attack disrupted traffic to the sites, but may also have been used to intercept and monitor traffic by tricking people trying to reach Asia Plus sites into visiting malicious sites.

Authorities in EECA countries also use coercion to stop people from circumventing censorship, targeting VPNs. In Turkmenistan, authorities demand people swear on the Koran that they will not use VPNs, and ask students to make declarations pledging to use the internet only for "educational purposes."

When there is a lack of clarity about what actions may result in persecution, this increases the likelihood of self-censorship and overcompliance. In July 2021, one of the biggest media outlets in Belarus, Onliner.by, removed the comment function from its website. According to its official statement, this was because "it is challenging even for a professional lawyer to define what is legal and what can be considered as extremism these days."

The inability to post online anonymously also increases self-censorship. Since 2017, Kazakh law obliges websites to require registration for anyone who wishes to leave a comment, verified either by SMS or digital signature. This leaves many people unable to speak out anonymously and therefore unwilling to express themselves publicly.

3 Spreading and encouraging disinformation and hate speech

For many EECA countries, dealing with online disinformation and hate speech is a double-edged sword. On the one hand, it is vital that they regulate dangerously false information in a human rights-compatible way (particularly on important topics, such as health and safety) and take steps to stop war propaganda spreading across online platforms. On the other hand, governments that have legal frameworks to tackle disinformation and dangerous speech may use the same laws to target forms of online expression that are unfavorable to the authorities, while overlooking disinformation or violent content spread by government agents or sources close to the state. Authorities also use emerging technologies to deliver state-sponsored propaganda.

Many autocracies or democracies experiencing democratic backsliding want to control and manipulate the information narrative, and states' and platforms' lack of human rights- and user-centric approaches are part of the problem.

3.1 State-sponsored use of disinformation and propaganda

Manipulating information flows online is different from traditional methods of digital autocracy such as blocking and censoring. In the words of the political science scholar Seva Gunitsky, the latter "rely on suppressing free flows of information" and, therefore, "do not live easily inside democracies." A more subtle method of control, informational flooding, may serve authoritarian purposes even in countries leaning toward democracy. Instead of restricting information flows, flooding facilitates them, but "the information itself is false, distracting, or otherwise worthless." The goal is "not to dominate the informational space but to dilute it."

Azerbahjani authorities commonly use online "trolling" networks to attack outspoken critics, and independent and opposition media, on social media platforms. Pro-government trolls leave hundreds of comments under posts in order to derail discussion and intimidate dissenters.

State-controlled Russian online "bots" and "trolls" plague social media, both inside the country and beyond its borders. During Russia's 2014 invasion of Crimea, the government deployed networks of bots and spam accounts. Today, online spaces are a key battleground for Russian aggression in the ongoing 2022 invasion of Ukraine. Russia reportedly implemented a mass blockade of Ukrainian activists on Facebook, Instagram, and Twitter using "troll factories" to suppress Ukrainian content by submitting spurious takedown requests.

During the 2019 Ukrainian election, Russian authorities had followed a similar approach, manifested in massive bot-attacks, propaganda campaigns, and paid advertisements supporting pro-Russian candidates.

The Kremlin floods the internet with pro-regime propaganda, diverting attention from negative news, and seeding confusion and uncertainty by disseminating alternative narratives about events. In this

way, new technologies make it more efficient to drown out criticism and inflate apparent support for the regime.

As Russia's invasion of Ukraine continues, Russian authorities have only increased their use of online propaganda to manipulate public opinion in Ukraine and to convince Russian audiences that Putin's so-called special military operation is justified, and that civilians have been spared from harm. When it comes to the conflict, the information war between Russia and Ukraine is no less important than the war on the ground.

Russian disinformation is also a serious issue in Central Asia and South Caucasus, as well as in Moldova.

In Central Asia, Russia reportedly uses disinformation campaigns to entrap the media and the public in "digital tribalism" — that is, "when discussion group members or trolls evaluate information not on the basis of compliance with generally accepted standards of evidence or common understanding, but on the basis of whether it supports the values and goals of a given digital tribe and whether this information is confirmed by their leaders."

