

Russia's Tech Authoritarianism on the Occupied Territories of Ukraine



JUNE 25, 2026

**Briefing of the
Commission on Security and Cooperation in Europe**

Washington: 2026

Commission on Security and Cooperation in Europe
234 Ford House Office Building
Washington, DC 20515
202-225-1901
csce@mail.house.gov
<http://www.csce.gov>
@HelsinkiComm

Legislative Branch Commissioners

SENATE

ROGER F. WICKER, MISSISSIPPI *Chairman*
SHELDON WHITEHOUSE, RHODE ISLAND
Ranking Member
JOHN BOOZMAN, ARKANSAS
KATIE BRITT, ALABAMA
JOHN FETTERMAN, PENNSYLVANIA
RUBEN GALLEG0, ARIZONA
MIKE ROUNDS, SOUTH DAKOTA
JEANNE SHAHEEN, NEW HAMPSHIRE
THOM TILLIS, NORTH CAROLINA

HOUSE

JOE WILSON, SOUTH CAROLINA
Co-Chairman
STEVE COHEN, TENNESSEE *Ranking Member*
ROBERT ADERHOLT, ALABAMA
EMANUEL CLEAVER, MISSOURI
LLOYD DOGETT, TEXAS
JAKE ELLZEY, TEXAS
RICHARD HUDSON, NORTH CAROLINA
GREG MURPHY, NORTH CAROLINA
MARC VEASEY, TEXAS

Executive Branch Commissioners

DEPARTMENT OF STATE, *to be appointed*
DEPARTMENT OF DEFENSE, *to be appointed*
DEPARTMENT OF COMMERCE, *to be appointed*

ABOUT THE ORGANIZATION FOR SECURITY AND COOPERATION IN EUROPE

The Helsinki process, formally titled the Conference on Security and Cooperation in Europe, traces its origin to the signing of the Helsinki Final Act in Finland on August 1, 1975, by the leaders of 33 European countries, the United States and Canada. As of January 1, 1995, the Helsinki process was renamed the Organization for Security and Cooperation in Europe [OSCE].

The membership of the OSCE has expanded to 57 participating States, reflecting the breakup of the Soviet Union, Czechoslovakia, and Yugoslavia.

The OSCE Secretariat is in Vienna, Austria, where weekly meetings of the participating States' permanent representatives are held. In addition, specialized seminars and meetings are convened in various locations. Periodic consultations are held among Senior Officials, Ministers and Heads of State or Government.

Although the OSCE continues to engage in standard setting in the fields of military security, economic and environmental cooperation, and human rights and humanitarian concerns, the Organization is primarily focused on initiatives designed to prevent, manage and resolve conflict within and among the participating States. The Organization deploys numerous missions and field activities located in Southeastern and Eastern Europe, the Caucasus, and Central Asia. The website of the OSCE is: <www.osce.org>.

ABOUT THE COMMISSION ON SECURITY AND COOPERATION IN EUROPE

The Commission on Security and Cooperation in Europe, also known as the Helsinki Commission, is an independent U.S. Government commission created in 1976 to monitor and encourage compliance by the participating States with their OSCE commitments, with a particular emphasis on human rights.

The Commission consists of nine members from the United States Senate, nine members from the House of Representatives, and one member each from the Departments of State, Defense and Commerce. The positions of Chair and Co-Chair rotate between the Senate and House every two years, when a new Congress convenes. A professional staff assists the Commissioners in their work.

In fulfilling its mandate, the Commission gathers and disseminates relevant information to the U.S. Congress and the public by convening hearings, issuing reports that reflect the views of Members of the Commission and/or its staff, and providing details about the activities of the Helsinki process and developments in OSCE participating States.

The Commission also contributes to the formulation and execution of U.S. policy regarding the OSCE, including through Member and staff participation on U.S. Delegations to OSCE meetings. Members of the Commission have regular contact with parliamentarians, government officials, representatives of non-governmental organizations, and private individuals from participating States. The website of the Commission is: <www.csce.gov>.

Russia’s Tech Authoritarianism on the Occupied Territories of Ukraine

JUNE 25, 2026

Page

COMMISSION STAFF PRESENT

Alanna Novetsky, Communications Director, Commission for Security and Cooperation in Europe	1
---	---

PARTICIPANTS

Iryna Adam, Research Associate, the Atlantic Council’s Digital Forensic Research Lab	2
Maksym Beznosiuk, Analyst, the Jamestown Foundation, and Associate Fellow, GLOBSEC	4
Steven Feldstein, Senior Fellow, Carnegie Endowment for International Peace	6

Russia's Tech Authoritarianism on the Occupied Territories of Ukraine

June 25, 2026

Commission on Security and Cooperation in Europe Washington, DC

The briefing was held from 2 p.m. to 2:56 p.m., Room 50, Dirksen Senate Office Building, Alanna Novetsky, Communications Director, Commission for Security and Cooperation in Europe, presiding.

Ms. NOVETSKY: Good afternoon. My name is Alanna Novetsky, and I am the communications director at the U.S. Helsinki Commission. I am pleased to welcome you to this briefing, Russia's Tech Authoritarianism on the Occupied Territories of Ukraine.

Recently, I was talking with a colleague who runs an organization that helps people, especially minors, learn about ways to escape the occupied territories and then access the resources needed to do so. She told me a story about being on the phone with a 17-year-old boy who lives in eastern Ukraine and was considering leaving to go to government-controlled Ukraine. At 17, his formative years of schooling had been learning a Russian curriculum, but he maintained his Ukrainian identity and tried to learn Ukrainian in secret.

