Commission on Security & Cooperation in Europe:
U.S. Helsinki Commission

"Internet Freedom in the OSCE Region: Trends and Challenges"

Committee Staff Present:
Jordan Warlick, Staff Associate, Commission for Security and Cooperation in Europe

Participants:
Sanja Kelly, Director, Freedom on the Net, Freedom House;
Dariya Orlova, Senior Lecturer, Mohyla School of Journalism in Kyiv, Ukraine;
Berivan Orucoglu, Human Rights Defenders Program Coordinator, The McCain Institute;
Jason Pielemeier, Policy Director, Global Network Initiative

The Briefing Was Held From 1:02 p.m. To 2:18 p.m. in Room 215, Senate Visitors Center, Washington, D.C., Jordan Warlick, Staff Associate, Commission for Security and Cooperation in Europe, presiding

Date: Tuesday, November 14, 2017

Transcript By
Superior Transcriptions LLC
www.superiortranscriptions.com

WARLICK: All right. I think we'll go ahead and get started. On behalf of the Helsinki Commission, welcome and thank you for coming to today's briefing on internet freedom in the OSCE region. My name is Jordan Warlick, and I am responsible for media freedom issues at the Commission.

It goes without saying that the internet has fundamentally changed the way we communicate and receive information. This has, by and large, been for the better, allowing for greater access to information and freedom of expression. Yet, in this constantly evolving landscape of new technologies are new threats and tactics to control and manipulate information. These range from far-reaching restrictions, such as excessive internet regulation or government shutdowns of websites and social media platforms to more proactive tactics, such as arrests of online journalists or campaigns to actively spread disinformation.

While autocracies increasingly fear the power of the internet and crack down on online activity, democracies struggle with how to counter foreign content manipulation campaigns without undermining internet and media freedom. OSCE-participating states have agreed to uphold the principles of free expression and free media, which should apply as much on the net as off the net.

This is a big subject to tackle, but we're fortunate to have such an expert group of panelists to help us dig deeper into the issues. Earlier today, Freedom House released its annual Freedom on the Net report, copies of which have been made available. We'll first hear from the director of Freedom on the Net, Sanja Kelly. She'll share the general findings of the report with us, as well as a more targeted assessment of the situation in the OSCE region. Following Sanja, we have Dariya Orlova, who is a senior lecturer and deputy director of research at the Mohyla School of Journalism in Kyiv. Dariya will shed some light on the specific trends in Ukraine, which has seen one of the greatest declines in internet freedom over the last year and has been a top target for Russian interference. Dariya was a journalist herself in Ukraine, prior to her academic career.

Next, we'll hear from Berivan Orucoglu, program coordinator of the Supporting Human Rights Defenders program at the McCain Institute. She previously served as senior communications adviser to the U.S. ambassador to Turkey and has experience as a journalist at various news outlets in Turkey, Europe and the United States. Turkey's internet freedom record has declined significantly in recent years, which I'm sure Berivan will elaborate much more for us on.

Finally, Jason Pielemeier is policy director at Global Network Initiative, and works with policymakers and other stakeholders to enhance protections for free expression and privacy globally. Before joining GNI, he was special adviser at the Department of State, where he led the internet freedom, business and human rights section in the Bureau of Democracy, Human Rights and Labor. We will follow remarks from our panelists with a question and answer session.

Thanks, again, to our panelists for being here today, and Sanja, if you could please start us off.

KELLY: Thank you very much, Jordan. I'm deeply grateful to the U.S. Helsinki Commission for the opportunity to address this important topic.

My name is Sanja Kelly, and I'm the director for Freedom on the Net project at Freedom House. As some of you might know, Freedom House is the oldest American human rights organization working on the ground in over 30 countries to help democratic governments and to support human rights defenders, independent media and political dissidents. Although our programs are far-reaching, we're perhaps best-known, actually, for our publications. And as Jordan mentioned, today, we are releasing the eighth edition of one of our signature reports: Freedom on the Net, which examines the state of internet freedom in 65 countries globally.

Freedom on the Net is kind of a Michelin guide for net freedom, because we rank governments based on their performance, so you can immediately see on our website, and then also in our publication, what score countries receive, what their strength and weaknesses are and how they compare to one another.

The findings of this year's Freedom on the Net are particularly disturbing. And we had seen that internet freedom has declined for the seventh consecutive year as governments around the world have dramatically increased their efforts to manipulate the information on social media. The Chinese and Russian regimes have pioneered many of the techniques that we will be talking about today, but this manipulation issue has really gone global, and we have seen that governments in 30 out of 65 countries that we examined have employed some of these methods.

I will just give you a few examples. In the Philippines, we have seen keyboard armies actually writing about these issues on behalf of the government, covertly, and kind of giving the indication that policies by the government are widely-supported. We have also seen armies of trolls paid by the Turkish government attacking journalists and attacking human rights defenders.

The OSCE region itself, with its 57 member states, is diverse in terms of – in terms of geography and in terms of type of polity. It encompasses countries that are some of our best performers on the index, so countries like Estonia, Iceland, Germany, the United States and so forth. But then, it also encompasses some of the worst performers. So those would be Uzbekistan, Russia and Turkey. And one of the worrisome observations from our study is that Russia, an OSCE member, is using the internet to interfere in democratic processes in other OSCE member states – not just the U.S. and Western Europe, but also in places like Armenia, Ukraine and elsewhere.

These same manipulation techniques, including paid pro-government commentators, bots and fake news, that the Russian authorities have been using in their disinformation campaigns abroad, have long been used, actually, against Russian independent journalists, political opponents and other critical voices. But this is just only one of the aspects of controls on the internet that we had seen from the Russian government. For example, amid major anti-government protests held in 2017, the Russian government scrambled to further tighten control

over the internet, and now, with presidential elections looming in March of 2018, lawmakers took every opportunity to push through legislation aimed at curbing dissent online. The space for anonymous communication shrunk as the government imposed restrictions on VPNs and proxies, which are key tools employed by both activists and ordinary users to use the internet in relative safety from the government's surveillance, while also allowing access to sensitive content.