In Georgia, local observers documented the existence of government-affiliated groups spreading disinformation on social media platforms to influence public opinion. During the June 2019 anti-government demonstrations, activists reported that attackers used bots and sponsored posts to undermine the protests and disseminate pro-government information. In 2021, the Georgian far-right launched a disinformation campaign blaming pro-Western liberals for the death of a TV cameraman targeted in the anti-LGBTQ+ attack at Tbilisi Pride.

A particularly terrifying example of Belarusian online propaganda includes the government release of paid YouTube ads featuring recorded confessions by Roman Protasevich and Sofia Sapega, who were detained by authorities in Belarus after the notorious forced downing of a Ryanair plane in Minsk. The ease with which the government was able to post the ads on the international video platform raised questions about YouTube's ability to stop its platform from being used to spread authoritarian propaganda.

3.2 Failure to address hate speech, or incitement of it

States do wrong not only when they actively spread disinformation, but also when they allow, encourage, or engage in online harassment and the spread of hate speech online, particularly when directed at vulnerable groups such as women or LGBTQ+ individuals.

Azerbaijan is notorious for online harassment of women, frequently targeting women activists, and even women family members of activists, for attacks, including hacking and blackmailing.

Azerbaijani journalist Arzu Geybulla was targeted for online harassment after an opinion article alleged that she had disrespected the martyrs of the conflict between Azerbaijan and Armenia and that she "hated Azerbaijan and its people." Ms. Geybulla was forced to temporarily deactivate her Twitter, Facebook, and Instagram accounts after she started receiving threats.

Russia is infamous for actively encouraging hate speech and violence against women and LGBTQ+ people. After the government passed the so-called gay propoganda law, which imposes fines for exposing children to homosexuality, online and offline violence against LGBTQ+ people was officially legitimized. Russian LGBT Network has documented a rise in homophobic vigilantes and anonymous groups like "Pila" ("Saw") that dox LGBTQ+ individuals online and offer rewards to anyone who "hunts" them like animals. One person on Pila's list, bisexual activist Elena Grigorieva, was killed in 2019.

Russian authorities are extremely reluctant to investigate crimes against LGBTQ+ people. They are more keen to prosecute women and LGBTQ+ individuals for their online activities. Russian authorities filed criminal charges against feminist and LGBTQ+ activist Yulia Tsvetkova, requesting that she serve between two to six years in prison for managing a feminist social media page that encourages people to share body positive, artistic depictions of vulvas. After two years, the Russian court acquitted her.

Online content moderation is necessary to mitigate the risks of content or activity that incites violence and hatred. But it is crucial that such moderation efforts are consistent with human rights obligations. Access

Now's 26 recommendations for content governance that respects human rights guides states and private actors on how to minimize the adverse impact of regulating online forms of expression.

4 Mass and targeted surveillance

Surveillance can be generally divided into two types: targeted and mass. Targeted surveillance usually involves the use of spyware technologies, which specifically target and infect one device or account at a time. Mass surveillance refers to a range of measures aimed at surveilling and exerting control over large sections of the population. In the digital age, such measures may include the use of CCTV cameras and facial recognition technologies, as well as disproportionate and unnecessary mass collection and retention of personal data.

4.1 Video and biometric mass surveillance (e.g. cameras and facial recognition technologies)

Belarus provides a recent and highly concerning example of facial recognition technologies being used for surveillance and political persecution. The E.U., U.K., and the U.S. have sanctioned private company Synesis[5] whose product Kipod is ranked as the ninth most accurate facial recognition algorithm by the U.S. National Institute of Standards and Technology, for providing Belarusian authorities with a surveillance platform reportedly used to repress civil society and democratic opposition members.