He knew that every passing day, it became more likely that he would receive a Russian draft notice. He told my colleague that he was worried about moving to government-controlled Ukraine, though, because he did not think that they would sell him bread. What do you mean, she responded. Why would they not sell you bread? He said, well, I have been practicing my Ukrainian, but it is not perfect, and they told us that in Ukraine, if you speak Russian, they will not sell you bread.

I think this story is instructive for two reasons. First, we are about to discuss how Russia has developed a truly impressive, comprehensive tech-enabled repressive apparatus in the occupied territories over the past 14 years. It is also true that Russia has capabilities that allow it to monitor and punish Ukrainians on the individual level. Yet, there are still many people, even those who have never experienced the freedom of living in government-controlled Ukraine, who are holding out hope, trying to escape, or resisting in ways big and small.

On the other hand, as Russia's war drags on and the occupation of eastern Ukraine and Crimea deepens, the likelihood that Ukrainians on the occupied territories will seek out outside information and understand that there is an alternative to Russian oppression

shrinks. Russia's reeducation and propaganda efforts are so advanced that even this boy, who has taught himself Ukrainian and sought out information about how to leave, was worried about not being able to buy bread in Ukraine. Had things gone differently, the same boy may well have become a soldier in the Russian army, sent to the front lines, and commanded to take up arms against his country.

It sometimes seems difficult for Americans to understand the urgency Ukrainians feel about defeating Russia fully, liberating the occupied territories, and ensuring that Russia is unable to fight further wars. However, as we will hear from this esteemed panel of experts over the next hour, the situation on the occupied territories is not static. Russia is getting better and better at quashing opposition and reengineering the Ukrainians under its rule in service of its genocidal war. If we act—and, if we act before it is too late, there are steps that we can take to support Ukrainians, like the 17-year-old boy—who wish to see their country whole, their people free, and their region at peace.

First, we will hear from Iryna Adam, who will give us an overview of how Russia's capabilities have evolved over the past decade and a half. Iryna is a research associate at the Atlantic Council's Digital Forensic Research Lab. She has years of experience working on information warfare, including at the Center for Strategic Communications and Information Security under the Ministry of Culture and Information Policy of Ukraine.

Next, we will hear from Maksym Beznosiuk, an analyst at the Jamestown Foundation and associate fellow at GLOBSEC. Maksym is a strategic policy specialist and prolific researcher and writer on all things Russian military, European security, and hybrid warfare. Maksym will zoom in further on how Russia has combined violence and digital isolation in its efforts to control the Ukrainian population under its rule.

Last, but certainly not least, we will hear from Steven Feldstein, a senior fellow at the Carnegie Endowment for International Peace in the Democracy, Conflict, and Governance Program. Steve is an expert on tech authoritarianism and digital technology's impact on war, and has looked at these challenges from both inside and out of government, including as a deputy assistant secretary in the Democracy, Human Rights, and Labor Bureau of the Department of State. He is the author of "The Rise of Digital Oppression: How Technology Is Reshaping Power, Politics, and Resistance," and the forthcoming book "Bytes and Bullets: Global Rivalry, Private Tech, and the Shape of Modern Warfare." He will take us through the strategic implications of Russia's growing tech authoritarian apparatus and perhaps give us a sense of what we can do about it.

Iryna.

Ms. ADAM: One of the key dangers of Russia's war against Ukraine, and their current approach to war, is their integration of physical strikes alongside territory annexation and attacks in the information environment, followed with control over information on temporarily occupied territories of Ukraine, or the TOT. Not so long ago, President Putin signed a decree outlining Russia's national policy strategies through 2036, which is built around the idea of Russia existing as this kind of State of civilization. One of the main goals is very ambitious. By 2036, the Kremlin wants over 95 percent of its population to self-identify as Russian.

This poses a kind of problem for them, specifically on Ukraine's TOT, as to achieve that they need to launch massive propaganda programs in Crimea, Donetsk, Luhansk, Zaporizhzhia, and Kherson, which are all essentially designed to erase the said Ukrainian

identity and establish the identity as a Russian. One of their first and most fundamental tools in this is the information blockade. We now have reports of Russian authorities checking residents' phones in temporarily occupied territories, blocking internet access, or completely limiting access to Ukrainian and Western media outlets.

Internet access being frequently cutoff, especially when it comes to access to Ukrainian and Western media outlets, creates a kind of gap that needs to be filled. It is usually filled in by Russia's own information ecosystem. Since 2023, Russian-controlled Telegram channels, television channels, radio stations, and news websites have been operating nonstop in the occupied territories. They are broadcasting messages that include aggressive disinformation narratives, including a lot of anti-Ukrainian narratives, glorify the Russian war effort, and also glorify the alleged rebuilding. Residents were even given free connections to a package of television channels called *Russkiy Mir*, or "The Russian World," which is a very good name for kind of ideology that these channels promote.

It is blocking the information. Russia is also actively flooding the information space with their own narratives and messages. Last year, in our joint investigation with our Ukrainian partner, OpenMinds, we discovered over 3,600 Telegram channels that have sent over 300,000 comments on Telegram between January 2024 and April 2025, which were specifically targeting Ukrainian populations in the TOT, with some of the individual channels posting as many as 1,300 comments in a day. Which amounts to a kind of comment every 36 seconds, indicating bot activity. These bots crafted tailored messages for occupied territory audiences, differentiating their content from the ones aimed at audiences inside Ukraine and Russia.