And then, there is another new law which requires users of online messengers to register their phone numbers, linking their online communication to their real identities. And LinkedIn was the first major international platform blocked for refusing to comply with data localization requirements. We've seen social media users imprisoned for their expression online, and we've also seen LGBT activists charged with spreading so-called gay propaganda online, and they were issued hefty fines. But overall, in terms of the region, internet freedom in the OSCE – in the OSCE has followed similar patterns as the rest of the world. And of the 19 OSCE countries we examined, 12 declined, four improved and three saw no notable change. And I would like to highlight the following three trends over the past year that contributed to this overall decline.

Number one, as I mentioned, is this issue of growing online manipulation. And as online censorship and other restrictive tactics prove inadequate in curbing dissent, more and more governments are now mass-producing their own content to distort the digital landscape in their favor. Our study documents that the creation of online government propaganda, through government-sponsored websites and outright editorial directives to news media were among the most widely-utilized methods of manipulation, and they were followed by paid government commentators, by use of political bots and international – and intentional distribution of false news stories – "fake news," as you will have it.

Although some governments sought to support their interests and expand their influence abroad, as was the case with Russia, in many cases, governments actually used these methods inside their own borders to maintain their hold on power. So, in Turkey, for example, some six thousand people have allegedly been enlisted by the ruling Justice and Development Party to manipulate discussions, to drive particular agendas and counter government opponents on social media. The second trend I wanted to highlight is this issue of physical attacks. And the number of countries that featured physical reprisals for online speech increased by 50 percent globally over the past year. And this trend was mirrored in Eurasia as well, where online journalists and bloggers who criticized the government, who wrote about corruption or about social issues such as LGBTI rights were beaten, and in some cases, murdered. Perpetrators in most cases remained unknown, but their actions often aligned with the interests of politically powerful individuals or entities.

In Russia, for example, in May of 2017, Dmitry Popkov, who is editor-in-chief of a local newspaper and online outlet, was shot and killed in his home by unknown assailants. Popkov was known for his critical reporting on corruption, abuse of power and criticism of authorities. Failure to bring to justice perpetrators of these attacks perpetrates a cycle of impunity and creates a chilling effect for others writing on the same substantive issues. And then, I want to bring up this issue of technical attacks, because this is something that we have highlighted as a global trend, and it has been a particularly important trend in the Eurasia region. Technical attacks

against news outlets, opposition and human rights defenders has generally been on the rise globally, but our analysis showcases, actually, that the greatest number of successful attacks – meaning when the websites were taken down, or when activist networks were infiltrated – actually took place in Eurasia and Latin America.

Indeed, the security vulnerabilities present government-affiliated entities with an opportunity to intimidate critics or censor dissent online while avoiding responsibility for their actions. And it is often difficult to identify, with certainty, those responsible for anonymous cyberattacks, including when suspicion of government involvement are high. There are several outcomes, or several particular ways in which we had tracked some of these attacks. So we had found that the most frequent outcome of these attacks was actually having websites temporarily disabled. So these types of attacks, you know, are often perpetrated through DDoS attacks; they're a relatively easy and relatively inexpensive way to retaliate against those who report on sensitive topics. And we had seen that in a number of countries. In Azerbaijan, for example, the independent online news platform Abzas was subject to a series of DDoS attacks in January 2017, and they were actually online until they were able to migrate to a more secure service.

We've also seen, as an outcome of these attacks, increased surveillance of reporters and dissidents. And just to give you an example, in August of 2016, reports emerged that Kazakh opposition figures and dissidents living abroad were targeted with malware attacks, with evidence suggesting that the attacks were conducted by agents of the government via an Indian security company called Appin Security Group.

We've also seen websites and social media accounts being compromised. So, for example, in Belarus, on the eve of the March 25th Freedom Day demonstrations, the Facebook account of one of the opposition leaders and a chief organizer of the protests was hacked, and the account, then, after it was hacked – it actually disseminated fake posts under this opposition leader's name that actually discouraged people from attending the demonstration.

So the issues that I outlined are serious and pressing, and given that many of our social interactions today take place online, this fight for internet freedom has become inseparable from the broader fight for democracy and human rights. And I'm just going to offer a few recommendations in the end, in terms of what can be done to help remedy this issue. So, number one would be, through Congressional appropriations, we should ensure robust funding for the State Department and other relevant agencies for internet freedom programs that support advocates around the world in combating disinformation. They also provide cybersecurity training to civil society and independent journalists, and enable emergency assistance for human rights.

I would also urge the U.S. Congress and the Commission to speak out and condemn publicly when someone is arrested or physically attacked for simply posting their views online on politics, human rights or social issues. And that will send a message that these incidents do not go unnoticed by the U.S. government. I think, domestically, we need to ensure that political advertising is at least as transparent online as it is offline, and online political ads should indicate who sponsored them, and social media companies should make this information available and indicate the source of payments for such ads. And finally, better media literacy is needed to help

citizens discern fake news from trustworthy sources, and Congress should review current law and policy with this in mind and assist in these educational efforts through speeches, town halls and other constituent engagements. Thank you.

WARLICK: Thank you very much, Sanja, for the summary of your findings in your report and for offering those recommendations to us. Dariya?

ORLOVA: So first of all, thank you for the opportunity to participate in this discussion, and also provide an overview of the Ukraine case. According to this year's Freedom on the Net report, Ukraine has shown to be one of the biggest declines among examined countries. The country has lost seven points compared to the previous year. The major reason of the decline is the introduction of bans on several Russian internet services, including two popular social networks, VKontakte and Odnoklassniki, a popular email service, Mail Ru, one of the most widely-used search engines, Yandex, and several other online services as part of sanctions against Russian companies.