Meanwhile, China, notorious for its sophisticated mass surveillance apparatus, is supplying surveillance technology to countries such as Uzbekistan, Kyrgyzstan, and Kazakhstan, often for free. Ostensibly intended to support so-called smart-city infrastructure and to advance public safety, this move suggests that China aims to extend its authoritarian powers in the

5. The company operates under multiple legal entities' names.

region by helping local leaders curtail democracy. The fact that China is focused on supplying this tech primarily to "fragile" states with dubious human rights records is troubling, since this makes it more likely such states will use imported "political illiberalism" to curb human rights.

The Ukrainian government has also deployed surveillance techniques.[6] Peacetime initiatives such as the "Safe city" and "Safe country" projects, which included installing facial recognition-enabled cameras in public places, already posed human rights risks. These risks have grown substantially since Russia's full-scale invasion. Biometric and other sensitive data of vulnerable war-torn populations could now fall into Russian authorities' hands.

Ukrainian government has also used technology from the notorious facial recognition firm Clearview AI, a company that illicitly scraped billions of photos of people to compile its huge database, and is now facing fines or bans in multiple jurisdictions in the U.S., E.U., Australia, and Canada due to data protection and privacy violations. Additionally, in July 2017, the Center Myrotvorets, an organization that studies national security breaches in Ukraine, launched IDentigraF, which uses facial recognition technology to identify individuals from photos and videos. The U.N.'s monitoring mission in Ukraine previously raised concerens about Myrotvorets' publically disclosing journalists and activists' private data and labeling them as terrorists, separatists, or threats to national security. The U.N. mission called on Ukrainian authorities to conduct an investigation and take measures to remove personal data from the website. The launch of IDentigraF has therefore raised fears of further privacy intrusions or its use by the occupying Russian forces.

EECA authorities used the COVID-19 pandemic as another excuse to increase surveillance under the guise of public health interests. Of all such abusers in the region, Russia did so most aggressively. The government repurposed security cameras to track COVID-19 patients' movements and mandated the installation of a monitoring app with access not only to geolocation data, but also the bulk of all host device data. While COVID-19 has had a significant impact in Russia, observers have questioned the balance between

6. The current situation with digital rights in Ukraine cannot be fully assessed according to peacetime metrics. On March 1, 2022, Ukraine notified the United Nations Secretary General of the derogation from some of its human rights obligations, in accordance with Article 4 of the International Covenant on Civil and Political Rights (ICCPR) and Article 15 of The European Convention on Human Rights(ECHR), for the duration of the martial law introduced on February 24. Nothing in this report should be construed to justify Russia's illegal aggression against Ukraine.

protecting public health and restricting rights, given the country's track record of human rights violations and enthusiasm for surveillance technologies.

Russia has only increased its surveillance capabilities since the pandemic began, rolling out a Face Pay system in the Moscow underground that uses facial recognition technology to allow passengers to pay for rides. According to Russian digital rights group Roskomsvoboda, Face Pay is "a dual-use technology, which can be used on the one hand for the convenient use of transport, but on the other hand, for surveillance and capturing people's personal data." A notable example of the latter includes its use by authorities to justify detaining activist Mikhail Shulman for participating in political protests. NTech Lab and VisionLabs are the two leading Russian companies that supply facial recognition technologies to the Russian government.

Data collected through cameras is also at risk of being sold on the black market. Roskomsvoboda has documented cases of CCTV footage being leaked and sold online, with people paying to spy on specific individuals identified by the cameras. Given the limited access to such footage, law enforcement members are the most likely culprits behind the leaks.

4.2 Mass interception and data collection

Facial recognition data is not the only concern in the EECA region, where many states also undertake unwarranted collection and retention of other kinds of data. The European Court of Human Rights has, on numerous occasions, declared Russia's blanket interception of mobile telephone communications, which is common practice, unlawful. Yet the country's Yarovaya law requires companies to store the content of voice calls, data, images, and text messages for six months, and their metadata for three years. Meanwhile, the DPI-based Russian System for Operative-Investigative Activities (SORM) serves as a technical framework for electronic surveillance across Central Asia and Belarus, further harming privacy and free expression in the region.