Their comments fell into kind of three broad categories: Very pro-Russian, very pro-Ukrainian, and the kind of more neutral ones, which were just generically calling for peace but were also trying to allege that Russia is the reasonable party in this conflict. Pro-Russian propaganda was promoted twice as often on temporarily occupied territories by these channels than in any other kind of audience that they have been active in. They were not promoting pro-Russian narratives quite as often within kind of communities that were aimed more at Ukrainian and Russian audiences directly.

Their themes ranged from praise of local infrastructure repairs and Russian social services to very active attacks against President Zelensky specifically, who appeared in nearly one in six bot comments, making him the most frequently mentioned individual in the comments in general. A high volume of comments which are expressing a specific viewpoint can create the impression that it represents the majority opinion in the community. Considering the lack of internet access, the lack of ability to communicate with each other and also with other kinds of cities and towns, both in the TOT and in the liberated Ukraine, this can create a very disorienting narrative for the audiences within the TOT.

Even more so, this can create the illusion of the agreement and of the acceptance of the Russian occupation for audiences inside Russia and abroad in general, in Ukraine or in the West, kind of creating an evidentiary basis for Russia's occupation. The information war is also evolving in ways that extend well beyond Ukraine's borders, with Russia now developing a new state-controlled super app called Max that could lead to further entrenchment of digital authoritarianism. Max is part of the Kremlin's border effort to replace foreign digital platforms with Russia's own centralized domestic ecosystem for communications, public services, and everyday online activity. It is part-mentioned—it is in part developed and based on China's own WeChat.

As of last year, Max is required to come preinstalled on new phones sold in Russia. The authorities have also now ordered banks to stop using Telegram and WhatsApp in favor of Max, pushing universities, schools, and public agencies to do the same. For people in TOT, this is a direct threat, as Russian occupation authorities have increasingly pushed residents of occupied Ukrainian territories into Russian identification, economic, and telecom systems, with Max coming as kind of the next layer of that integration. Once the residents are dependent economically and administratively on Russian digital infrastructure specifically, opting out becomes harder, if at all possible.

The surveillance implications of this app are also serious, both for the TOT as well as Western audiences, with Max collecting user data, including IP addresses, behavioral metrics, and any kind of contact information, and its privacy policy openly stating that data may be shared with third parties and State agencies. Which can potentially include Russia's surveillance apparatus and, directly, its FSB's SORM interception system. The strategic importance in such data is that it can be abused by an authoritarian system. It can help map diaspora communities outside of Russia, track activists inside and outside of Russia within the TOT. It can help monitor cross-border relationships, which is especially pertinent for the TOT, and also enable transnational repression.

Russia is not just targeting occupants of residents of occupied territories anymore. It is running English-language information operations aimed at Western audiences using platforms connected to the Russian Foreign Ministry. Now Moscow has also announced that Max will become available through telecom operators across 40 countries in Latin America, Asia, Africa, the Middle East, and Eastern Europe, significantly expanding Russia's potential digital reach. What is happening in occupied Ukraine is a structured, multi-layered system, understanding of which is essential both for supporting Ukraine as well as for defending the broader security of information systems across the board.

Thank you.

Ms. NOVETSKY: Thank you, Iryna.

Maksym.

Mr. BEZNOSIUK: Okay. Good afternoon. Thanks for the invitation. It is an honor to join this discussion today.

The situation in occupied Ukraine remains deeply concerning. Russia increasingly relies on the comprehensive occupation system designed to permanently integrate occupied territories into the Russian State, erase Ukrainian identity, and suppress any form of resistance. For approximately five million Ukrainians living under Russian occupation, there is a constant struggle for survival on a daily basis.

Residents face routine document checks, surveillance, phone inspections, filtration procedures, and the constant risk of detention for perceived disloyalty. The conditions I have just described did not emerge overnight. Since 1922, Russia has gradually transformed military occupation into a comprehensive system of governance designed to make its control permanent. Russia has pursued this objective through several mutually reinforcing mechanisms rather than through one linear process.

First, Russia has pursued the objective of reproducing the Russian State inside of occupied Ukraine by establishing key institutions there. It has replicated much of its Federal administrative architecture across the occupied territories, seeking their full legal, economic, political, and administrative integration into Russia. In 1925, Russia also finalized the integration of the occupied regional administrations into a Federal digital moni-

toring platform, the Governor's Dashboard. This allows the Kremlin to monitor budgets, personal performance, construction projects, and administrative compliance in real time, placing occupied territories under the same performance metrics and digital oversight mechanisms as those used in Russia.

Second, since 1922, Russia has also isolated occupied territories from the Ukrainian information space, promoted Russian-controlled applications and information channels, and tightened control over communications and online activity. Third, the Kremlin has expanded coercive passportization measures, linking access to basic services, employment, and property rights to Russian citizenship, while also increasingly using citizenship status to facilitate military registration and mobilization in occupied territories.

Fourth, Moscow has also focused on the systematic erasure of Ukrainian identity across education, media, culture, and public life, while simultaneously replacing it with Russian ideology, culture, language, and historical pro-Russian narratives. Russia banned the Ukrainian language in schools, removed Ukrainian books, and hindered access to Ukrainian remote education opportunities. Moscow has also imposed militarized education programs, youth organizations such as Yunarmiya, Voin, Movement of the First, and increasingly used cultural institutions, patriotic websites, and digital platforms to reinforce pro-Russia historical narratives and cultivate hostility not just toward Ukraine, but toward United States and overall West.

