THE PROMISES WE KEEP ONLINE: INTERNET FREEDOM IN THE OSCE REGION

HEARING

BEFORE THE

COMMISSION ON SECURITY AND COOPERATION IN EUROPE

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

JULY 15, 2011

Printed for the use of the
Commission on Security and Cooperation in Europe

[CSCE 112–1–7]

Available via http://www.csce.gov

U.S. GOVERNMENT PUBLISHING OFFICE

93–371 PDF WASHINGTON : 2015

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMISSION ON SECURITY AND COOPERATION IN EUROPE

LEGISLATIVE BRANCH COMMISSIONERS

HOUSE	SENATE
CHRISTOPHER H. SMITH, New Jersey, *Chairman*	BENJAMIN L. CARDIN, Maryland, *Co-Chairman*
JOSEPH R. PITTS, Pennsylvania	SHELDON WHITEHOUSE, Rhode Island
ROBERT B. ADERHOLT, Alabama	TOM UDALL, New Mexico
PHIL GINGREY, Georgia	JEANNE SHAHEEN, New Hampshire
MICHAEL C. BURGESS, Texas	RICHARD BLUMENTHAL, Connecticut
ALCEE L. HASTINGS, Florida	ROBERT F. WICKER, Mississippi
LOUISE McINTOSH SLAUGHTER, New York	SAXBY CHAMBLISS, Georgia
MIKE McINTYRE, North Carolina	MARCO RUBIO, Florida
STEVE COHEN, Tennessee	KELLY AYOTTE, New Hampshire

EXECUTIVE BRANCH COMMISSIONERS

MICHAEL H. POSNER, Department of State
MICHAEL C. CAMUÑEZ, Department of Commerce
ALEXANDER VERSHBOW, Department of Defense

THE PROMISES WE KEEP ONLINE: INTERNET FREEDOM IN THE OSCE REGION

JULY 15, 2011

COMMISSIONERS

WITNESSES

APPENDICES

THE PROMISES WE KEEP ONLINE: INTERNET FREEDOM IN THE OSCE REGION

July 15, 2011

COMMISSION ON SECURITY AND COOPERATION IN EUROPE
WASHINGTON, DC

The hearing was held at 10 a.m. in room 210, Cannon House Office Building, Washington, DC, Hon. Christopher H. Smith, Chairman, Commission on Security and Cooperation in Europe, presiding.

Commissioners present: Hon. Christopher H. Smith, Chairman, Commission on Security and Cooperation in Europe; Hon. Phil Gingrey, Commissioner, Commission on Security and Cooperation in Europe; and Hon. Steve Cohen, Commissioner, Commission on Security and Cooperation in Europe.

Witnesses present: Dr. Daniel Baer, Deputy Assistant Secretary for Democracy, Human Rights and Labor, U.S. Department of State; Dunja Mijatovic, Representative on Freedom of the Media, OSCE; Sec. David J. Kramer, President, Freedom House; Rafal Rohozinski, Senior Scholar, Canada Center for Global Security Studies and the Citizen Lab, University of Toronto; Ivan Sigal, Executive Director, Global Voices; and Dr. Charles Lee, Former Chinese Political Prisoner.

HON. CHRISTOPHER H. SMITH, CHAIRMAN, COMMISSION ON SECURITY AND COOPERATION IN EUROPE

Mr. SMITH. Commission will come to order, and good morning to everyone. And I want to welcome our very distinguished witnesses and all those who are interested in this very, very important topic of global online freedom.

Sadly, online censorship, surveillance and the intimidation of online speech is not restricted to countries where it is commonly reported, especially China, Vietnam and Iran. It is increasingly common in member states of the Organization for Security and Cooperation in Europe, broadly speaking, in Europe and the former Soviet Union.

With this hearing, we seek to draw the world's attention to the arrest of bloggers, to the blocking of websites, the surveillance and intimidation of peaceful political activists, to aggressive denial-of-service attacks and to violent intimidation by some OSCE member states. For example, Belarus is blocking social networking sites such as Twitter and Facebook and temporarily shutting down opposition Internet sites.

Turkey is set to require a mandatory nationwide Internet filtering system on August 22nd, unprecedented in scope in the OSCE space and compounding the already aggressive blocking of around 1,400 websites and broad restrictions on content. Kazakhstan, which already blocks a number of popular blogs and media sites, is also in the process of creating a national Internet, having recently decided that all .kz domain names will have to operate on physical servers within its borders.

No less disturbing is the violent intimidation of dissent in Russia. Though Russia does not aggressively censor terms or significantly block access to information on the Internet, as China does, it has its own crude but effective methods for controlling the Internet. Mafia thugs in league with the government beat people and instill fear in Russian bloggers and journalists. According to the Committee to Protect Journalists, quote, "Online journalists in Russia and throughout the region whose work appears on the Russian language Internet known as Runet, have faced physical intimidation, attacks and threats for far longer than has been widely noted in either Moscow or in the West."

In a report issued by OpenNet Initiative, the authors—one of whom is here with us today—concluded that Internet controls in the Commonwealth of Independent States have evolved, quote, "Several generations ahead of those used in other regions of the world." Runet controls are not only mirroring past oppression, the authors said, they're foreshadowing the future of Internet control worldwide. The prospect of the Internet environment deteriorating to that level is frightening, and surely is a call to action. At the signing of the Helsinki Final Act in 1975 President Gerald Ford stated that history will judge the signatories, quote, "Not by the promises we make, but by the promises we keep." This is as true now as it was then. All 56 OSCE states have agreed to respect their citizens' human rights and fundamental freedoms, including the freedom of expression. But some do not do so, and are not only not improving but even backsliding. And I do look forward to our witnesses today and what they can do—or what they will recommend as to how we might turn this around.

Turning to our first panel, I'm very pleased to welcome Dr. Daniel Baer, deputy assistant secretary at the Department of State for Democracy, Human Rights and Labor. And his portfolio includes Internet—the Internet Freedom Office.

Dr. Baer was sworn in as deputy assistant secretary on November 23rd of 2009. He—prior to joining the Department of State, Dr. Baer was assistant professor of strategy, economics, ethics and public policy at Georgetown University's McDonough School of Business, where he taught business ethics to MBA and undergraduate students. 2007 to '08 he was a faculty fellow at the Edmond J. Safra Foundation Ethics—Center for Ethics at Harvard.

In 2004 to '07 he worked at the Boston Consulting Group, was project leader and provided strategic advice to leaders in corporate government and nonprofit sectors. Dr. Baer has also worked in the Office of African Affairs, the Office of East Asian and Pacific Affairs, and the Office of Multilateral and Global Affairs. So he has a very, very wide swath of experience, and we are deeply grateful to have him here today to testify before the Commission.

So, Dr. Baer, please proceed.

DR. DANIEL BAER, DEPUTY ASSISTANT SECRETARY FOR DEMOCRACY, HUMAN RIGHTS AND LABOR, U.S. DEPARTMENT OF STATE

Dr. BAER. Thank you very much, Mr. Chairman. I appreciate your affording me the opportunity to address an issue with profound implications for the exercise of human rights in the OSCE region and across the globe, ensuring a free and open Internet. This hearing is emblematic of the Commission's strong defense and dedicated promotion of human rights principles enshrined in the core of the Helsinki Final Act and the Universal Declaration of Human Rights.

I value the opportunity to work with members of the Commission and your superb staff. The Commission's efforts greatly strengthen mine and that of Assistant Secretary Posner and our colleagues at the State Department as we work with other governments, civil society advocates and the private sector to defend and advance human rights and democratic governance.