Kazakhstan has legally enshrined practices countering digital crime, mandating the registration of all mobile network-enabled devices with service providers. This means that the state can access a person's SIM

card information and device IMEI codes, linked with government-issued identification. The practice gives authorities more capacity and opportunity for surveillance, wiretapping, and even disconnecting specific people.

States have also used the COVID-19 pandemic not only as a justification for increased surveillance, but also as an excuse to collect and store sensitive health and other data on a massive scale. Kazakhstan's government has continued to control the internet and limit people's digital rights, subjecting them to active electronic surveillance. For instance, the Smart Astana application, designed to monitor compliance with quarantine and self-isolation requirements, operates using both WiFi geolocation and Bluetooth, while Segrek monitors people's itineraries to confirm that they are only moving between work and home locations, as per COVID-19 restrictions. The personal data collected in this context has often been publicized without prior authorization. For instance, medical data stored in the Ashyq app, which records people's vaccination status, was shared with government agencies, who publicized the names of those violating self-isolation requirements and subjected them to disproportionate public attention and shaming. Meanwhile, in Armenia, local digital security groups have expressed concerns over the COVID-19 contact-tracing app, which collects geolocation and other personal data.

In the context of Russia's invasion of Ukraine, one vulnerability that Russia may exploit is access to Ukranians' data through platforms such as "Diya," which serves as a unified digital identity database of all citizens' available documents, including sensitive medical data and biometrics. There have been multiple allegations of hacks and leaks of information from "Diya," with personal data traded on Telegram channels. Given how, in Afghanistan, the Taliban got access to U.S.-made digital identity systems that could be used to hunt down Afghans who worked with the international coalition, the risks of any such leaks should be taken extremely seriously. The Ukrainian government has reportedly started to move its data and servers abroad while invading forces push deeper into the country.

Access Now warns states against using digital identity systems, which carry inherent digital security, privacy, data

protection, discrimination, and other human rights risks.

4.3 Targeted surveillance and hacking

Governments use targeted surveillance to suppress civil society activism, pursuing "inconvenient" figures, such as activists, opposition figures, and independent media. Tailormade spyware, such as the Israeli firm NSO's Group Pegasus technology, is often used to carry out this form of cyber espionage. Appin Security Group, Circles, Candiru, and Cytrox are other firms known to sell spyware in the EECA region. Spyware can activate a device's microphone and camera, access emails and texts, and track keystrokes.

In 2021, the Pegasus Project investigation, which was led by Forbidden Stories and Amnesty International and involved 80 journalists from 17 media organizations in 10 countries, revealed that dozens of Azerbaijani and Kazakh journalists and activists' phone numbers were on the list of numbers allegedly selected for Pegasus targeting. Amnesty International subsequently confirmed that the phones of at least four Kazakh activists' working for the Oyan, Qazaqstan youth movement were actually infected.

But this was not the first case of state-sponsored malware being spread in the region. In 2016, Kazakhstan reportedly targeted the publishers of the independent newspaper Respublika, as well as family members and attorneys of the co-founder and leader of opposition party Democratic Choice of Kazakhstan – among others – for failing to conform with state-driven policy.

Candiru is another Israeli firm that produces spyware, which has been identified by the Citizen Lab and Microsoft as targeting people in Armenia, among other countries. As of July 2021, 100 human rights defenders, dissidents, journalists, activists, and politicians were confirmed as victims. The Citizen Lab, Meta, and Google have also identified Armenia as a likely user of Cytrox's Predator spyware.

In Uzbekistan, the Canadian non-profit organization eQualitie has uncovered a campaign of phishing attacks targeting independent media and human rights activists. The technique involves creating a website that imitates a well-known online service's login page and encourages users to enter their credentials. Amnesty

International subsequently conducted an investigation into the campaign and discovered that the attackers deployed spyware on Windows and Android operating systems.

Individual activists, opposition members, NGOs, and media organizations in the region are regularly targeted for hacking of their accounts. In Belarus, for instance, authorities "seize" the accounts for opposition Telegram channels and identify the activists behind them, with physical repressions often following suit.