Fifth, the Kremlin has also increasingly focused on demographic engineering. While Ukrainians have faced forced mobilization, property confiscations, and employment challenges, Moscow has offered high salaries, subsidized mortgages, and relocation incentives to Russian teachers, doctors, cultural workers, and other specialists willing to move into occupied areas. Sixth, the Kremlin has also developed an extractive and militarized economic model, combining resource extraction with the systematic reorientation of local industry toward Russia's defense industrial base.

Occupational authorities have increasingly combined violence with technological tools that serve as an effective force multiplier and enabler for deepening the residents' dependence on occupation institutions and further entrenching their control. The occupation authorities have implemented a preventive threat elimination approach, assuming basic civilian disloyalty and treating every passive dissent as a potential security threat. Digital surveillance has been increasingly used alongside policing, including checkpoints and filtration procedures. This also includes monitoring communications, the Russian-controlled Max super app, mandatory biometric SIM registration, CCTV cameras, and efforts to identify any used unregistered phones by the local population.

Phones are routinely searched at checkpoints and during unannounced home raids. Processing Ukrainian media content, following Ukrainian news or pro-Ukrainian Telegram channels, or even having a VPN installed, can lead to detention, torture, disappearance, or transfer to filtration sites or prisons. Between 1922 and 1925, around 15,000 people were detained, although the number might be significantly higher as of today. Also, passportization illustrates how technology and coercion go hand-in-hand. Residents were pressured to accept Russian citizenship because basic services, employment, communications, and property rights increasingly depended on it. Once inside the system, they became more visible to Russian administrative data bases, military registration systems, and other mechanisms of State control.

To conclude, Russia's occupation system is designed to make Russian rule permanent. It does so through administrative coercion and integration, passportization, indoctrination,

surveillance, and demographic engineering, with technology serving as a force multiplier and enabler, making control more efficient and future integration with Ukraine virtually impossible.

Thank you. I look forward to the discussion.

Mr. FELDSTEIN: Great. Thank you so much. Well, I want to thank the Helsinki Commission for organizing this important briefing. I appreciate the invitation to participate.

What I would like to do, to complement what we have heard so far, is to present a bit of context and a broader overview about the evolution of Russia's digital controls, and how that is now currently being applied in the context of the Ukrainian occupied territories, I think an important aspect is that, first of all, many, if not all, the tactics that are being employed in the occupied territories borrow from Russia's repression playbook being used at home. What we have seen is a gradual evolution over time when it comes to increasing constraints within Russia's own information ecosystem.

In other words, what we are looking at in Russia, as compared to another authoritarian State like China, is not something that has been uniformly repressive over a one- or two-decade period. Instead, what we have seen is intensification. That intensification has been linked to the centralization of authority by Russia's President Vladimir Putin. As Putin has closed down and cracked down politically in the country, we have also seen a commensurate clamping down when it comes to information controls, when it comes to platform bans, when it comes to the imposition of surveillance.

You know, in many respects, I think an interesting kind of point of comparison with China is that you both see increasing levels, if not consistent levels, of material support coming from Beijing, but you also see a modeling effect taking place. Where, increasingly, the types of tactics employed in Moscow and other cities and now in the occupied territories borrow from a similar playbook to one that Beijing has used, both in terms of mainland China but also in Xinjiang. I think that is something to bear in mind as well.

One of the things that I think is important to recognize on the surveillance front in terms of what we have seen in Russia is that you have over 21 million surveillance cameras that are currently in the country being used, among the tops in the world. You have a number of safe cities. Moscow itself has over 217,000 surveillance cameras, many of which are now powered by biometric facial recognition technology. That is something that can be weaponized as needed. Even prior to the war, what we were starting to see already, especially in Moscow's Metro where you use face pay as a way to purchase a ticket, was a linkage between different types of ordinary transactions, commercial transactions, and the ability for that to then be weaponized by authorities as part of a vast surveillance system.

As Russia has gone to war, as conscription is something that has come into place, we then see authorities using that face pay system to identify people who are flagged the system for having evaded conscription so that they are then picked up. There is a very kind of, I think, important linkage between sort of ordinary systems that maybe initially were put in place and viewed as increasing efficiencies when it comes to providing public services with a weaponization that is very much linked to the political crackdown that is ongoing and intensifying in Russia.

Of course, it is not just surveillance cameras. It is everything from public Wi-Fi, which is also being used as a tool of mass surveillance, as well as the updating of its

surveillance system, SORM, which is able to provide—through network architecture is able to search data available in the system and can get names, passport information, location, tax IDs, addresses, and so forth. The surveillance aspect in terms of what we see in Russia is an incredibly important aspect of this.

Then, of course, we are also looking at censorship as well. Just as we are seeing those tactics used in the occupied Ukrainian territories, we also saw earlier this year a nationwide ban on Telegram occurring. Even before that, many other platforms, especially Western platforms, have been banned as well, forcing people to use VPNs, which authorities are increasingly trying to find ways to co-opt also. On the censorship side, you are also seeing this kind of blending between the two.

Then there are internet shutdowns is another aspect of censorship. There is a new law that was passed earlier this year in February in Russia that gives authorities the power to shut down the internet inside the country in a fully discretionary manner. Not only to shut it down nationwide—which has varying effects, something I have written about—but it also allows authorities to decide whether they want to shut down specific regions or certain cities without having to give any kind of justification. You have an even greater amount of discretion that is afforded that way.