So the ban was introduced in May this year. In justifying the ban, Ukrainian government argued that it is a security measure in response to the information war launched by Russia against Ukraine, pointing out that the – to the capacity of Russian security services to extract and use metadata on Ukrainian users from these platforms. The move got a huge public reaction, both inside the country and outside, particularly given the popularity of the targeted websites; to give you some figures, about 20 million of Ukrainian users were registered on VKontakte, and about 5.5 million users on Odnoklassniki, which means that every fourth Ukrainian was online on VKontakte.

Several other factors, however, also contributed to the Ukraine's drop in the index of internet freedom this year. Among those, persistent prosecution of social media users for expressing separatist viewpoints and threatening the territorial integrity of Ukraine. So, dozens of such cases have been noted. In addition, there has been quite a dangerous environment for online activists and journalists, particularly in the light of murder of online journalist Pavel Sheremet in July last year.

The report on Ukraine also reflects a tense situation with internet freedom, especially with regard to user rights violations and online censorship in the eastern part of the country, in the self-proclaimed separatist republics, where de facto authorities have been prosecuting and even imprisoning social media users and bloggers. So, this also contributed to the overall score of Ukraine. The ban on Russian social media by the Ukrainian government attracted fair criticism from various actors, however, primarily from the external ones. In the very country, response has largely been less critical, although one could observe divisions with regard to this issue and criticism as well. Acceptance of the ban by a significant part of the Ukrainian society, particularly among elites, is explained by the acuteness of challenges that Ukraine has been facing during the last three years.

So, as you might know, during these last three years, Ukrainians have experienced Euromaidan revolution, then annexation of part of the territory – Crimean Peninsula by Russia, and the eruption of armed conflict in the Eastern part of Ukraine. These actions were also

accompanied by a very harsh propaganda and disinformation campaigns coming from Russia, and the scale of these campaigns has been enormous during these last three years. It started with outspoken distortions in the coverage of Euromaidan protests and biased portrayal of protesters by Russian media, which contributed to polarization of Ukrainian society, particularly in the regions characterized by stronger historical and cultural ties with Russia, where people tended to consume Russian media, including news, quite a lot.

Thus, Russia utilized vulnerabilities of some of the social groups in Ukraine. Disinformation and propaganda has had quite many forms in Ukraine, starting from fake stories disseminated through the mainstream media, but not only. For instance, Russia created supposedly Ukrainian websites with very critical content about Ukraine and the government, but then journalist investigations revealed that, in fact, those outlets are located in Russia, and they don't even have local correspondents in Ukraine. So their whole content about Ukraine is coming from Russia, and what is more, they present themselves as Ukrainian media outlets, but in fact, they are not.

We have also seen proliferation of various agents conveying specific narratives into Ukrainian online public sphere. For instance, one of the most recent examples is that – the findings by the BBC on the Russian troll factory in St. Petersburg that worked with the self-styled Donetsk People's Republic in Eastern Ukraine to produce extreme propaganda videos that aimed to discredit pro-Ukrainian elements and stirred up the conflict in the region. So these videos were widely disseminated through social media.

In Ukraine, we have also found some other examples of such manipulations coming from external agents. In the online public sphere, for instance, Kremlin-aligned trolls have been observed posing as enthusiastic Ukrainian patriots online, creating several – not several, but dozens of thematic groups and communities in the social media, and observers have noted that the troll accounts operated in quite intricate networks and often highly-active in Ukrainian patriotic groups on social media, sometimes even acting as administrators of those pages. Their profile pictures have been observed to contain symbolic Ukrainian images, and those accounts typically posted content and comments that depicted the Ukrainian government as failing their citizens and calling for the violent overthrow of the current administration. So their biggest message and narrative was that, let's have the third Maidan – let's overthrow this government, which is not leading Ukraine in the right way.

However, it is not only external agents that have been flooding the Ukrainian online public sphere. There have been numerous attempts to manipulate online debate in Ukraine, coming from many different political actors inside the country. So we have seen the growing number of attacks on journalists – I mean, verbal attacks on journalists online, especially those journalists that produce some critical contents – some investigations. So their accounts on social media have been flooded with very negative comments from various accounts, most of which have features of trolls or bots. So, as a result, we now can observe social media fatigue among media community and broader public, too, in Ukraine, because of this toxic influence of paid commentators, trolls and bots. And many journalists claim that they feel discouraged to actively participate in the online debate because of this high presence of trolls and bots.

There are reports suggesting that the network of companies and organizations that offer such services to various actors, including politicians, is quite broad in Ukraine, and so there is the whole ecosystem that includes various actors that manipulate the online public sphere. So I think that this briefly tells us about the situation in Ukraine and the major challenges that Ukrainian internet freedom and actors of internet freedom have been facing so far, and I'll be glad to answer to your questions. Thank you.

WARLICK: Yeah, thank you, Dariya, for that summary of the significant challenges that Ukraine is facing. Berivan?

ORUCOGLU: Thank you. Thank you, Sanja, for a great report, and that very depressing one globally. (Laughter.) Actually, it really breaks my heart to talk in a panel about internet freedom and about Turkey, because not long ago – like seven years ago, Turkey was seen as a model country for Middle East and for other democracies. And yet, here we are, and Freedom House has every right to mention the sharp decline in internet freedom, because this is not only freedom of internet, but freedom of press, freedom of expression in general is restricted in Turkey, and by the day, we are losing more rights. And maybe, just to mention some figures would help you to have a better understanding.

Since 2013, it was the mark of the protests – Gezi protests – Turkish public has divided tremendously: pro-Erdogan, pro-government people and the people who hate Erdogan in whatever he does. So there is enormous polarization within the public, and the government is trying to control the message, not only in mainstream media, but also on social media. The mainstream media is under government control, either by government people or even the other opposition papers are trying to align themselves with government because they are scared of the bans and imprisonment, which they have every right to be.