Can I also take a moment to thank you for inviting the other witnesses you've welcomed here today. I'm thrilled to be here with my friends David and Dunja, both of whom I admire a great deal, and also with Mr. Rohozinski, Mr. Sigal, I feel honored to be in such great company. And I know that Mr. Lee will share his views too, and I'm glad for that.

Mr. Chairman, I endeavored in my written testimony to respond to your specific requests and to highlight key trends and concerns regarding a number of countries in the OSCE region, many of which you highlighted yourself, as well as to describe what we are doing institutionally within the OSCE to protect and advance Internet freedom. And I'd like to make just a few brief general comments here, and then take whatever specific questions you might have.

First I want to say a few words about why we, the United States, are committed to Internet freedom. The United States champions Internet freedom because it derives from universal and cherished rights: the freedoms of speech, assembly and association. An open Internet gives people a neutral platform from which to express their legitimate aspirations and shape their own destinies.

As Secretary Clinton has emphasized, the rights of individuals to express their views freely, petition their leaders, worship according to their beliefs—these rights are universal whether they are exercised in a public square or in an individual blog. The freedoms to assemble and associate also apply in cyberspace. In our time, people are as likely to come together to pursue common interests online as in a church or a labor hall.

As we all know, the Internet and other new technologies are having a profound effect on the ability to organize citizen movements around the world. And because repressive regimes understand this power, they are redoubling their efforts to control it. Recently in Vilnius, on the margins of the Community of Democracy's ministerial meeting, Secretary Clinton and I met with a number of activists, including several from the OSCE region, who spoke of the surveillance, hacking and harassment they face every day.

As Assistant Secretary Posner said earlier this week, "These are the acts of governments that fear their own people. In cracking down on the Internet, they expose their own lack of legitimacy." But speech is harder than ever to control in the digital age, and young people who have taken to the streets this year understand that it isn't pornography or pirating that's being suppressed; it's people and their legitimate demands for dignity and a say in the political and economic futures of their countries. As President Obama said in Cairo back in 2009, suppressing ideas never succeeds in making them go away.

The actions of these governments remind us of a basic truth. Governments that respect their citizens have no reason to fear when citizens exercise their rights. And governments that respect the rights of their citizens have no reason to fear a free Internet. Of course, repressive governments are also missing out. The Internet can be a force for social and political stability if governments use it as a way to better communicate with their citizens and to serve them in an open and transparent fashion.

The Internet offers an early warning signal for public discontent, and therefore a way to address grievances before they erupt into protests. As Assistant Secretary Posner said, governments should not shoot the instant messenger. They should address the underlying problems that cause citizens to lose faith in their governments and in the future.

Mr. Chairman, we are not cyberutopians who believe that the Internet is the magic answer to the world's human rights problems. Technology does not change the world, people must. And we must not forget that calls for freedom still spring from human dreams and resonate in human hearts even if they are shared by keystrokes and text messages. That's why we take a person-centered approach through our diplomacy, through direct support for embattled activists worldwide—we are helping people stay one step ahead of the censors, the hackers and the brutes who beat them up or imprison them for what they do online.

Since 2008, thanks to Congress' support, we have committed $50 million in direct support for activists on the front lines of the struggle against Internet repression. By the end of 2011, we will have allocated $70 million toward these efforts. Our programming responds to the most urgent priorities we hear from activists on the ground, including embattled democracy and human rights activists from the OSCE countries.

We're committed to a free and open Internet because it follows from our commitments to fundamental freedoms and universal values. These commitments, like all human rights commitments, are part of who we are; part of, as the title of this hearing suggests, the promise we keep. And, of course, it's also part of the promises at the center of the OSCE.

Mr. Chairman, as you know, the OSCE was the first regional organization to recognize that respect for human rights, pluralistic democracy and the rule of law are prerequisites for a lasting order of security and prosperity. And the OSCE was the first regional organization to acknowledge the vital importance of civil society. The Helsinki process must continue to be a pioneer for human dignity, civil society and democratic government in the digital age.

Challenges to Internet freedom in the OSCE region are illustrative of the issues we are addressing across the globe. Mr. Chairman, as you know, in the past the Helsinki process was a major international platform for defending the citizens expressing dissenting views, the samizdat, and for protesting the jamming of radio broadcasts. Today email, social networking and text messaging are new forms of samizdat, as well as indispensable tools of commerce, education and global communications.

As the United States has done since the inception of the Helsinki process, so too in this new century we stand with those in the OSCE region who seek to peacefully exercise their fundamental freedoms and promote and protect human rights including via new technologies. The United States will take every opportunity to work with the Lithuanian chair, the EU and other participating states and civil society to ensure that the OSCE sends a clear message from Vilnius on Internet freedom. If I were to distill that message into a Tweet to the world, it would be: Enduring freedom, new apps.

Mr. Chairman, when he—as you said, when he signed the Helsinki Final Act 35 year ago, President Ford famously said that "History will judge this conference not by what we say here today but by what we do tomorrow, not by the promises we made but by the promises we keep." He was right then, and his statement is even more true today. In this digital age, keeping our promises greatly depends on ensuring that the Internet is open and free.

Thank you, Mr. Chairman, and members of the Commission. I'd be glad to take your questions.

Mr. SMITH. Mr. Baer, thank you very much for your testimony, and for your leadership. This is certainly one of the cutting edge areas of human rights, and the alternative, the suppression of those rights by tyrannies—tyrannical governments and dictatorships. Let me ask you just a few questions, if I could.

We know Belarus—and we've had reports that in Belarus the Chinese have cyberpolice, and the experts in controlling the Internet have shared best practices there so that Lukashenko can better repress the dissidents and the democracy activists. What kind of information do we have regarding that kind of collaboration, not just in Belarus but in, perhaps, some of the other more repressive regimes in the OSCE region?

Dr. BAER. Thank you, Mr. Chairman. I think what you've highlighted is what we see as a growing trend in the last few years, which is that, as you said, there's an increasing sharing of what we might call worst practices—[chuckles]—in terms of Internet repression. And as governments are sharing—as nefarious governments are sharing their methods for repressing online speech or assembly, they're also developing new ones. They're innovating and sharing, which is—which makes it even more challenging.

And so certainly we are seeing—we do believe that governments are sharing techniques. And, you know, we are trying to respond in kind. We're trying to make sure that we are staying in touch with people on the ground and that we're listening to the new threats that they're seeing. You mentioned Belarus. We know that in Belarus there, as you talked about, there have been denial-of-service attacks, there's monitoring, there's shutdowns—it's a kind

of confluence of a number of Internet threats. And we're listening to people on the ground there and elsewhere and trying to make sure that we're providing them the support they need.

Mr. SMITH. But are the Chinese—is Beijing providing the all-important expertise to help Lukashenko and the others?

Dr. BAER. Without—I'd be happy to brief you in private on particular country concerns, but I think that it is fair to say that there is information sharing going on between a number of countries in terms of how to—how to limit online speech and activity.

Mr. SMITH. Including China?

Dr. BAER. I would expect that there's information sharing going on between countries that limit the Internet.

Mr. SMITH. OK. Let me ask you—several years ago I held a hearing that lasted some eight hours—it was the longest hearing I've ever chaired—we had Google, Cisco, Yahoo and Microsoft testify. And frankly, at the time, all four of those large companies were totally reluctant and enabling of—reluctant to share information and enabling of the Chinese dictatorship when it comes to repression via the Internet. Google since has come around to some extent, and I think a large extent. They now support the Global Online Freedom Act. Yahoo actually moved personally identifiable information when they set up shop in Vietnam, and they put that out of reach of the "Internet police," if you will, in Hanoi.