Now, one of the things that I think is important, that my colleagues have mentioned a bit, is the imposition of the Max super app, not only within Russia but how it is being applied and forced in the Ukrainian-occupied territories as well. In September 2025, the Kremlin introduced the super app in the occupied territories. What it does is that it merges communications, ID, payments, government services, housing, and other administrative functions into one single monitored ecosystem that automatically syncs with Russia's servers. What you see there is very much an analogy with China's WeChat app, which is another super app and also consolidates many different functions into one.

In Russia, there are now estimates of 100 million-plus Russians who are on Max. It is something that authorities require to come preinstalled on new phones. Banks and other important nodes of communication and transactions have been ordered to stop using Telegram or WhatsApp for client communication and instead to use Max as well. It is even expected that Max works during—otherwise, when you have internet disruption. There are specific built-in advantages that Russian authorities are trying to give to incentivize, if not coerce, Russian citizens into using Max.

In the occupied territories, part of the insidious aspect of Max is that not only does it force Ukrainians living in those territories to use it, in part because there are no other options available as other apps are curbed, but it is also something that is not accessible to outside Ukrainians. It then severs the connective tissue between Ukrainians living in the occupied territories and those living outside. I think that is one thing that is important to kind of—to think about.

Just to conclude, you know, I think it is important that you look at Putin's domestic insecurity and centralization of power, combined with a faltering war effort, as a driver of the intensifying repression that we are seeing both inside Russia and outside. Not only are we seeing in the occupied territories of Ukraine, but we are seeing an expansion worldwide into many other places. Something like 40-plus countries in Latin America, Asia, Africa, the Middle East, and Eastern Europe now have Max available for citizens to use through telecom operators. We see this as a playbook that has implications globally, not just something that is being used specifically within certain territories.

Why do not I—so I think, just to conclude, democracies need to think carefully how to combat these tools, both spreading public awareness about the coercive aspects of Max, thinking about how Max connects to Russia’s broader coercive agenda in places like Africa and the Middle East, to encourage alternatives like encrypted apps and communications platforms like Signal, and to make a diplomatic push against countries considering letting their internet service providers register Max. I think the good news is that Russia’s hardware commercial expansion is limited. There are constraints to how much Max will spread. I think the bad news is that this is just one set of a growing number of AI-enabled surveillance tools being peddled by authoritarian countries, with modeling happening in Russia and other like-minded countries, like Russia. I will stop there.

Thanks.

Ms. NOVETSKY: Thank you so much. Yes, so we are now going to move into a round of moderated questions, and then following that, we will open it up for all of you to ask questions. Start thinking about what you might want to ask, and when you are ready to ask your question, you can go and line up at this podium over here. Make sure to State your name beforehand.

Just to get started, Iryna, you mentioned how, in terms of news and entertainment, Ukrainians primarily only have access to Russia’s Russky Mir television package on the occupied territories. Well, as we have discussed, Ukrainians do not rely—do rely on circumvention methods to get media from outside. Doing so is becoming increasingly difficult and dangerous. Do you think there is a point where Ukrainians—on the occupied territories—may stop seeking out outside media? Do you feel that teenagers and parents are able to pass down tech habits, like using VPNs, to the next generation?

Ms. ADAM: I think that if we ever get to the point where accessing VPN becomes an actual physical danger kind of on the regular—for now, there are still kind of workarounds for it. There is also the incentive of using it for just purely communicating with the family that most of them will have left in the unoccupied territories of Ukraine, with their friends, with kind of just the desire to read more unbiased news. There will still be attempts to use VPNs to kind of somehow access this information. The more physical danger they will be in, I think it is hard to expect people to put their lives at risk for unbiased information.

At some point, there might be a kind of breaking moment where people have to settle with the Russian ecosystem. Potentially, if there is a full integration, Russians obviously still have some access to the outside world. They do also actively use VPNs. If we are looking at some sort of—of something that Russia sees as a total integration, if it stops feeling threatened, perhaps then people on temporarily occupied territories will have more access. For now, I think it is kind of very tentative, you know, like, what is the risk analysis?

How much do they want to read or engage with the outside world versus how much I want to stay safe, but also at the same time keep my family safe. Because any sort of danger that comes to an individual who is targeted by Russian authorities on the TOT is not just limited to that individual. It essentially covers their entire family immediately. That might be, kind of, a very negative incentive for people to co-opt more into Russian ecosystems, even though we do see a lot of kind of a desire to stay connected to Ukraine. You know, at some point, it is just a matter of danger.

Ms. NOVETSKY: Thank you.

Maksym, so you have spoken and written about how Russia is—Russia is importing Russians to live on the occupied territories. Not just ordinary people, whom they incentivize with different benefits like free housing and things like that, but also police officers and other security officials. How has Russia used its experiences governing within its own borders in implementing the occupation regime in Ukraine? Are there lessons or capabilities from Ukraine that you see Russian authorities implementing at home?

Mr. BEZNOSIUK: I mean, there is a—Russia has been increasingly using those—I mean, importing those Russians inside of Ukraine, just what they call “demographic engineering,” yes. Also, there is an issue with this because some of these police personnel, Russian guards, being imported to the occupied territories of Ukraine, also create simultaneous gaps in Russia. This creates a huge issue for their ability to insulate the regime. I think it might create some long-term adverse impacts, even though they recently announced the increase in funding for security and surveillance measures. I do not think it will help them to narrow this gap.