Right now, in Turkey, there are 150 journalists behind bars, and 200 media outlets are shut down. Over a thousand CSOs are also shut down. And after last year's failed coup attempt, more than 60,000 people have been arrested and 140,000 are fired or suspended from their jobs. And just last year, almost 4,000 people are sued for insulting President Erdogan on their social media accounts. And I want to remind that 240 of them were under the age of 18. So it is really grim – the situation is grim. The mainstream media already lost its touch with people, so people do not trust mainstream or traditional media, and the primary focus for news gathering is social media. So this also brought more restrictions to internet freedom, and especially in social media.

So most of the time, Turkey is seen and Turkey is reported as the world champion in Twitter censorship. And most of the content withheld or blocked requests are coming from Turkey, and unfortunately, this year, we didn't disappoint. Once again, in Twitter requests, Turkey has failed. And internet connection is so often slowed down – especially during security operations or protests or after terrorist attacks. Actually, when I first came to the United States, I was a little bit panicked, because I didn't have a wi-fi connection. So, automatically, I assume something big is happening. It was just Comcast maintenance. (Laughter.) But it takes me for a while to get used to this. Unfortunately, we are so used that internet slowing down or shutdowns. Access to, for example, Twitter, Facebook, YouTube, and WhatsApp are restricted so many times, and sometimes blocked – sometimes just for a couple of hours, or days,

depending on the situation, depending on the region, and mostly southeastern part of Turkey affected from those restrictions.

Oh, another – Wikipedia is permanently blocked, actually, in Turkey since May. So it's because of Turkey's involvement in Syrian war – or, allegedly – and popular VPNs and Tor is also blocked or limited. Over 100,000 websites are banned, and most of the time, the owners of the banned sites are not informed or have enough time to comply the requests. So there are so many websites are banned. And almost every day, minimum seven people are detained because of their social media posts. So people are actually quite paranoid to write anything or to talk about anything. And they have a good reason for it.

In recent years, after the coups, people, including journalists, academicians and activists, are hesitant to even like or retweet a post, because they don't know what it can bring in terms of charges, in terms of – it is so easy – the perception is basically, you can lose your job or your freedom if you are not supporting the government – more than the government, President Erdogan. So this is the general mood, and the government has so many tactics. Sanja mentioned that, for the last four years, government employed 6,000 trolls, basically, to harass and to control the online content and online discussions. They ended up harassing journalists, human rights activists or any citizen, basically, who is opposing President Erdogan and his policies.

And no one is immune. It included politicians, academicians, top models or film directors, singers. So anyone from society can be targeted by those trolls. And usually, those trolls are not only harassing them online, but most of the time, it brings prosecution after that. So this is the dangerous trend. Also, there was a hack in one of the ministers' email, and we learned from those leaked emails – we have 6,000 trolls, but also we have more people who are just die-hard loyalists, and only working for President Erdogan. And the smaller group, apparently, is looking for coders, graphic designers or former military members who have experience in psychological warfare.

And trolls are not the only thing that government is using to repress, basically, the free communication – free online communication. Turkey is one of the highest countries in using bots in Europe and Middle East and Africa. There is also one interesting – there was also an interesting case last year. The government is not only oppressing the opposing voices, but also eliminates competition within the governing party. Last year, prime minister – then Prime Minister Ahmet Davutoglu forced to resign after a blog appeared, which was called Pelican Brief. And it was basically harassing Davutoglu and his team, and he ended up resigning, and an Erdogan loyalist, basically, replaced him. And this blog was basically run by pro-government columnist and journalists who are known close to Erdogan and Erdogan family. And also, this year, apparently, they are hiring new hackers – it's called white hat hackers – and there was a online competition to find the best hackers to protect Turkey, which kind of creeps me, because I don't know what they are going to be responsible of.

If those are not enough, by the way, the police is also encouraging people – regular citizens to become ears and eyes of the state. So they have new applications and accounts, basically, to tell citizens to snitch others. So people are sending screenshots or links of certain Twitter accounts, and they send it to police so that others can actually follow up. And it is – the

pretext is always national security, and to protect country, but it ended up – people, for example, snitching about their coworkers which they don't really like. So there were so many examples. And also, this – the Turkish people, because of this whole harassment, basically, they rely on encrypting messaging. They don't trust anyone; they no longer use Twitter as – they still use Twitter or social media platforms, but they are more hesitant to share their own views. So they are using WhatsApp, Telegram or Signal or those kind of encrypted messaging services. And one of those messaging services became, actually, quite relevant, because after the failed coup attempt, thousands of people were arrested just because they have an application on their mobile phones. The application was called ByLock, and right now, 200,000 people are under investigation because of this application.

According to government, if you have any links to this application, this means that you are basically a coup plotter or you are trying to overthrow the government somehow. The good news is, even the government realized that this single app cannot be a whole evidence to imprison people. Bad news, there are so many people already in jail because of this application, for months. But I want to be fair – before the last year's coup attempt, no one ever heard of this application in Turkey other than this Gülenist group who were basically in charge of the military failed coup attempt.

And I just want to make a warning to U.S. public, basically, because this attitude towards the Gülen group –they were actually the allies of Erdogan until very recently – and in the United States, there is almost an understanding that this group is kind of tolerant, moderate and basic activist organizations. The perception in Turkey – opposition or government, everyone – almost everyone unites that this is not a really clean organization. They are not transparent. They are responsible of the failed coup attempt, which attempted – 250 peoples' lives, and thousands of people were injured. And more than that, they are not only responsible of the failed coup attempt, but till recently, they are the ones who were doing the illegal wiretapping, or they were the ones harassing people online, fabricating evidence, which ended up so many journalists in jail in 2008 and basically until 2012.