And Microsoft and Cisco, however, seem to be moving forward unperturbed by how their enabling of a dictatorship has led to arrests. And in the case of Cisco they're selling capabilities that, you know, the Interpol and the FBI—you know, state-of-the-art police techniques, sharing of information, routers, it's just—it's just extraordinary—policenet which gives the secret police extraordinary capabilities. And I'm wondering if you're seeing those companies and others exhibiting the same kind of enabling of dictatorship in the OSCE space?

Dr. BAER. I think—I think you're right to highlight the importance of private companies in the Internet freedom conversation. Most of the Internet is made up of private assets, and obviously most of us use the services that companies provide; that's how we access the Internet. I think that what we've seen in the last few years, as you rightly point out, is an evolution in the way that companies are thinking about this. I think that increasingly companies are realizing—as we should never forget that companies are made up of people, and people who often when they understand the nature of the consequences, perhaps unintended consequences, of decisions they make, can manage around them.

And so, you know, one of the initiatives that we're quite keenly following is the Global Network Initiative, which is made up of Microsoft, Yahoo and Google. The director of the Global Network Initiative is here with us today. I saw her in the audience before I came in. You know, that's meant to be a way for companies to come together and talk about what a principled approached to doing business in this space looks like, and to make commitments to do so. And I think we see that as a promising way forward, both because it establishes commitments, but it also provides a forum for companies to share, quite practically, the challenges they're facing.

So, you know, you brought up the issue of storing data outside of—outside of Vietnam. You know, that was a lesson learned from the Shi Tao case. You know, storing data—where you store data matters. And so that's a practical conversation that companies can have. I think that, you know, this is an evolving conversation. I think it's one that's important; we should keep our eye on. I think that there are a number of companies that are—and actors within companies that are taking a lead on this and who recognize that this is a conversation that they have to be a part of.

Mr. SMITH. Let me just ask two final questions then yield to Dr. Gingrey. The—I mentioned earlier—or you mentioned as well, with regards to obscenity and issues of that kind, you know, when—and I will be reintroducing the Global Online Freedom Act shortly—the previous versions and any version makes it very clear that we're talking about nonviolent political speech, nonviolent religious speech, conscience but not obscenity—as even the Supreme Court has said—is not protected speech. And I think you would agree with that.

But if I—how would you recommend we deal with the hate speech, especially the anti-Semitic speech that is very often generated in this country? I mean, I do believe passionately in free speech, but there are lines that need to be drawn and, you know, some of the anti-Semitic speech that I've seen on the Internet is just without parallel—the hatred and the animosity towards Israel and Jews in particular. Do you have any thoughts on that?

Dr. BAER. I appreciate your raising that, and I think it's one of the places that we have room to continue and bolster the conversation going forward. I work very closely—my office is next door and I was sworn in on the same day as and with—Hannah Rosenthal, our special envoy to monitor and combat anti-Semitism. And we've talked about this several times, and how we can really foster a conversation that reckons with the fact that a commitment to free speech entails also a commitment to speak out when hateful speech is put into the public sphere, to defeat it through the force of argument and to express our disapproval of those kinds of utterances.

I think that there is a—there's obviously—the challenge that arises, as you point out, is that we want to be very careful about any limitations on speech because we know that while well-intentioned actors may use them well-intentionedly [ph], other actors will exploit those as an excuse to limit the kinds of speech that ought not be limited. And so that's the challenge that we face in this conversation.

And I think we remain committed. Hannah has been pounding the pavement, traveling the world speaking out against it. We remain committed to fostering a conversation that deals with hate speech and recognizes it as an onerous and terrible thing.

Mr. SMITH. I would just add, many of our colleagues in the European countries, including France and a number of the other countries, you know, are very concerned about the anti-Semitic speech and are befuddled as to why we can't make a clear distinction between grossly hateful speech and freedom of speech.

Two final questions—Internet-restricting countries—if you were to say which countries in the OSCE space are the worst, if you could, tell us what those countries are. And with regards to the

money that has been appropriated to pierce the firewalls, in particular, the firewall in China, the Falun Gong, as you know, has developed an extraordinary capability to pierce that firewall so that people can access the Internet without fear of government intrusion, almost, for want of a better word, an unfettered access to the Internet.

Why hasn't that money flowed to them, since they have an off-the-shelf capability? I mean, I spent the better part of three hours six months ago with some of their practitioners, some of their technological people—tech people, and I was amazed. And I understand from peer reviews that it does work. Will that money indeed flow to them so that they can do that work?

Dr. BAER. On your first question, in terms of Internet-restricting countries, it's a difficult ranking to make because of the dynamism of the way that threats are evolving. So whereas in one country, you may have extraordinary legal restrictions—you mentioned the new—the pending new filtering regime that is set to take place in Turkey—in another country, you may have threats that are good, old-fashioned brutality mixed with online activity.

So, you know, we're concerned about actions in Russia to punish bloggers or things like that. I mean, obviously, Belarus continues to be a prime concern. But you mentioned—the countries that you mentioned in your opening statement, I would say we have concerns about all of them. All of those countries are areas of concern, and in different ways.

And one of the things—one of the challenges not only in our policy, but also in our programming—and I'll talk about our programming now—is to respond to the specific context of each country. You know, that's why we keep in such good touch with people on the ground, because what—the tools that are needed, the supports that are needed in one place may not be the same as the tools or supports that are needed in another. And we're working very hard to deliver customized supports to the people on the ground.

Mr. SMITH. But if you were to say, what are the top five or the worst five, I should say, just so that we can better hone our focus?

Dr. BAER. You know, State Department guys get in big trouble when we make ranking lists—[chuckles]—on the fly. I think I would say the handful of countries that you mentioned in your opening statement would certainly pass muster as a top five.

In terms of your question about the programming, first of all, let me reiterate our thanks for Congress' support for Internet-freedom programming. We see that as essential to the United States' global push to advance and support Internet freedom.

The way that we approach this is to take a venture capitalist-style approach. Part of the challenge, again, is the fact that whereas five, ten years ago, there was really only one salient threat to Internet freedom, and that was blocking, increasingly what we're seeing is—and the cases of Belarus and others are prime examples—is that it's not just blocking; it's the fact that people can't associate or communicate securely. It's the fact that their websites get attacked by nefarious actors and taken down. And so we need a range of tools.

And we also need to make sure that the people on the ground know how to use them and know how to use them safely so that

they're not putting themselves or others at risk. So our portfolio of investments includes a range of tools, including circumvention technology, which you brought up, as well as other tools to help people communicate securely and to keep their websites up, et cetera, as well as the training or the underground railroads that distribute those and give people the kind of cyber self-defense training that they need.

In terms of the specific tool that you brought up, it is one of the tools in our portfolio, but we don't comment publicly on our grants, because we want to give our grantees the discretion to do so. That has been publicly brought up by the grantee, and I'd be happy to—I have met with your staff in the past, and I'd be happy to meet again to talk about the upcoming round of grants. I think you'll be quite pleased by the portfolio.

Mr. SMITH. Mr. Gingrey.