Authorities in Azerbaijan are also known for hacking dissenting activists' Facebook accounts, frequently targeting feminist activists. Ahead of International Women's Day in 2021, a number of women's social media accounts and emails were hacked and their data leaked. The country's Ministry of the Interior and the Ministry of Transportation, Communications, and High Technology (MTCHT) is believed to have been complicit in at least one of these attacks, as the Azerbaijan Internet Watch traced it to their IP addresses. Other targeted groups include human rights lawyers, opposition student activists, and freelance journalists.

Russia also is known for frequently hacking civil society and those critical of the regime. In 2021, Russia infiltrated the United States Agency for International Development (USAID) email system and sent messages to human rights groups, nonprofit organizations, and think tanks, with links to spyware that allowed the Russian government to surveil the recipients' computer networks.

Alarmed by these practices, Access Now and the coalition of over 150 civil society organizations have called on states to implement an immediate moratorium on the sale, transfer, and use of surveillance technology, and to conduct an independent, transparent, and impartial investigation into cases of targeted surveillance and export licenses granted for targeted surveillance technology. Governments should also consider sanctioning the private companies who may assist authorities in the EECA region in violating human rights through the use of such surveillance technologies.

III. Tools to fight digital authoritarianism

States crack down on internet freedoms because they realize that the internet is a powerful tool for self-organization and sharing information. Governments that want to control the narrative and accumulate power feel threatened by the possible use of digital spaces to criticize state policies, access independent sources of information, and find like-minded communities.

If the internet can be used to repress, it can also be used to resist repression.[7] Digital authoritarianism must be met with digital resistance. Independent people-to-people civic tech initiatives are some of the most

7. In her Eurasianet piece "Civic tech activism vs. digital authoritarianism," Barbara von Ow-Freytag characterized the dynamics of the post-Soviet digital landscape as a "game of cat-and-mouse over control of digital technology"; while autocrats seek control in the cyberspace, "activists and opposition movements [are catching up], skillfully and effectively mastering the Internet for their causes." Oxford Internet Institute researcher Aliaksandr Herasimenka, writing for the German Marshall Fund of the United States on the 2020 protests in Belarus, argued that "the increased reliance on digital technologies, as well as the need to address surveillance and censorship, facilitates the emergence of the newer forms of civic organizing and leadership in autocracies." He noted the increased role of "digital dissidents" in recent protest movements in Belarus, Russia, and Ukraine. According to him, the predominantly anonymous and disconnected nature of social media (in particular, of messaging programs and information channels on applications such as Telegram) revolutionized the protest movement, as it allowed prospective activists to connect and interact without a specific leader or formal organizational structure. Andrea Kendall-Taylor, Erica Frantz, and Joseph Wright wrote in Foreign Affairs, "Just as today's autocracies have evolved to embrace new tools, so, too, must democracies develop new ideas, new approaches, and the leadership to ensure that the promise of technology in the twenty-first century does not become a curse."

powerful tools for such resistance.

In Belarus, people shared tools and resources for resistance before, during, and after the 2020 presidential election. Collaborative civic tech projects made it possible for people to safely and effectively exercise the human rights denied to them by the state. Belarusians used online initiatives to verify and count votes, document crimes committed by election commissions and law enforcement authorities, provide assistance to political prisoners, share ways of monitoring and circumventing shutdowns, and discuss new forms of protest.

The instruments to fight digital autocracy go beyond grassroots digital activism. Since digital forms of repression are always complemented by conventional ones, they must be addressed as a multi-faceted issue. Whether people's human rights are being violated online or off, citizens should be able to hold the perpetrators accountable and demand state policy changes and the revocation of repressive laws.