So this – we're not talking about a group of really clean activist organization, but unfortunately, it seems that the dislike of Erdogan in the West, especially in the U.S., seems to give a free pass to Fethullah Gülen and his organization. But for so many people in Turkey, people have great difficulty to understand this attitude. Yes, there are so many reasons to criticize Erdogan. We do it every day. But this doesn't mean that some of the measures, at least, have some sort of a pretext. Yes, Erdogan used this as an excuse to oppress more critics. And there are so many people in jail who have nothing to do with Gülen – basically, journalists, activists – they always criticized Gülen, but they ended up in jail. This is Erdogan. But also, Gülen, who is residing in the United States, is a huge issue for Turkish people. And for the first time, the entire Americans and Turkey is in 90 percent. So people are united against that and I really warn the U.S. public to be more careful when dealing with Gülen. There is a reason that – of this whole attack and whole criticism about Gülen in Turkey.

Last but not least, yes, the situation is grim, but Turks are resilient and creative. They come up with different tricks every day to basically overcome the obstacles and restrictions. For example, one banned website recently celebrated its 41st new domain name – (laughter) – and it's

not the only one – so many of them. And I'm not going to be able to tell the trick, but smart Turks can access Wikipedia with just a minor trick. I don't want to tell about it because – (chuckles) – then it can also be banned. But thank you for listening, and I'm open to questions.

WARLICK: Yeah, thank you very much for describing the realities in Turkey. The statistics you referenced were pretty incredible and very disturbing. Jason?

PIELEMEIER: Thank you Jordan, and thank you to the Helsinki Commission for hosting this event. Thank you to the fellow panelists. Just want to start with a brief introduction to the Global Network Initiative, for those who don't know us. GNI is a global multi-stakeholder platform that's dedicated to the protection of free expression and privacy online. Our members include internet and telecommunications companies, human rights and media freedom groups, academics as well as investors. So a very broad-based coalition.

We work with four principal functions. The first is, we have a set of GNI principles and related implementation guidance, which provide a framework for responsible company decision-making and action in response to government requests and demands. We foster accountability through an independent assessment process to evaluate our member companies' implementation of those principles. On the basis of this, sort of, trusted platform, we then create. We do shared learning, both internally among our members, which is a, kind of, closed, private conversations, as well as externally with relevant stakeholders, including government. And then, finally, we promote collaborative policy engagement on the issues that are central to our mission.

In almost all of those areas, we use and place tremendous important value on the Freedom on the Net report, and I'd like to just take this opportunity to thank Sanja and her team of incredible writers and editors for producing yet another year of invaluable, if disheartening, reports. I also want to pay special attention and send my thanks to those organizations that provided financial support to Freedom on the Net, without whose support this report can't cover nearly as many countries as it does. So, in particular, I want to note GNI members Google and Yahoo – now Oath – who supported the report again this year. And I also want to acknowledge the vital support of the State Department's Bureau of Democracy, Human Rights and Labor, where I worked until quite recently. I hope the folks here on Capitol Hill remain committed to supporting DRL's amazing internet freedom grant work, including its support for Freedom on the Net.

So I want to talk a little bit about some of the trends that have been discussed so far, but place them, perhaps, in a little bit of a longer historical timeline. I think that you can see a lot of the activity that's been taking place – the, sort of, repressive activity that's been taking place online of late as a reaction to some of the frustrations that governments have had in trying to take simpler routes to getting rid of problematic content or surveilling people who they think are using the internet in ways that undermine their own regime security.

So, you know, traditionally, the kind of initial approach of repressive governments to problematic content – content that they see as problematic is to try and censor it. I think, increasingly, they have found that they don't have as much leverage over the principal social media platforms as they would like, and they have become frustrated with their inability to get as

much compliance as they would like to see from the major net companies. I think, you know, GNI, certainly – we'd like to take some of the credit for that. Our principals help provide a framework and support for companies in pushing back against over-broad requests from governments.

And then, on the surveillance side, I think, you know, in particular, the increasing use of encryption, both HTTPS encryption for web searches as well as end-to-end encryption for messaging has made it more difficult for repressive governments to have direct access to the content of individuals that they are trying to monitor. And so, what we're seeing is sort of an evolution of tactics in response to some of those frustrations.

So I would characterize those in two general, sort of, categories. One is defensive maneuvers by governments intended to protect themselves from activities that they see as threatening to their power base, and then, offensive, which is a newer set of activities which include activities that go beyond just their own, you know, traditional jurisdictional borders. So, to speak a little bit about some of the trends that we observe in each of those categories, first, on the defensive side, folks who study history may remember in the 1970s and '80s – in particular, in Latin America, an economic model called import substitution industrialization, where developing countries essentially imposed very high tariffs on imports in order to try and shelter and build up domestic industrial production. This was largely a failed economic strategy, but I think I see some parallels in today's, sort of, internet era – what I'll call internet substitution informatics. So it's ISI, but a different kind of – a different realm, and a different set of techniques.

So governments are essentially increasing the scrutiny and their requirements for foreign media generally, and foreign social media specifically, as well as supporting the development and protection of national champions – so trying to build up national competitive social and internet services – social media and internet services. So you see that, for example, in Turkey; Turkcell has come out with a new search engine called Yaani, which is intended to promote Turkish culture and values.

You see that in Russia, with some of the – the protectionism for some of the Russian internet media companies, which are seen as useful and more accessible and more compliant for government, as opposed to the foreign media – foreign and social – foreign media and social media companies. I think that also is – it dovetails with some of the threats we've seen just in the last week from President Putin to respond, quote/unquote, "tit for tat" to the forced registration of RT here under FARA. And so no action has been taken, but there's certainly a signal that there may be steps taken in days to come against foreign social media, in particular U.S. social media.