HON. PHIL GINGREY, COMMISSIONER, COMMISSION ON SECURITY AND COOPERATION IN EUROPE

Mr. GINGREY. Thank you, Mr. Chairman and Dr. Baer. I—the old saying comes to mind: It's easy to recognize a speck in someone else's eye, yet we might indeed have a plank in our own. Let me ask you this question: We've had some hearings—in fact, recently—on Internet security in this country, more in regard to advertisers' cookies and tracking people and off of social networks and websites, et cetera, and how we should really strike that balance.

And the United States itself has certainly faced some recent criticism for its push to obtain personal information in the private correspondence, as I said, of social media users in the name of things like combatting terrorism, pursuing criminals or even to serve legal notices to our citizens.

Does the government's reach in these areas deter users in this country from freely utilizing the Internet services? And are not these intrusions affecting freedom of expression on the Internet in the United States?

Dr. BAER. Thank you very much, Congressman. I think that the question you pose reflects what we have long acknowledged, which is that there are challenges to preserving a free and open Internet and making sure that we're taking care of security concerns, law-enforcement concerns and harnessing the full commercial power of the Internet.

Just because they're challenges doesn't mean they're unsolvable. There are challenges in the offline world to figuring out how to make sure that we are permitting companies to do business and innovate and develop new ideas as well as making sure that consumers are protected, et cetera.

So I don't think they're necessarily new challenges, but they're certainly challenges. I think, you know, that the secretary in her Internet-freedom speech this year, in February, laid out a number of those tensions and the tensions that we face in crafting policy. And, you know, in some sense it's even harder in this sphere because the technology evolves so quickly that it's at a hyper speed. And so you have to be incredibly careful in the way that you respond—the policy responds.

And I think that's why it's so important that we have guiding principles, that we have our commitments to free expression, that we have the commitments that are in our Constitution and the commitments to fundamental freedoms that are in the Helsinki Final Act and that we don't lose sight of those as we attempt to craft policy to manage the commercial and security aspects of the Internet.

Mr. GINGREY. If you could maybe give us some specifics what the State Department overall is doing within OSCE to combat the attacks on freedom-of-speech association on the Internet. You have in general said that in response to some of these countries that Chairman Smith talked about, that you're ready, willing and able, from the State Department perspective, to assist. But what specifically, if you could give us some—

Dr. BAER. Well, obviously, we have—specifically, we have programs and we have diplomacy with the OSCE member states. But within the OSCE, our ambassador, Ian Kelly, raises these issues in the permanent council on a regular basis. And we—in the lead-up to the Astana Summit last year, we worked very hard to develop language that we hoped would be—would be part of the action—the plan of action coming out of the summit.

As you know, there was no plan of action adopted at Astana. But we are going to work again this year in the—in the run-up to the upcoming ministerial in Vilnius in December to try to make sure that a statement affirming the application of the same fundamental freedoms that have applied offline to the fact that they apply online, and not just freedom of expression, but of assembly and of association as well—we're going to try to get that language into the outcome document from the Vilnius ministerial as well. And we'll continue to raise these issues as we can within the OSCE.

I would say that I think that one of the great assets of the OSCE in terms of Internet freedom is the next witness that you'll hear from. Dunja's work has been—first of all, she never stops. She's everywhere, all the time, working with governments. I see her at blogger conferences. I see her all over the place, and we work together very well. And I've really appreciated the work that she's done. I think that she's a clarion call. She—her reports and her statements really do call out the areas in which we should all be focused within the OSCE region. So I would point to her as one of the successes of the OSCE and Internet freedom.

Mr. GINGREY. Yeah. Well, it seems to me—and this is—certainly, I'm not being critical of it, but it sounds to me that it's just a matter of expressing in a formal manner our righteous indignation over some of these things and shining the light of day on activities and hopefully embarrassing the bad actors into behaving.

But in regard to real specifics, any kind of a hammer, it really doesn't sound that you've described one to me. And maybe it's not needed, but it seemed like to me—[chuckles]—it would be very helpful if we had that.

Dr. BAER. I think there are—I think you're right. I think there are opportunities to operationalize the commitment to Internet freedom in other aspects of the OSCE in ODIHR. You know, there will be opportunities on the ground in field offices, et cetera.

But as we look back at the history of the OSCE, I think in many respects, the hammer—the hammer that the OSCE has is the incontrovertible, undeniable truth of the principles on which it's founded. And so I think that to the extent that all of us continue to call out violations of those principles, that is the hammer. And it's not ineffective.

Mr. GINGREY. Yeah. I would agree with that. Thank you very much, Dr. Baer. And Mr. Chairman, I yield back.

Mr. SMITH. Mr. Cohen.

HON. STEVE COHEN, COMMISSIONER, COMMISSION ON SECURITY AND COOPERATION IN EUROPE

Mr. COHEN. Thank you, Mr. Chairman. Let me ask you just a couple of questions. After the Arab Spring, where the Internet was credited with so much of the Egyptian revolution, have we seen more restrictions on Internet activity in other places around the country—around the world?

Dr. BAER. It varies. In some places, yes, although we don't—it's hard to attach causality to that. You know, after the Arab Spring, when the stories were written, many of them were breathless about the fact that the Internet had played a major role. And to me, I've said, you know, you've got a bunch of 20- and 30-somethings—and the whole range of society, but a lot of 20- and 30-somethings that the stories were focused on. If there were stories about them doing something that didn't involve the Internet, that would be the story. I mean, these days, the Internet is so much woven in to daily life and indeed, into the story of human rights, that it's necessarily part of the story.

And because of that, I mean, I think we do see that when—that other governments are certainly paying attention. They are—whether or not they're taking action, they're paying attention to what's going on.

Mr. COHEN. So you haven't seen a spike?

Dr. BAER. I mean, I think we've seen certainly increase—we were worried about the trend in China in the last six months. There's been increasing extra-judicial detention of lawyers, et cetera, crackdowns on religious groups, et cetera. But I don't know whether we would causally link that to the Arab Spring.

Mr. COHEN. You co-opted the chairman's four or five countries. What would be the next four or five countries? [Laughter.]

Dr. BAER. I'd like to take that question.

Mr. COHEN. You'd like to take that question?

Dr. BAER. I'd like to take that question and come back to you with a considered answer.

Mr. COHEN. OK. And none of the countries that he mentioned are—they're all within our area of—our jurisdiction. Cuba and China weren't mentioned. Is that the reason? Because Cuba and China I would think would be at the top of any list.

Dr. BAER. Right. Oh, sure. I mean, China has the longest history of Internet restrictions. Cuba has significant restrictions. Vietnam has significant restrictions. So if we're looking outside of the OSCE region, you know, there are a number of others we could—we could—[inaudible].

Mr. COHEN. What's—in Turkey, what we're concerned about—I didn't realize they had this situation, their 138 words. George Carlin would probably know them all.

Dr. BAER. Right, he only knew seven—he only needed seven. [Chuckles.]

Mr. COHEN. That's right. How many do you know? And what are they, translated into English?

Dr. BAER. The collection of words is—each of the words is meant to be—the stated intent is to filter out obscene content. But obviously, 138 words would be—is a large number of words. And we have serious concerns over it, that as well as the law that authorizes the takedown of websites that could possibly be implicated in one of seven or eight crimes, and then the fact that Turkey has blocked over 5,000 websites. There are serious concerns with the condition of Internet freedom in Turkey and of media freedom, more generally.

I was talking with Dunja before I sat down today, and their latest numbers are that over 70 journalists are in prison there. So we have serious concerns, and we'll continue to raise them with the Turkish government.

Mr. COHEN. And is—are there particular concerns about references to the PKK or to Ataturk?