While we demand systematic change and advocate for global pressure on digital dictators, self-help measures remain essential for civil society to combat digital authoritarianism tactics, build resilience, and mitigate cyber threats. As this report demonstrates, activists in the EECA region need access to technical means to protect themselves, as well as to prevent future censorship.We urge governments, tech companies, nonprofits, and funders to expand their support programs and provide civil society with free and secure VPNs, antivirus programs, encryption tools, DDoS protection, and other essential technology, equipment, and services, as well as to invest in further developing these products.

Below you can find some basic tips to increase your digital safety and resilience. However, it is important to understand that digital security is highly contextual, for individuals and groups, and there are no one-size-fits-all solutions. If you are an activist, human rights defender, journalist, or part of a civil society organization, and you are at heightened risk and need emergency assistance, or advice tailored to your specific needs and context, reach out to Access Now's Digital Security Helpline.

Tips and tools for resistance:

Use a virtual private network (VPN) for censorship circumvention and for more secure browsing

A VPN is a service that allows you to connect to the internet via an encrypted tunnel. When accessing the internet through a VPN service, your IP address and online activities are hidden from your Internet Service Provider (ISP) or a malicious actor trying to track you, such as an attacker monitoring connections to a public WiFi hotspot. A VPN can help you circumvent the blocking of websites or online platforms, including specific services such as social media platforms and instant messaging apps. Be mindful: not all VPNs can guarantee your privacy or offer you the same level of protection. When choosing a VPN provider, opt for open source tools with publicly accessible codes and transparency on how they protect your data. Read this guide (English | Russian) from the Electronic Frontier Foundation (EFF) to determine which VPNs would be the best in your case.

Activate two-factor authentication (2FA) for your online accounts

2FA is an essential tool for securing online accounts. As the name suggests, it protects your account via two factors of authentication: a first factor that you know, such as a password, and a second factor, which can be a physical USB security key, a one-time token generated by an authentication app, or another method. This infographic lists the pros and cons of different two-factor methods.

Encrypt your device with full-disk encryption

This kind of full-disk encryption makes data stored on your mobile and computer devices available only if you enter a decryption key. This prevents others from getting unauthorized access to your data through physical possession of your device (e.g. upon detention, confiscation, temporary seizure of your device, or theft). Microsoft's Windows operating system is equipped with BitLocker encryption, which is unfortunately only available on devices operating on the Professional or Enterprise versions of Windows 10. Any edition of Windows 11 has encryption. People with Mac OS devices can use the FileVault encryption technology built into the operating system.

Ensure you remove your data securely

Secure data removal can help you permanently erase your data and make it impossible to retrieve. A safer way to delete data is to use software that ensures the seemingly empty space is overwritten with something else. Secure deletion tool BleachBit can be installed on Windows, while Mac OS devices come with a preinstalled tool.

Stay with secure instant messaging apps

Such apps keep communications between you and your contacts private by using end-to-end encryption technology to protect their content and metadata. One free, secure messenger application, which is compatible with all mainstream operating systems, is Signal. Another option is Wire, which does not require a phone number to use. Like Signal, it provides secure messaging by default, and also allows you to enable additional security features, such as disappearing messages and two-factor authentication.

Use privacy-enhanced browsers

Privacy-enhanced browsers enable you to stay hidden from data-sniffers online and to circumvent censorship. They allow you to visit websites through encrypted connection only, to conduct private searches without storing your search history, to block ads, and to activate advanced privacy-enhancing options. Many commonly used browsers, such as Google Chrome, are known for leaking personal data and lacking privacy protection. More trustworthy browsers include Firefox Focus (the privacy-enhanced version), Tor Browser, Brave, the DuckDuckGo browser on its mobile app, Bromite, and Onion Browser, the Tor Project browser for iOS.

Protect your website from DDoS and other attacks

Cloudflare's Project Galileo provides free cyber security protection to organizations working in the arts, human rights, civil society, journalism, or democracy that are the targets of DDoS and other cyber attacks. Deflect, a website security service built and operated by eQualitie, is another good option.

Use antivirus protection

For people using devices with Windows operating systems, Windows Defender comes pre-installed. For those using Macs, MalwareBytes, Avira, and AVG are good choices.