Ms. NOVETSKY: Steve, you have—you have written extensively about how Ukraine’s innovation in drone warfare, artificial intelligence, and other emerging technologies has supported—helped them have some successes in their war effort. To what extent has Ukraine been able to use any technological prowess to reach people under occupation? Could you talk a little bit more about how United States, Europe, and other democracies could invest in connecting Ukrainians in the occupied territories, and why that would be in their interests?

Thank you.

Mr. FELDSTEIN: Yes. Thanks for the question. I mean, I think you are right that, first of all, we have seen some incredible innovations take place in Ukraine, particularly when it comes to the war effort. We are actually now at a point where many of these innovations are being exported and being used by much larger militaries and other governments, who are studying—whether it is civilian, you know, the Diia app, or whether it’s looking at counter-drone systems, and so forth.

You know, the big conundrum—and it is not just the Ukrainian-occupied territories. It is many other places as well that I have looked at, whether it is Iran and its closed information environment, whether it is reaching dissidents in China as well. There is sort of fundamental difficulty, particularly when there is such a coercive level that Russia or any occupying authority is willing to deploy. What happens is it becomes more of an issue of behavior, as opposed to technology, in that there is an incentive for people not to risk—as my colleagues have mentioned—taking undue risks, even when it comes to accessing information or so forth, because the repercussions of potentially being caught are so high that that becomes a pretty pervasive disincentive.

This is sort of a variation on the chilling effect. What you see is that you hear, if you are in the occupied territories, of different people who have been identified through surveillance, picked up, or so forth. You then sort of are disincentivized to do things. Now, there is a whole ecosystem out there of different types of decentralized freedom technologies that are around. You know, encrypted chats, different types of mesh networks like Bit.ly—not—bitchat, and others, that I think have some possibility there. I don’t know.

I mean, I think the big question is, can you scale it up? Can you do so in a way that evades the notice of Russian authorities? Can you mitigate risk while offering up potential

tools? I do not think there is an easy way to do that. I think a lot of it actually relies on small, discreet physical networks, where people can show and demonstrate how these tools can work, and also provide the right risk mitigation strategies so that you are not handing someone something that will then be sort of signing their prison sentence. It is a tough issue; I will say that.

Ms. NOVETSKY: Thank you. Just one more question for the entire group. You have all talked a bit about how the information that authorities are collecting through these various surveillance methods has been used sort of against Ukrainians, as well as Russians, and others. Could you talk—could one of you or any of you talk a little bit about what it might look like if Russia decides to scale up using this data more aggressively or openly? Also, what might it look like for Russia to use data from, say, the Max app that it is collecting from others outside of Russia and Ukraine?

Ms. ADAM: My personal concern with the scaling of the Max app is that I personally would not really want to live in a society where I am texting people actively who have Max on their phones, because I do not know on a technical level what data it could collect through their phones of me, and kind of what will later be done with that data. I kind of see Max as just an additional vector for Russia to scale its cyberattacks to actively steal data at both a commercial and a State level.

I would be very kind of concerned about personal data leaks, about organizational data leaks, about, you know, like, money being stolen or taken for ransom from banks, or sensitive information being leaked from government organizations. It is just—I think, for me, personally, it would be uncomfortable. We all know that most social media companies are taking more of our data than we might want them to have. I personally prefer American or Western companies doing that versus Russian very overtly state-controlled app that has potential ties to the FSB.

Mr. FELDSTEIN: Yes. I think there is a—potentially significant risk set of risk factors, depending on how and when Russia chooses to weaponize what it's doing with the Max app and those users in its ecosystem. I would sort of point to two aspects, both the control/censorship aspect as well as the weaponization of surveillance, the collection of information as part of that. I can look to WeChat and extrapolate examples from that, I think, that would apply to Max.

One example is that you have algorithmic censoring taking place in WeChat. What do I mean by that? I mean, essentially what it means is that, based on keywords and other sorts of analysis, people will send information from one user to another who is connected on WeChat. Citizen Lab has done a great study on this. If it contains a picture linked to one of a certain number of banned images or words that are also linked to that, it will automatically censor it so the person receiving the message will never even get it. That is what you are getting with machine learning algorithms in place.

Now, is that something taking place in Max? I do not know specifically. My guess is most likely, if not now, fairly soon. It is certainly something that could happen, because we already see it in place in China. Similarly, with surveillance, what you can do is once you get access to the information, and once you are able to kind of take advantage of data integration between different silos of information—so health records, banking records, geolocation of where you are based on your phone, you know what you post on social media. The more you can bring all that into one collective data base, the more you can then do something with that information.

You can do specific parameter searches based on who was in a specific area, who is saying this type of thing, and from what city. Who are they connected to on Max? Who are their friends? Who are they communicating with? And you know what? Then you can pick up all of them. You can bring them in. You can threaten a few of them with incarceration. You could spread fear through that network. Immediately, it brings about a chilling effect and has an insidious impact on that network in that particular community. You know, I am sure some of that is already happening, but the potential for weaponizing that is unlimited in terms of what the Russian authorities potentially could do when you have access to that type of information.

Ms. NOVETSKY: Thank you, all. Yes, I would like to open it up now for audience questions. Please head over to the podium if you have a question, and we will be happy to answer.

QUESTION: Hello. My name is Mamie Powers. I am the managing editor of Eurasia Daily Monitor at the Jamestown Foundation.

I have a question for Steven, actually. You mentioned Russia's methods are largely mirroring those in the PRC and Xinjiang. I kind of have two questions. Could you maybe expand a little bit on those parallels with the PRC and what they are doing in Xinjiang? Also, I am wondering if you have seen any evidence of PRC involvement in helping Russia develop these things, or if it is more Russia mirroring what the PRC is doing.