Dr. BAER. My understanding is that some politically sensitive topics are—political sensitivity is the rationale for blocking certain websites.

Mr. COHEN. All right, so Erdogan is just as concerned about Ataturk as the other party?

Dr. BAER. Certainly there have been examples of material that involved Ataturk that has been blocked.

Mr. COHEN. I thank you for your time and I look forward to your answer on the next four or five countries. I yield back the remainder of my time.

Dr. BAER. [Chuckles.] Absolutely.

Mr. SMITH. Dr. Baer, thank you very much for your testimony. If you could get back to us with some of those follow-ups as quickly as possible, including the first five and the next four or five, it would be very helpful. Again, it helps us to focus our resources on the most egregious violators, so I do thank you for that.

And I do hope as well that your office will look very carefully at the Global Online Freedom Act and hopefully endorse it. I know that it has to go through a lot of check-offs for that, but you know, it is an idea whose time has come and would give you the ability to really hold countries to account and to designate—the designation "Internet-restricting country" would trigger a number of very important policies towards that country. So I do hope you'll take a good look at that, as well.

Dr. BAER. Thank you, Mr. Chairman. I'm in active and very fruitful conversations with your staff and will continue to be, so—

Mr. SMITH. Dr. Baer, thank you very much and we really appreciate your leadership.

Dr. BAER. Thank you.

Mr. SMITH. I'd like to now ask our second panel—matter of fact, we're going to have to combine panel two and three, a little change of procedure, because we do have a large series of votes that will

probably take over an hour and a half to complete on the floor of the House. And I would not want to inconvenience our witnesses more than we probably already will.

So let me ask, if I could start with Dunja Mijatovic, who's the OSCE representative on freedom of the media. She is an expert in media law and regulation and in 1998 was one of the founders of the Communications Regulatory Agency in Bosnia. She helped create a legal, regulatory and policy framework for the media in a complex postwar society.

She also involved—was involved in setting up self-regulatory press council and the first free media helpline in Southeast Europe. Ms. Mijatovic has flown all the way from Vienna to join us at this hearing today. The timing of her appearance is fortuitous, as her office just released a report detailing the legal provisions and practices related to freedom of expression, the free flow of information and media pluralism on the Internet in the OSCE region. Look forward to her testimony.

Then we'll be hearing from David Kramer, who's the president of Freedom House and former assistant secretary of state for Democracy, Human Rights and Labor as well as a former Helsinki commissioner, often sitting right here, asking the questions, not giving answers. So I thank him for being here.

And without objection, all of your very, very extensive bios will be made a part of the record. Each of you are highly distinguished and have great resumes that speak to a broad range of issues, including the one at hand.

We'll then hear from Rafal Rohozinski, senior scholar, Canada Center for Global Security Studies and the Citizen Lab at University of Toronto. He was also one of the lead authors of an important report on Internet freedom in the OSCE region called "Access Control as Part of the Open-Net Initiative."

Next we'll hear from Ivan Sigal, executive director of Global Voices, a virtual community of more than 300 bloggers and translators around the world who work together to publish reports from blogs and citizen's media everywhere with an emphasis on voices that are not ordinarily heard on the international media mainstream.

And then we'll hear finally from Charles Lee, a Falun Gong practitioner and former Chinese political prisoner, who spent from 2000 to 2003—2003 to 2006, I should say—was unjustly incarcerated in the laogai in China and suffered gross indignities to his person while he was held there. He believes that technology sold by Cisco is violative [ph] of the law and has filed a lawsuit against Cisco. He also—and he and others have been briefing members on Capitol Hill, including Frank Wolf and many others about a huge breakthrough in technology that pierces the firewall in China, but he also has spoken out about how China is sharing its worst practices with the OSCE region.

So I'd like to now, if I could, begin with Ms. Mijatovic, if you could proceed as you would like.

DUNJA MIJATOVIC, REPRESENTATIVE ON FREEDOM OF THE MEDIA, OSCE

Ms. MIJATOVIC. Thank you, Chairman, members of Commission. I'm honored to be here again, actually the second time since I was appointed. I appreciate this invitation very much, particularly in light of the report that you just mentioned we published, and I would like also to mention that the report was commissioned by my office, but the author of the report is distinguished Professor Yaman Akdeniz from Bilgi University in Istanbul.

For centuries the right to be heard has been seen as the cornerstone of democracy. We can all agree with this. It enables other rights to exist, and in the age of a borderless Internet, the protection of a right to freedom of expression regardless of frontiers takes on a new and more powerful meaning.

The argument for freedom of expression on the Web is a double-edged sword. And it's a hotly debated issue nowadays. On one side, it is upholding civil rights and, on the other, allowing governments and censors to question people's own judgments. The Internet at its best is a cyber-experience on every single topic imaginable from personal pages detailing the life and thoughts of a schoolchild to multinationals promoting their wares online. Governments, however—too many governments, I would dare to say, within the OEC region— have already begun to impose controls on the Internet, threatening the potential of this new medium.

As an international community of users and providers of information, we are at a dramatic turning point. The Internet will change the way people live. It offers extraordinary opportunities for enhancing creativity and learning for trading and relating across borders, for safeguarding human rights, for realizing democratic values and for strengthening pluralism and cultural diversity. The change holds promise, but also holds challenges for all of us.

One of the major challenges is to confront ways in which to spread access through the Internet so that the whole world can benefit rather than creating gaps between information rich and information poor. The exploration of cyberspace can be a civilization's truest, most challenging and also very controversial calling and adventure. The opportunity's now before all of us to empower every person to pursue this opportunity and not to restrict and to suppress free speech. However, the exploration of cyberspace brings both a greater opportunity and in some ways more difficult challenges than any other previous human adventure.

National actions must fit into pattern of international understanding or in the best ways in which to deal with the Internet content issues. Just for reminding us—and I will use United States as an example—the Internet is the fastest growing medium ever. While it took your country 38 years to reach 50 million radio users, 10 years to reach the same number of television viewers, in only five years in the case of the Internet. So we can also see this, you know, how quick we are moving in this adventure.

We already live in digital age, a time in which we can create truly democratic cultures with participation by all members of society and, in only a few years from now, this participation will virtually include most of world citizens. So despite the progress we see, some challenges and preconditions remain. The first one is

surely, as I mentioned at the beginning, access to the Internet. Without this basic requirement, without the means to connect and without an affordable connection, the right to freedom of expression and freedom of the media become meaningless in the online world.

The second one is restricting this freedom and restricting free flow of information which is also one of the basic OSCE commitments, and I would even go so far to say that the free flow of information is, in my view, an oxygen of cyberspace. If we stop it, the Internet cannot breathe. It becomes a meaningless tool.

Why do certain governments try to block, restrict and filter this flow? I'm asking myself by doing this job all the time. To protect us from terrorism, child pedophilia, human trafficking, and other forms of threats and make our societies more secure? All mentioned are legitimate reasons that should not be challenged by anyone. But to protect us from criticism, satire, provocative and shocking comments, differing views, tasteless and sometimes controversial content—for that they do not have our permission. We as the citizens that voted for them never asked or obliged them to shape our minds and opinions. And again I repeat: In too many OSCE participating states this is happening on a daily basis. I'm seeing this every day, but do I travel—during the time I travel to participating states, talking to the civil society, but also talking to the authorities that are informing me about their attempts to restrict and to suppress further.