Those sort of building up in support for domestic internet services, I think, are also in line with kind of the broader strategy that you see recently in Ukraine, right, attempting to basically ban Russian social media. Not as much in order to protect any kind of domestic incumbent, but rather as a security measure.

And sort of similar to that, you know, there is a very sort of conscious and by now several-year-old strategy on the part of certain authoritarian leaders, in particular in the OSCE region, to kind of – to discredit Western social media platforms. So Zeynep Tufekci, the Turkish scholar, has called this Erdogan's strategy to demonize social media. And certainly Vladimir Putin has been quite vocal in his criticism of platforms like Facebook and Twitter. So I think that, you know, some of those efforts to discredit the Western social media companies, I think, are also part of a broader attempt to try and get the public in some of these places to either move away from or approach what they see on those platforms with caution.

And I think, unfortunately, the media narrative and policy narrative that's evolving here in the U.S., as well as it has a somewhat longer history in Western Europe, around hate speech and fake news is playing into that. So, you know, you hear some of these authoritarian leaders saying, yeah, we told you that these platforms were dangerous places where horrible things happen. And without any sense of irony for what sort of role they may have played in fostering some of the hate speech and so-called fake news, they are now very happy to see people in the U.S. and in Western Europe calling for limitations on these platforms and essentially approving of regulation of speech on social media platforms.

Another trend that has certainly picked up steam and is well-documented in the Freedom on the Net report is the push for increased data localization. So Russia has its very strong personal data law, which requires any data operators that record, systematize, accumulate, store, amend, update, and retrieve data collected on Russian citizens to do so on servers located physically in Russia. The enforcement of that to date has been spotty. Dariya mentioned or Sanja mentioned, I think, that LinkedIn was the first sort of trial balloon. So LinkedIn was essentially pushed out of Russia for not complying. You know, LinkedIn did not have a huge business there, so it wasn't a huge deal to them or, I think, to the Russian government. So it's still unclear whether or not they would be willing to take similar steps towards some of the larger platforms, but we've heard just in the last week threats to sort of make Facebook the next company against whom the Russian media regulator might enforce that law. And we've seen that kind of personal data law copied in other CIS companies, for example in Kazakhstan.

It's unfortunate, I think, that – and again, with each of these examples, I think that the governments, in particular in the OSCE region, have been able to cite sort of legitimate policy rationales as a pretext for what are essentially authoritarian maneuvers. So, in the case of data localization, they can point to the data protection laws in Europe in particular and some of the incipient data localization in Western Europe. So, for example, Turkey's data protection – Turkey has a law on the protection of personal data which came into effect in 2016 which limits the transfer of personal data out of Turkey and puts burdensome obligations on individuals to transfer personal – which transfer personal data to another country. It also created a Data Protection Board, which is staffed by political appointees rather than technical staff, to assess which other countries provide a, quote/unquote, "adequate" level of privacy protection.

So this is very similar to the European Privacy Shield arrangement, which has gotten a lot of attention in terms of its application to the U.S. And not to in any way suggest that the European Privacy Shield or data-protection regime more broadly is intended to enhance European surveillance – I don't think that's the case at all – but I do think that you could

question the motives of, for example, the Turkish government, whether it really is about protecting Turkish – data of Turkish individuals, or rather an attempt to concentrate that data domestically, where it's easier to get access to it.

So, moving to some of the trends we see on the offensive side, again, one that was noted in the Freedom on the Net report was the increased use of spyware or hacking tools against – very specifically against targeted individuals, either journalists or opposition figures. That's something we've seen worldwide, but also in the OSCE region. Azerbaijan journalists have been targeted, and it seems clear the government may have had a hand in that. The opposition in Kazakhstan has documented in court case that's been brought by the Electronic Freedom Foundation. Going back a couple years now, Privacy International did a landmark, very extensive report on surveillance in Central Asia that documented purchase orders by many Central Asian regimes to some of the Western companies that produce this spyware, and there's very little control domestically within those governments – within those countries in terms of how the government has used that software.

I think, you know, again, the concerns around surveillance that came out of the Snowden revelations in 2013 have undermined, I think, some of the criticism of this trend. And I think, unfortunately, also some of the attention to concerns about extremist content and terrorist use of the internet have been a ready justification that some of these authoritarian governments use to justify the purchase and use of these hacking tools.

The other big trend, which is the headliner for this year's Freedom on the Net report, is the use of misinformation. So Berivan talked a little bit about the RedHack leak in Turkey, and the insight that it provided into the Turkish government's attempt to sort of smear political opponents and engage in psychological warfare, as you said. Clearly, we see this coming out of Russia for political purposes, as Sanja and the report rightly points out, not just targeted against the U.S. but against a large number of countries, many of whom are in the OSCE region.

But we also have seen good journalistic reporting on covering some of the misinformation that's really purely for economic purposes, so the infamous Macedonian journalists – oh, sorry, not journalists, but teenagers – (laughter) – who were, you know, basically cut-and-pasting right-wing disinformation, and packaging it in a way that they could get as many clicks as possible and generate actually fairly significant income, at least by Macedonian standards.

And, of course, the Western policy narrative that we've seen cited as a justification for this kind of – in particular the cross-border manipulation of information is the very internet freedom agenda that the U.S. government, with strong support from both sides of – both parties here on Capitol Hill, has pursued. Of course, that's extremely cynical and disingenuous, but that is the excuse and the pretext that is at times cited by authoritarians who – authoritarian regimes.

So those are some of the trends that I think we've seen increasingly. I'm, you know, particularly concerned with the copycatting and the exchange of worst practices, perhaps we can call it, that we see in the OSCE region, in particular in the CIS region – a lot of exchange of knowhow. You know, the Russian SORM system – the System of Operative-Investigative

Measures – which is the sort of surveillance at the internet-backbone level, is reproduced in a number of countries in Central Asia, and relies heavily on Russian companies who provide some of the hardware and software components of that. A lot of these tactics we're seeing modeled, whether it's just, you know, sort of observing it and copying it, or whether there is, you know, some kind of collaboration and cooperation among these governments is still not entirely clear.