Resources for resistance:

Fighting internet shutdowns

Advocacy initiatives like the #KeepItOn coalition, and network disruption monitoring tools are essential for anticipating, documenting, and tracking internet shutdowns in the EECA region and globally. The OONI Explorer is an open data resource on internet censorship around the world. The Internet Outage and Detection Analysis (IODA) project and Google's traffic and disruption tracker provide near-real time data to identify internet outages on various networks. These tools enable risk calculation and harm mitigation.

Getting direct digital safety assistance

The Access Now Digital Security Helpline is a free, 24/7 service for journalists, activists, human rights defenders, and civil society groups at risk around the world, offering advice for improving your digital security and emergency assistance when you need it. The Helpline offers assistance in 11 languages, including Russian, Tajik, and Ukrainian, and you can expect a response to your inquiry within two hours.

Reducing risk and protecting your community

The Digital First Aid Toolkit is a free resource to help rapid responders, digital security trainers, and tech-savvy activists to protect themselves and the communities they support against the most common types of digital emergencies and risks. It is also useful for activists, human rights defenders, bloggers, journalists, or media activists who want to learn more about how to protect themselves and others.

Learning the basics of digital safety

The Consumer Reports Security Planner is a free tool that provides recommendations on how to safely back up files, browse online without being tracked, avoid hacking and phishing, and prevent identity theft.

Developing a plan to stay safe

EFF's Surveillance Self-Defense is an essential collection of guides providing you with step-by-step action plans to stay safe from electronic surveillance in different scenarios (e.g. when setting a password, removing data, using a VPN, etc.).

Getting assistance in your language

The Cyber Beaver service shares Russian and Belarusian-language instructions for protecting digital accounts and devices and provides real-time digital security assistance to journalists, bloggers, and activists. It is accessible via a Telegram channel and Telegram chatbot.

Understanding digital security in Ukraine

Digital Security Lab Ukraine equips like-minded activists with knowledge of digital security and internet freedoms. It advocates for the rights to online freedom of expression and privacy, carries out digital audits, and delivers expert advice.

Using technology for positive change

Teplitsa. Technologies for Social Good is a Russian-language public education project aimed at increasing cooperation between the non-profit sector and IT specialists, and strengthening civil society through the smart use of technology.

IV Conclusions and recommendations

As long as digital authoritarianism remains a threat to human rights and democracy in the EECA region, the world must work together to keep a spotlight on the issue and combat digital repression.

Recommendations for international foundations, donors, and development agencies

- Support and coordinate efforts to monitor and raise awareness of the persistent trend toward digital authoritarianism in the EECA region;
- Provide funding, technical support, and capacity-building opportunities to actors engaged in combating digital authoritarianism; and
- Create and leverage existing partnerships and diversely represented coalitions to initiate campaigns and coordinate advocacy on combating digital authoritarianism (including sanctions, judicial and quasi-judicial proceedings, and forensic investigations).

Recommendations for states

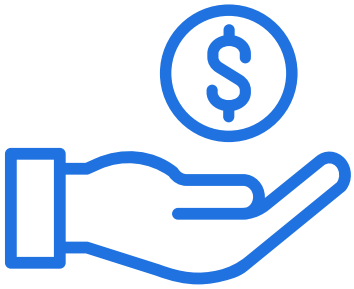
- Commit to protecting and meaningfully implementing human rights obligations and to advancing norms, under a shared vision of how to govern and regulate in the digital age while fulfilling human rights obligations;
- Enact relevant national reforms aimed at dismantling legal, executive, and judicial frameworks that allow digital authoritarianism to flourish;
- Cooperate and consult meaningfully with civil society and private actors to diligently address the threats of digital authoritarianism and shrinking civic space;
- Remove barriers to civil society accessing resources, including travel visas, corporate registration, and financial or banking accounts and capabilities; and
- Follow the recent recommendations of U.N. Special Procedures, including the Special Rapporteur on the right to freedom of peaceful assembly and of association, including ensuring that all associations, whether registered or unregistered, can fully enjoy their right to seek, receive, and use funding or other resources from natural and legal persons, whether domestic, foreign, or international, without prior authorization or other undue impediment