There is no security without free media and free expression, and no free expression and free media without a security. These two terms should come hand in hand and not fight each other, like we see in so many parts of the world. And there is no better place, at least in my modest view, to discuss and fight for both in the OSCE—than the OSCE. Security and human rights are both at a heart of Helsinki Act and our standard commemorative declaration as well as the OSCE principles and commitments that we share. So why do we still struggle? We can also ask ourselves, and why are we so afraid from words and where does this fear come from?

Our common goal achieving the promises we made should be a free, open and safe Internet. Very simply, when services are blocked or filtered, users of Internet platforms everywhere cannot be served effectively. Today, many governments disturb the free flow of our online information. Popular tactics include incorporating surveillance tools into Internet infrastructure, blocking online services, imposing new secretive regulations and requiring licensing regimes. Since my time is limited, I will finalize my statement without mentioning particular countries, but I'm ready to reply to any of your questions.

I have a brief recommendation and a comment at the end. I would like to stress once again that blocking access to Internet or banning certain content has proven to be totally ineffective. I call it—maybe too bluntly—when I talk to the authorities within the OSCE region: I call it a lost battle. Even by trying to establish regionalized networks, it will not be possible to gain full control over the communication exchanged and information shared on the Web. Any attempt to hinder the free flow of information to disproportionally restrict the right to free expression, to block dissenting opinion, or to prevent critical voices from being heard will

prove to be short-sighted because a free Internet and independent media are a means and not an end in itself.

Finland and Estonia are countries that should be followed, in my view. They introduced pioneering legislation which established the access to Internet as a constitutional right. In France, the constitutional court ruled in a similar way, but they have still a long way to go.

In order to pay tribute to the unique contribution the Internet has given to participatory democracy, to freedom of expression and to freedom of the media, it is only fitting to enshrine the right to access the Internet on exactly that level where such rights belong, as human right with a constitutional rank. Perhaps the time is ripe to turn a new page in the history of fundamental rights and establish access to Internet as universal human right. It would be promising indeed to see the number grow of the OSCE participating states which recognize this principle on a constitutional level. The Internet is a fantastic resource that has fundamentally changed our societies for the better. We should not be afraid of it. It will continue to have a positive impact if we allow it. The lesson is simple: The Internet must remain free and safe. Thank you very much.

Mr. SMITH. [Off mic]—thank you very much for your testimony. I really appreciate it. We all do, and your work and your report.

I—we do have a series of 16 votes followed by two additional votes. Without objection, all of your prepared testimony is going to be made a part of the record for the hearing record. Technically we will have to briefly go to a briefing, and Mark Milosch and Shelly Han, our policy—senior policy adviser and chief of staff, will chair the—that part. We will try to come back when there's a motion to recommit. We should have about 25 minutes, but there are 16 back-to-back votes.

No one can ever predict this, believe me, or else we wouldn't have done this at this particular time. So I apologize for that inconvenience to all of you, but —and I can assure you that all of us will read your testimonies very, very carefully and react to them because you provide us a blueprint for going forward as well as information in terms of where we are right now. So thank you so much, but I will though ask Secretary Kramer if he could begin his testimony, and then we will then become a briefing; but all of your testimonies are part of the official record.

Secretary Kramer, please.

SEC. DAVID J. KRAMER, PRESIDENT, FREEDOM HOUSE

Sec. KRAMER. Mr. Chairman, thank you very much for the opportunity to be here. It's always a pleasure to appear before you and the Commission.

In the interests of time, let me just very quickly say the last time I appeared before you was before an HFAC subcommittee, and we were talking about Belarus. And despite the gravity of the situation there and the pressure and attacks that protestors and civil society activists, journalists and others face on a daily basis in Belarus, I have to tell you, Mr. Chairman, I am more optimistic that that situation is going to change for the better before too long. I think Alexander Lukashenko's days are numbered. He is in the

gravest situation he's ever faced, and I don't think he's going to be able to come out of it.

So many thanks to you in particular, Mr. Chairman, for your sponsorship and support and leadership on the Belarus Democracy Act that passed the House last week, an extremely important piece of legislation, and very much hope that that will move through the Senate, and get the signature of the president very soon. So many thanks for that.

Mr. SMITH. Please share that with Orest as well because he has done the lion's share of—[inaudible]

Sec. KRAMER. I do on—I do almost on a daily basis. Absolutely.

Mr. Chairman, my organization, Freedom House, produced this report, "Freedom on the Net 2011," in April of this year. It's the second time we have done this report, and in this report we looked at 37 countries around the world, and in the OSCE region, we looked at 11 countries.

You and your colleagues had asked about some rankings of countries. This is not a comprehensive list of OSCE member states, but I think it does give you some sense of where countries stand. There are some countries that stand out.

As Dunja mentioned, Estonia is at the top of the list; the United States is not too far behind; Germany, the U.K. and Italy all stand in the free category. We rank countries as to whether they're free, partly free or not free in—when it comes to Internet freedom.

In the partly free category—and this is based on their scores, so I'm going from the best scores down to the lowest scores—would be Georgia, Turkey, Azerbaijan, Russia, Kazakhstan, and then, in the very last category of not free, would be Belarus, not surprisingly and unfortunately.

Mr. Chairman, Freedom House produces this report, but it also engages in activities in promoting Internet freedom, across a range of activities, in helping with censorship-circumvention technologies in countries where the Internet is restricted. We build indigenous capacity to promote and support the use of anti-censorship tools in highly repressive environments, provide technology to developers and work with international bodies, including with the OSCE, and it's a real privilege for me to be here this morning with the high representatives for special—for media freedom in the OSCE region.

There are—it is not surprising, I think, that many of these governments that I listed do their best to try to suppress Internet freedom just as they do with other kinds of freedom and other kinds of media. Belarus, as I indicated, is at the top of the list in trying to crack down on Internet freedom, and the Internet is simply the latest frontier for which Belarusian authorities try to restrict freedom in their country.

But Belarus is not alone. The other—a number of the other countries that I mentioned are equally engaged in activities and efforts to crack down on Internet freedom. Some of them just simply haven't kept up with the Internet and communications revolution sufficiently to be able to do so, but I think if we look at their efforts in cracking down on TV and radio and newspapers, it is not a stretch to assume that the Internet is very much on their radar screen and will be the next target of their efforts.

It is very important to defuse the impact of the latest online calls to protest—or rather in an effort to defuse the online calls to protest in places like Belarus, we see these governments impose restrictive and repressive measures to spam online threads about protests, misuse hash tags, create fake Twitter accounts to undermine actual activists, engage in all kinds of activities; so they're both using the Internet and they're also trying to crack down on it, and I think that's something we very much have to keep in mind.

My testimony goes into a number of countries. I already offered you the rankings. I do want to highlight and mention the work that the State Department is doing including when I was there at the State Department and funding became available to promote Internet freedom. I commend the Obama administration and DRL in particular for the work it's doing in this area. And also as Dan Baer said, I do want to acknowledge Ian Kelly, our OSCE ambassador in Vienna for the work he has done and for his outspoken record in stressing the importance of Internet freedom.

I think, in the interest of time, I will forego going through the details of each of the countries, but in my written testimony, I go into more detail on the cases of Belarus and Azerbaijan, Russia, Kazakhstan and Turkey, which are reflected in our Internet freedom report. I do also refer to one country that is not reflected in our report, and that is Hungary in light of the concerns that have been expressed about a media law that was passed last year in Hungary and is being implemented this year and the potential impact that that could have on Internet freedom as well.

So, with that, let me close there in the interests of yielding time to my fellow panelists. Thank you.