But we, I think, need to take heed of that and do as much as we can collectively as organizations that support internet freedom, as individuals working to support internet freedom, and as components of the U.S. government to ensure that we are providing the right counter sort of channels of information sharing to increase awareness not only of digital security measures and ways to avoid surveillance and censorship, but also making sure we are articulating what good policy looks like so that those governments that are sort of on the edge, trying to figure out how to regulate the internet, have good, clear examples of how to do it in a rights-respecting way so that they can balance that against some of the more problematic and authoritarian models that are being provided.

So I'll stop there. Happy to engage in Q&A.

WARLICK: Yeah, thank you very much for sharing some of the trends that you're seeing from the diverse GNI member perspective.

We're running a little bit short on time, and we don't want Sanja and Dariya to miss their flights, but I will just go ahead and ask a couple of questions to you now and then open it up to Q&A. So hopefully we can get a few in if we can please make answers as brief as possible.

So, first, to Sanja and Jason, you've both been tracking developments in the internet freedom space for some time. Has there been a particular country that has most surprised you this year in the OSCE region – for Sanja over the course of this report, and Jason in the last year at GNI and the State Department – and either for the better or for the worse?

And then, to Berivan and Dariya – Dariya, you mentioned that the, you know, Ukrainian elite have maybe been a little bit less critical as a result of the acuteness of the challenges Ukraine is facing. How encouraged are both of you, in Turkey and Ukraine, by the civil society and public response to what's been going on? And how much of an influence do you think that this could have on the top levels of government, or does any chance for improvement need to originate from the top? And further, how can the U.S. government and specifically the U.S. Congress better support civil society and internet freedom advocates?

Whoever would like to start. Maybe Sanja and Jason's question first.

KELLY: Sure. So, in terms of some of the biggest surprises, actually, it was Ukraine for me because until recently Ukraine actually fared reasonably well in terms of internet freedom, and it is over the past year that we have seen these new restrictions surface. I think for me personally it's been particularly disappointing because in order, essentially, to fight Putin's tactics, you know, the Ukrainian government has embraced censorship, and in a way has become like Putin in this particular extent. So that would be one particular country.

Another one that – perhaps it's not as surprising, but it's definitely a diversion from the past, is the case of Azerbaijan. And Azerbaijan has always been in the business of restricting internet freedom, at least since we started tracking the country, but their tactics have changed over the past year. So, in the past, they seem to have focused on actually arresting online journalists and online activists who were speaking out against the government, but they actually weren't blocking many websites. And, in fact, that's one of the key reasons when, you know, we would go and talk to the government officials or when they would make presentations at international conferences, they would say, oh, what censorship in Azerbaijan? We're not blocking really anything. And that has changed over the past year.

So they had passed a new law that essentially authorizes blocking in wide circumstances, mainly in the circumstances where national interests or the interests of the society are being impacted. And as a result, we've seen a number of independent websites, including an online TV channel as well as Radio Free Europe/Radio Liberty, being blocked. So, anyway, just a change of tactics there.

PIELEMEIER: So I guess I would call attention in particular to some of the countries that actually do fairly well on the report, notwithstanding the fact that they operate in a very difficult neighborhood where there are a lot of challenges that they have to deal with and no easy solutions. So in particular Georgia, which is in the top 10, I think deserves a lot of credit. You know, the record there hasn't always been great, but over time they've managed to avoid some of the worst decisions that some of their neighbors have made and they've managed to maintain a relatively liberal, rights-respecting environment online. Also worth pointing out Armenia and Kurdistan as countries that are – that do relatively well. And I think it's really incumbent on all of us to not only call out those countries that do really poorly, but also acknowledge the countries that are doing relatively well, and make sure we provide support to them so that they can continue to demonstrate in a kind of more locally appropriate and perhaps adaptable way how to protect internet freedom in that region.

I also would just point to the Ukraine as kind of one of the countries of biggest concern, not because I – you know, certainly the difficult environment that they face, the difficult information environment as well as the physical attacks and conflict in that country, are in some ways unique. But really for those very reasons I think it is incumbent on all of us to be doing more to provide support to reformers who are trying to take advantage of what, you know, I think a lot of people see as a really once-in-a-generation opportunity to liberalize the legal architecture in that country.

That window, I think, I fear is closing. I mean, Dariya can speak to it much better than I can, but I feel that window of opportunity is closing quickly, and it's only going to get more and more difficult to implement, you know, liberal reforms. And so I commend those here on Capitol Hill who have made Ukraine a real sort of consistent point of attention and focus, commend organizations like Internews and others within GNI who have been doing a lot in that country, but really encourage more of all of our organizations and entities to do more to support in particular internet policy reform in the Ukraine.

WARLICK: Thank you.

Dariya and Berivan, if you'd like to answer the other question I asked or respond to any of the other comments.

ORLOVA: Yeah. So you asked about the reaction of the civil society to the ban and to other initiatives that could threaten the internet freedom in Ukraine. Well, actually, when it comes to this particular ban, I would say that the voice of those who opposed to it was quite weak in Ukraine. So even if they – of course, there have been actors who – I mean, like some NGOs, some journalists – who expressed their criticism of the move. However, they haven't been very active in expressing that and reaching like the big media discourse. And that is explained by the extreme sensitivity of the issue of the Ukraine-Russia war, because there's this general atmosphere of fear in Ukraine that Ukraine's territorial integrity and sovereignty still under threat, and so let us not discuss that a lot.