Thank you.

Mr. FELDSTEIN: Yes. Thanks for the questions. You know, I have studied fairly extensively in the past, you know, the kind of coercive digital methods being used in Xinjiang. What you see is really a combination of physical coercion, grid-style policing, right? Some of it is very traditional, in that you are establishing the physical presence of security officers in key areas, you know, cities, urban spaces, and so forth, throughout, you know, the region. Then you are combining that with really cutting-edge algorithmic and biometric tools, and so you are trying to bring the two together. You are both trying to collect as much information as you can on a digital basis, and then you are combining that with a kind of physical incarceration aspect. A million-plus Uyghurs have been imprisoned. I think we have mentioned that many, certainly thousands, of Ukrainians have been imprisoned as well in the occupied territories.

When you combine those two together, not only does that allow you to solidify your control apparatus, but it gives you kind of nearly unlimited access to information that can otherwise be weaponized by the authorities. That is something that we saw pioneered by China. That was the first time that we had seen it anywhere in the world, where you brought together the physical with the digital, and did so in a pretty seamless way. Of course, you know, it took many hundreds of millions of dollars to both install and to perpetuate, but that was kind of part of the deal there.

You know, what we are seeing—I mean, certainly there is a big modeling effect, a demonstration effect that other countries have studied, although very few have had the capacity to be able to kind of implement that. What we know with China and Russia is that there have been a lot of levels of cooperation. I would not say that China is driving this. Russia has plenty of resources and has a deep technological capability itself. It has companies that are able to provide this equipment. That there is material support in terms of, you know, Chinese technology that does make its way in. We also know that there are regular meetings between security forces and so forth. I do not know what hap-

pens in those closed-door meetings in those rooms, but my guess is that they are sharing lessons and that there is quiet support that is continuing.

I think a really good question to ask, and one that I hope analysts continue to probe, is what is the depth of that cooperation? To what extent are specific lessons or tactics that are being implemented in China making their way over and then being deployed in Russia as well? That, I think, is an area that remains fairly opaque.

Ms. NOVETSKY: Anyone else want to add to that, or not? Okay. Any other questions?

QUESTION: Excuse me. Hello, everyone. Thank you so much for your report. My name is Olga Usenko. I am with the Atlantic Council here.

I wanted to ask what the United States and Western allies of Ukraine can do to help Ukraine to challenge the situation on the occupied territories? Maybe sanctions, maybe other recommendations you can give. Time is very, very crucial now for us. You know what is going on in the occupied territories; we do not have time. We cannot leave these people being brainwashed for such a long period of time.

Thank you.

Mr. BEZNOSIUK: Well, the problem, because of this isolation, there is no information coming in. It is important to help raise awareness. Because many people in occupied territories, for instance, have no idea that they can be evacuated. They have been brainwashed on a daily basis that nobody wants them back in Ukraine. This is one aspect, so to break through this informational blockade. Also, ensure those encrypted channels of communication with them and ensure that there is access, for instance, to Ukrainian education and remote educational opportunities. Because right now it is becoming more increasingly difficult, and Russia tries to shut down those things. Often, people that try to access those educational opportunities study at Ukrainian schools remotely, and they are facing repercussions. Yes, they can be detained, yes, the parents of those children, for instance. This is a serious issue.

Yes, and also help to pressure Russia to open more evacuation channels and let people be evacuated, because there is a huge, I mean, filtration. There is, like, the border still existing, even though they were given—all these people were given Russian passports, most of them. Still, they are not able to leave those territories like normally. It takes several hours. There is FSB. There are multiple document checks. They look for—they check their phones for any information. If they even use VPN, for instance, they can be detained. Like, if they have any history of pro-Ukrainian position. Yes, so it is, like, to pressure Russia to ease those measures, filtration measures, to let people get out. Help with this informational channels.

Also, financial support, because lots of people get evacuated, and that is now around 1,000 people per month on average, which is much lower, actually, than before. There is only one humanitarian corridor from Belarus to Ukraine. Just lots of issues with accommodation and funding overall. Yes, those people did not have families; they faced a lot of challenges and also reintegration support. Maybe Western allies can help as well.

That is briefly, thank you.

Ms. ADAM: I want to second Maksym's points, but also to add that just kind of in general Western support to Ukraine in the efforts of retaking the territory militarily, or to just establishing itself in a position where, during potential peace talks or any kind of agreements, Ukraine has more leverage to advocate for its temporarily occupied territories, to either reintegrate them or to at least ensure that they have some sort of rights

and ability to access to information from the Ukrainian territory, to be able to live their lives, to be able to communicate with their loved ones in unoccupied Ukraine, would be—that is something that is incredibly useful for us.

Also, any sort of, kind of, information sharing or technical expertise in reaching closed environments is, I believe, always very useful. I am sure that there are things that Ukraine can share with its partners at this point from our own experience, but there are also things that Western partners can still share with us. I am sure that these channels of knowledge sharing exist, but they are kind of quintessential for us in our own efforts to help the temporarily occupied territories and the people stuck there.

Mr. FELDSTEIN: Yes. I have a few thoughts. You know, I worked for—my last job at the State Department was in the Democracy, Human Rights, and Labor Bureau. One of our—my roles, my responsibilities, was to—in the region that I was responsible for, which was Sub-Saharan Africa. To pressure and work with other countries to the extent possible to push back against repressive activities taking place. Whether by governments or others, to shine a spotlight, to work with colleagues in interagency to impose sanctions, to work with like-minded countries who are equally appalled by human rights abuses that we saw to pressure and shame those countries undertaking these kinds of activities.