Mr. MILOSCH. Thank you very much, Mr. Kramer. As the chairman said right before he left, we are now in briefing mode. We'll continue and hope that he will be able to return when they're debating a motion to recommit. We will proceed now to Mr. Rohozinski.

RAFAL ROHOZINSKI, SENIOR SCHOLAR, CANADA CENTER FOR GLOBAL SECURITY STUDIES AND THE CITIZEN LAB, UNIVERSITY OF TORONTO

Mr. ROHOZINSKI. Thank you very much. First of all, I'd like to thank the Commission for the opportunity to appear and testify at today's hearing, which comes at a particularly important moment. The Internet has precipitated perhaps the fastest and largest expansion in rights in human history. And yet we find ourselves at a constitutive moment where our actions, our leadership, can lead to two opposing outcomes: one of which promises a future of greater freedoms and transparency; the other threatens a return to a darker, more authoritarian past.

My name is Rafal Rohozinski. I'm a senior scholar at the Canada Center for Global Security Studies, and CEO of the SecDev Group and Psiphon, Inc. For the past 10 years, I've been a principal investigator of the OpenNet Initiative, a collaborative international research project between the University of Toronto in Canada, Harvard University, Cambridge University and the SecDev Group

which has studied and documented the practice and policy of Internet censorship and surveillance worldwide.

We have published more than two dozen case studies and reports and are currently publishing our third volume that documents censorship practices in over 70 countries worldwide, including all of the members of the OSCE. The OpenNet Initiative has created the largest and most comprehensive profile of how countries seek to shape access to cyberspace through a combination of regulation, repression and technical means.

Now, just over 65 years ago, Winston Churchill warned an American audience of the dangers of an Iron Curtain falling across Europe, casting a shadow of authoritarianism and depriving citizens of their basic democratic rights. Churchill spoke in 1946 at a time when the United States stood as a(n) uncontested global power. He urged the creation of norms and institutions that would safeguard freedom and actively oppose the forces of authoritarianism. For Churchill, the end of World War II was a constitutive moment, when the choices made by the victorious allies would have enduring consequences for the causes of freedom in Europe and elsewhere.

Today, we stand at the threshold of a similar constitutive moment, brought about by a revolution whose long-term consequences we are only now starting to grasp. For the past two decades, the emergence of the Internet and cyberspace has led to the largest sustained global expansion of knowledge, rights and freedoms. Over a third of humanity is connected to the Internet, and they are almost as many cell phones in circulation globally as there are people. Significantly we are now seeing the coming of age of digital natives, those who have grown up knowing only a connected world. Two-thirds of those currently accessing cyberspace are under the age of 25, and over 80 percent of those use one form of social media or another.

But the numbers do not do the justice to the social significance of this expansion. So pervasive and all-encompassing is this revolution that it's difficult to see just how fundamentally it's changed the exercise of individual human rights and how much it's added to the cause of basic freedoms and the abilities of all people, no matter how small, to make their voices heard. We need not look any further than the color revolutions in the Commonwealth of Independent States or the recent Arab Spring to witness the extraordinary power of networked social movements.

But the tectonic plates of cyberspace are also shifted. The U.S., once the heartland of the Internet, makes up approximately 13 percent of the global Internet-connected population. Europe and the U.S. are approximately 40 percent. The center of gravity is fast shifting to the south and to the east. The consequences of the shift are of direct relevance to today's proceedings.

A digital curtain is descending across the globe that threatens to reverse the gains made possible through the emergence of the global commons of cyberspace. Just over half of the world's Internet-connected populations live under one form of restriction or another, and that number is fast rising. Since 2003, when we first documented the emergence of the "Great Firewall of China," more than 45 states worldwide have adopted similar means for turning the

Internet from a global commons into a series of gated communities. Eurasia, and in particular the states of the former Soviet Union, are a petri dish of experimentation in the new forms of online repression that deprive citizens of the means to demand transparency from their leaders, accountability from their governments and the right to seek social and political change.

These new forms of restrictions, which we document as second- and third-generation controls, leverage the ability of governments to create restrictive legal environments that attempt to enforce self-censorship through fear of punishment. They also include the application of sophisticated technical means, just-in-time blocking, disrupting access to critical information resources at times when they are most needed, sowing disinformation and otherwise manipulating information flows. They also include the use of targeted online attacks, denial of service, injecting false content and sophisticated information operations—and I mean this in the military sense—turned inwards at domestic populations.

These controls are pervasive but also applied selectively, such as during elections in order to discredit legitimate opposition groups and deprive them of the right to free and unfettered speech. And I say for the record, as someone who operates a circumvention company, that no circumvention technology can effectively combat second- and third-generation techniques, which are becoming the global norm.

In Kazakhstan, Uzbekistan, Turkmenistan and Russia, and notably in Belarus, these techniques have been used with great success to silence opposition groups, driving them and their followers offline. In fact, in all post-Soviet states, the Internet is subject to one form of control or another. Indeed, the mechanisms for control are getting deeper and more coordinated through regional bodies such as the Shanghai Cooperation Organization and the Collective Security Treaty Organization, as well as bilateral cooperation between governments and their security services.

Tragically, perhaps, we are complicit in this growing trend towards authoritarianism. Our own fears of cyberinsecurity and terrorism make it easier for others to appropriate these terms to justify political repression. Terrorists can morph into anyone inconveniently opposed to the political status quo; and calls for changing the Internet, introducing greater security and the ability to identify users, helpful in tracking down hackers and cybercriminals, find their place in the arsenal of repressive regimes as a means of selectively prosecuting human rights activists, journalists or anyone seeking to struggle for social and political reform.

Our emphasis on harmonizing laws on cybercrime and seeking global solutions to global security—to cybersecurity paradoxically makes it difficult to assert and demand respect for freedom of expression and access to information online.

And security is not the only means by which rights can be suppressed. Net neutrality, copyright enforcement and the empowerment of telecommunications carriers to clean pipes are convenient means for regimes with less-than-democratic tendencies to offload and outsource policing and ultimately repression. There are no simple solutions to these challenges, only difficult tradeoffs. To para-

phrase the words of the immortal Pogo: We have met the enemy, and he is at least partially us.

So what is to be done? Future historians will look back at this time and see it as a constitutive moment. Before us are some hard choices, but also clear norms and ideals that have been core to the Euro-Atlantic alliance for the past 50 years and part of our shared cultural and historical heritage. Leadership comes from the courage to make hard decisions in pursuit of a greater common good. In this respect, a commitment to an open, global commons of cyberspace is by far the most important and far-reaching objective for the U.S. and its like-minded partners in Europe and globally to support.

Security is an important obligation of the state but must be balanced against preserving the right to dissent, communicate and act online, even if it comes at costs. This is especially true as the new generation of digital natives find their own voice in the online world. New forms of protests, whether they come in the form of making public confidential information, as in the case of WikiLeaks; or the "hacktivism," as has been exercised by LulzSec and Anonymous, may be the necessary friction for preserving a global norm that enshrines the right to seek and access information.

We must carefully adjust our own laws to make accommodation for some of the new forms of dissent that will emerge. Is there really a difference between picketing an employer during a labor dispute and making his website and Internet systems inaccessible through denial-of-service attacks? These are important questions, and we must pause before we consider how to address them, as the rules that we apply will have repercussions well beyond our borders. In a global world, there is no such thing as a purely domestic policy.