Recommendations for businesses and private entities

- Cease to provide tools, financing, or services to actors in the EECA region with a history of human rights violations;

- Commit to fulfilling business and human rights obligations under the United Nations Guiding Principles on Business and Human Rights and the Organization for Economic Co-operation and Development Guidelines for Multinational Enterprises;
- Map the value chain for exposure to business activities in the region, adopt policies and practices that promote human rights-centered business environments, and identify, assess, and address the heightened human rights risks inherent in the region.
  This should include:

1. Conducting human rights impact assessments before exit or entry into markets in the region, and ongoing human rights due diligence to identify and address risks arising from business operations in the region;
2. Releasing regular transparency reports on government demands for user data or requests to restrict or block services and user accounts; and
3. Engaging in remedial actions, including legal advocacy, and navigating state sanctions and other restrictions with a human rights-based approach, in close collaboration with civil society.



Recommendations for investors

- Conduct ongoing, enhanced human rights due diligence and check for any direct equity or fixed-income investments in the region to understand potential direct or indirect risks occurring through investment;
- If you do identify any companies in your portfolio which may directly or indirectly cause or contribute to a human rights violation through their operations, engage with their executive management directly to confirm that they understand and acknowledge the risks, and that they are taking steps to mitigate these;
- Consider excluding companies that are unwilling or unable to mitigate their exposure to human rights harms from your portfolio; and

- Engage with civil society and human rights organizations to learn more about specific risks, including those related to unintended harms, posed by your portfolio companies.

Recommendations for civil society

- Insofar as it is safe to do so, individually and collectively pressure state and non-state actors who resort to digital authoritarianism tools or facilitate their use; and
- Conduct educational, analytical, and advocacy activities to raise awareness of the persistent trend toward digital authoritarianism in the EECA region.

Useful sources

- Sebastian Hellmeier, The Dictator's Digital Toolkit: Explaining Variation in Internet Filtering in Authoritarian Regimes Politics and Policy, 44-6, December 2016, pp. 1158-1191
- Richard Fontaine, Kara Frederick, The Autocrat's New Tool Kit: The next generation of repressive technology will make past efforts to spread propaganda and quash dissent look primitive, The Wall Street Journal, March 2019
- Andrea Kendall-Taylor, Erica Frantz, Joseph Wright, The Digital Dictators. How Technology Strengthens Autocracy, CNAS, February 2020
- Erica Frantz, Andrea Kendall-Taylor, Joseph Wright, Digital Repression in Autocracies, V-Dem Institute, 2020:27, March 2020
- Erica Frantz, Andrea Kendall-Taylor, A dictator's toolkit: Understanding how co-optation affects repression in autocracies, Journal of Peace Research, 51-3, March 2014, pp. 332-346
- Eda Keremoğlu, Nils B. Weidmann, How Dictators Control the Internet: A Review Essay, Comparative Political Studies, 53 (10-11), March 2020, pp. 1690-1703
- Marie Lamensch, Authoritarianism Has Been Reinvented for the Digital Age. Surveillance and propaganda have always been central to the autocratic playbook. Digital technologies have made repression and control much more pervasive, efficient and subtle, CIGI, July 2021
- Sergei Guriev, Daniel Treisman, How Modern Dictators Survive: An Informational Theory of the New Authoritarianism, November 2015
- Erica Frantz, The Tools of Dictatorship. How artificial intelligence is benefiting current and potential autocrats, December 2020

Contact

For questions and more information, please contact:

Anastasiya Zhyrmont
Campaigner, Eastern Europe & Central Asia, Access Now
anastasiya@accessnow.org

Natalia Krapiva, Esq.
Tech-Legal Counsel, Access Now
natalia@accessnow.org

accessnow

Digital Dictatorship

Authoritarian tactics and resistance in Eastern Europe and Central Asia