However, some positive signals that could be observed in Ukraine recently include a quite strong reaction of NGOs with regard to several proposed bills that also included some of the provisions that potentially could lead to restrictions in terms of internet freedom. And then NGOs united – Ukrainian NGOs united – and they have been quite unanimous in their criticism of those provisions. And so in one of the draft – one of the bills that was accepted, this dangerous provision was deleted from that. So I would say that's an example of some positive impact that NGOs can have when it comes to the restrictions of the internet freedom.

So, to summarize, when it comes to the conflict with Russia issue, it's very sensitive, and you cannot expect much strong voices in Ukraine. But when it comes to restrictions with regard to some political implications, one can expect such voices.

WARLICK: Thank you.

ORUCOGLU: You asked how encouraged I am, and I'm a natural-born pessimist, so not very much. But I think things will get worse before it gets – or even if it gets – better.

The thing is, I 100 percent agree to Sanja and her recommendations, especially about the speaking up part, because for most of the activists or imprisoned people the only thing that matters, you know, and helps their release is the international support. And with this administration, but also even with the Obama administration, Turks were very much disappointed because they didn't really see the support or public support of the imprisoned activists or the journalists. And so, so many people are actually looking for Congress to speak out when there is human rights violations or against press or private citizens. And I agree with you that DRL is doing a very important job, but we see less and less State Department's involvement about those issues.

So, absolutely, the activists not only in Turkey but in the region are looking forward to hear just a little something to keep them going on, because if anything the authoritarians – not only Erdogan, but other authoritarians as well – really care about their international image. So

they are affected, and they actually sometimes end up releasing people who are in prison. So the international community needs to speak up, and this is my expectation as well.

Thank you.

WARLICK: All right. Well, I think we'll open it up if anyone in the audience has a question.

Yes?

Q: For Jason, then back to Sanja. This important report comes at a time also when the large media and internet companies are accelerated in size so dramatically. We see the alignment of civil society and freedom seeming to be much more comfortable with the private sector, and are kind of looking to the private sector to help us navigate where to go. But at the same time, the sheer scale of Google and Amazon and Facebook and – is a flipside of that story. I'm curious where you would comment that this report leads into the OTT data streaming discussions at U.N., and how the future of mobile banking and data flows across government lines – you know, will we lean towards less regulation or more government control?

WARLICK: If you could also please introduce yourself?

Q: Well, I'm affiliated, in a sense, with Freedom House. We are supporters of Freedom House.

WARLICK: OK. Thank you.

PIELEMEIER: So I think that there's a number of components to your question. I think the issue of data flow restriction is a really concerning one to us at GNI. I think there are – I mentioned the trends around data localization – and also the broader issue of data protection, and how that could end up affecting when and where and how companies can share information even within their own sort of corporate systems when that information has to flow from one country to another. And again, I don't want to pass any judgment on, you know, data protection measures, which are sort of outside of our scope, but I do think governments need to be very concerned and very careful with how they develop restrictions on data flows because we have seen already the appeal that such restrictions have to authoritarian governments who want to use them as a pretext for their own information-control measures. And so whether the data restrictions are being designed to protect – to protect privacy or to – in furthering some sort of economic or trade priorities, I think it's just really incumbent on democratic governments to think very carefully about the way in which they approach those kinds of potential restrictions.

And I think, you know, really we would say that there needs to be kind of a presumption in favor of the free flow of data. And so we should only restrict it in those rare circumstances where there is an extremely compelling policy rationale, and enough safeguards built in around whatever system is being designed to ensure that that data restriction will not lead to the fracturing of the internet and cannot be used as a pretext for other governments to do what might essentially amount to censorship or surveillance.

WARLICK: Thank you.

Would anyone else like to comment? Sanja?

Q: About the large players, large actors. (Laughter.)

KELLY: Well, I think it's been interesting to observe how certain partnerships between civil society and the private sector have evolved. And I think in many ways that has happened because the private sector and the companies don't like restrictions and regulation. So then, as part of their business model, they actually don't want to see censorship and they don't want to be subjected to the policies that we see in China and Russia and other places. So it's in their interest to actually promote internet freedom. And for that reason we had seen, you know, some quite successful partnerships between NGOs and human rights defenders in the field, and then companies like Google and so forth, many of which are GNI members.

So I think on the flipside of that coin we've also seen that the products of some of these companies are actually, you know, spaces in which some of the key trends that we identified in this year's report, it's where they happen. And in many ways, then, these, you know, products and tools have become ways through which governments and malicious governments are able to manipulate and in some ways restrict freedom of expression.

So I think it's an interesting dynamic to observe and, you know, we'll see what the future brings. But I do want to highlight that civil society has had pretty successful partnerships with many of the companies.

WARLICK: Thank you. Do we have any more questions? I think we have time for one more.

If not, I'll just welcome all of you to give any final remarks you'd like to give.

KELLY: Well, thank you all very much for coming today and for taking an interest in this important subject. You know, I just want to highlight the importance of U.S. Congress and the Helsinki Commission in speaking out against the abuses because, I think as several of us have mentioned, that has proven to be critical in highlighting some of these cases, and in some instances the release of activists who were imprisoned for simply speaking out on democracy and human rights.

And I also want to echo what several of my colleagues up here said, that, you know, we have personally witnessed the success of the State Department programs in much of the world when it comes to protecting internet freedom, and not many governments and not many entities are actually funding this very important fight that is currently going on to prevent internet censorship from happening. So a lot of the partners that we see on the ground, a lot of the frontline human rights defenders, are really relying on the support from agencies such as the State Department and DRL. So I just want to underline the importance of supporting their important work through appropriations and other measures.

WARLICK: Thank you.

Anyone else?

ORUCOGLU: Completely agree, everything she said. (Laughter.)

WARLICK: Well, very well said, Sanja. And thank you so much to all of the panelists for being here and for all of you for coming. That concludes our briefing.

KELLY: Thank you. (Applause.)

[Whereupon, at 2:18 p.m., the briefing ended.]