I see very little of that happening right now with this administration. I think, you know, frankly, there is a whole host of things that the U.S. pressure could do. Will it solve the issue in the occupied territories? No. It will raise the cost for Russia in terms of undertaking things that, right now, I think it is getting away with because it is a silent crisis. It is one that does not get the attention that it should. Frankly, it is not one that is a high enough priority at all within the Trump administration. Part of that is the dismantlement of the very institutions, like DRL and others, that are directly responsible for helping to be the tools that would confront these issues.

To me, it is a mixture of—at the moment, the problem is that you have a deprioritized policy apparatus that is not paying sufficient attention to the crisis at hand. The tools that otherwise would be used to address these issues have been unfunded or are not being deployed toward this issue. The sanctions and other types of punitive measures that could be done to heighten pressure are not being used. As a result of that, Russia, I think, is not paying the price that it should for the activities it is undertaking. There are a lot of things that could be done, I think, by the U.S. Government tomorrow that would start to make a meaningful difference in terms of turning the—at least the public reputational tide against Russia in a much more serious way.

Ms. NOVETSKY: Thank you. Any other questions from the audience?

QUESTION: Thank you so much. Shannon Simrell, U.S. Helsinki Commission.

Zooming out, maybe to a bigger concept beyond just sort of these specific apps that we are talking about, and looking forward to the time when Ukraine and its allies can look instead from Ukrainian defense to ensuring that Ukraine gets a just and durable peace, what do you think that the role of limiting Russia's ability to use below-the-threshold technological repression will figure into a conversation about assuring a just and durable peace for Ukraine? Is it time to be more comprehensive in the way that we talk about ending wars and ensuring justice?

Thank you.

Ms. ADAM: I do think that for the peace to be enduring, there has to be some sort of controls over Russia's influence in the information environment. Not only in Ukraine,

but kind of influence that it has with Ukrainian Western allies and the rest of the world. The influence that Russia has in Latin America, in Africa, in Asia, Southeast, and Eastern Asia. They do continue promoting the same kind of narratives that they have been promoting for 10 years, 20 years, 30 years ago, and during the Soviet Union. Their metanarratives do not necessarily change. They are kind of ever-persisting.

We are seeing the evidence of their influence on Russia's own population right now. There is a relatively high percentage of support for the war effort and for support of Putin's presidency, which might potentially just be falling now purely because of Ukraine's bombing off Russia's oil infrastructure. Their influence in the information environment is ever-present. It would be very naïve to expect that they would stop just if we reached an actual peace. Even if we were to reach the 1991 Ukrainian borders in the most perfect kind of utopian scenario, we regain all of the territories, Russia would not relinquish the sort of control and the ecosystem that it has in the territories that it possesses now.

Before the full-scale invasion, the sort of, like, network of telegram channels that I mentioned that existed in the occupied territories, Russia created and deployed those for essentially the entirety of Ukraine. There were dedicated Telegram channels for Western regions, for Kyiv, for central Ukraine, for southern Ukraine. They were pumping out the same kind of narrative because Russia expected to take Ukraine in a couple of days and to fully occupy it. They were prepared. They kind of built their own foundation years in advance, essentially. Even if the peace is reached, even if the current ecosystem is taken down, there are going to be efforts to establish a new one.

It is going to be kind of ongoing if we do not get to a point where we can at least pressure Russia into being a more, kind of, better digital citizen for its own citizens, for its neighbors, for just the general global community. There has to be some kind of conversation, or sanctions, or pressure, or an environment where we can come to some sort of a consensus for the piece to be truly longstanding in the long run.

Ms. NOVETSKY: Thank you. I think we have time for one more question. Yes, go ahead.

QUESTION: [Off mic.] Hi. Sorry. My name is Jenna [sp]. I was wondering how, if at all, you think that Apple removing the Max app from the App Store will affect Russian utilization of Max as a propaganda tool, and if you expect other countries, other companies, to follow that precedent.

Mr. FELDSTEIN: I mean, it is—I would say it is a good precedent, but at this point you are already looking at an ecosystem that is sort of deliberately segregated from Western technology, Western apps. I think, you know, part—I think in part for Russia, I am not sure it has—it will make much of—any of a difference, especially when you are mandating, you know, by the Russian government, that all new phones come preinstalled with Max. It does not matter if you have to get it from the Apple Store or not. Now it is on there anyway, and you are cutting off access to other things.

I would say, in places where there is a more contested environment, where Max is something that could be installed, or users could have an option to use it but maybe could revert to other apps, that is where I think market pressure can play a role. I think it is something that can be a really important tool to use in contested environments where, you know, the usage of Max is much less solidified.

Ms. NOVETSKY: Okay. Well, thank you all so much for being here, and thank you so much to our panelists. I think it is about time to wrap up. Thank you so much for joining us. [Applause.]

[END]

[Whereupon, at 2:56 p.m., the briefing ended.]





The United States Helsinki Commission, an independent federal agency, by law monitors and encourages progress in implementing provisions of the Helsinki Accords.

The Commission, created in 1976, is composed of nine Senators, nine Representatives and one official each from the Department of State, Defense, and Commerce.

www.csce.gov

youtube.com/HelsinkiCommission

facebook.com/helsinkicommission

flickr.com/photos/helsinkicommission

x.com/HelsinkiComm