In specific terms, at the highest level, this Commission should encourage our European partners to remain committed to a global commons of cyberspace. Calls such as those put forward by some members of the U.N. to end the multi-stakeholder engagement on governance of cyberspace should be strongly resisted. Pressure should be applied through bilateral agreements such as—as well as organizations such as the WTO to ensure that restricted access to content online is also framed as a trade issue, with consequences and sanctions against countries pursuing these practices. Access to an uncensored Internet should become a basic measure of freedom and demographic—democratic progress and made a condition for recipients of preferential U.S. trade relationships or development assistance. Access to political content via the Internet should become a central component of monitoring the freedom and fairness of national elections, as important as the right to assembly and balloting. Preserving the global Internet commons will not be easy, but the costs of not doing so are greater. The rise of a new superpower in the East is occurring just as the tectonic plates of cyberspace are shifting to the same region. The historic moment in which we live and which has greatly expanded human expression, quest for knowledge and an ability to network on a planetary scale risks becoming a fading chapter in a future where the same technologies enable surveillance societies that far exceed those which

George Orwell's "1984" could imagine. The future is ours to lose, and as in those days of March 1946, when Churchill warned us of the Iron Curtain, now is the time for us to courageously make choices so that our constitutive moment, the future of cyberspace, furthers rather than constrains the universal values of dignity, freedom and right to choose.

I thank you for your time and attention.

Mr. MILOSCH. Thank you very much, Mr. Rohozinski. That—there's a lot to return to in that testimony. I particularly appreciated your image of the—of the digital curtain.

Now we'll proceed to Mr. Ivan Sigal.

IVAN SIGAL, EXECUTIVE DIRECTOR, GLOBAL VOICES

Mr. SIGAL. Good morning, Commission. Thank you for the opportunity to address the subject and the topic of online freedom of expression in the OSCE countries. My name is Ivan Sigal. I am the executive director of Global Voices, a community of bloggers, writers and translators from around the world who amplify and analyze the most interesting conversations appearing in citizen media. Global Voices also has a team of writers and analysts who focus on the former Soviet Union, and my testimony today is informed in part by their analysis and their research.

So my perspective today is slightly different from the—kind of the state and institutional perspective that we've heard thus far from the international organizations. I am trying to channel or represent a diverse set of voices and perspectives that are coming from individuals who are on the cutting edge of the creative process of generating content, news and information for their own communities in their own contexts, and I think the important thing for me in all of this conversation is to figure out how we can support and emphasize that the work of building and creating networks starts with individuals and citizens in their own communities and is focused primarily on creative capacity.

I'd like to look specifically at the question of recent attacks and challenges in the OSCE region, focusing very much on the former Soviet Union. I'd like to say that while attacks have been occurring in this region for quite a few years, those targets have mostly been mass media and more institutional targets. And the change that we've seen recently has been much more of a focus on individuals and social networks. Those targets have fewer resources, less experience, and face a different kind of risk than traditional mass media.

A recent example is Belarus, and we've heard a good deal about that today, so I only want to emphasize that the targets of social media networks themselves are focusing on a different kind of challenge than what we've seen, which is that creative hacking and targeting of individuals that are part of a social media network themselves are not just out going after elites and journalists and kind of leaders or representatives of communities, but individuals who are acting in their own interests, without necessarily an awareness of the impact that their participation in these social media networks will have.

More generally, the mix of tactics of suppression and repression that we see in the OSCE region has a—has a long history, a com-

bination of filtering and hacking of websites, physical threats and intimidation, propaganda and defamation, burdensome legal and regulatory environments, market manipulation and the use of other legal controls such as tax inspections that worked to threaten an earlier generation of content providers online. The targeting of individual websites, online publications and individual writers through a range of online and offline tactics is also not a new story in the region. The concern is that, as the Internet access grows across the region, governments will step up their restrictions, targeting not just the relatively elite communities, but all citizens writing and sharing content on a range of user-generated platforms.

And while the tactics may change, the overall strategy of mixing tools of repression to achieve various ends remains in place. The ultimate goal of this kind of harassing activity seems to be to systematically suppress speech and media content that questions the legitimacy of those in power, and particularly those who question how power and wealth are gained and distributed. It is notable as well that some of these practices are not restricted to nondemocratic regimes. Recent mass media laws in Hungary also treat websites as mass media, for instance.

I'd like to provide you with a short list of some of the tactics and speech—to suppress speech. My testimony goes into them in some detail, so I'll just give you the categories here. Those are: legal and regulatory controls; pressure on service providers and intermediaries; extralegal responses; propaganda, misinformation; disinformation campaigns and harassment of individuals; and indirect methods that are not directly related to speech, such as violence, destruction of property, arson, physical and psychological pressure.

In this context, what can OSCE member states and the U.S. government do? The document of these abuse tactics is well—reasonably well established, as reports referenced earlier and throughout the panel today have shown, thanks to activists and freedom of expression watchdog activities. The OSCE should continue to support and promote monitoring and documentation of member states' activities in this sector, both in their own work and in the work of civil society watchdog groups. The deeper question is the willingness of governments to apply the political will to create positive incentives for citizens to participate in public spheres, pursuing both the letter and the spirit of OSCE rights obligations and the Article 19 of the U.N. Declaration of Human Rights.

These commitments are not just about the economic or scientific benefits of increasing Internet penetration, a concept that many FSU countries and governments support, but about the political and civic rights of their citizens. Without politically legitimate and accountable governance, the political will to foster these rights is unlikely to appear. And to be clear, not every government in the former Soviet Union applies restrictions on online speech to the same measure or kind. The picture is varied, with some countries working to meet their obligations.

So in my testimony, I think for—in interest of time, I won't go through the details of it. And in my testimony, I have a set of ideas about how principles—about some principles for removing suppres-

sion of speech and discouraging self-censorship in the context of existing laws and legal frameworks within the former Soviet Union. They exist ideas about restrictions on the nature of filtering if it is absolutely necessary, ideas about the restrictions of the use of hate speech or negative speech laws to suppress broader classes of speech, and ideas such as requirements for independent courts rather than administrative uses for law. I'll leave that—I'll leave that to you to read later on.

I want to—I want to focus at—for the end of my testimony on the idea of support for generating and creating contexts for people to participate more positively. There are positive reinforcements that the OSCE member states can follow, supporting both the letter and the spirit of their commitments. From the perspective of citizen interests in online environments, this includes a focus not just on access to information, but on the opportunity for online participation, creation and engagement, online and networked media environments. Speech rights precipitate assembly movement and all other rights. Without the medium of speech, other rights are difficult to assert.

There has, in the past year, been an appearance of newly assertive civic voices in several OSCE countries that have poor records on government legitimacy issues such as free and fair elections, corruption and repressive security regimes. The use of information technology tools and platforms that combine data analysis, visualization tools mapping community participation and reporting, and subject-specific expertise point to the creation of projects that are specifically designed to highlight corruption, create transparency and demand governmental accountability. Examples include a project called "Help Map," which allowed Russian citizens to volunteer information and resources to fight fires in the summer of 2010, Roskoms yetka [ph], a crowd-sourced map in which Russian citizens can document instances of bribery, and RosPil, which documents—which crowd-sources independent analyses of Russian government procurements.

These projects show the potential that citizens of—in the former Soviet Union have to find creative solutions to their own problems. Such projects can demonstrate that drivers of change often come from inside repressive environments, and that with greater connectivity, opportunities to participate can create meaningful change. Supporting the continued openness and unfettered nature of the Internet provides projects such as these with a firm foundation for the emergence of creative opportunities for people to express their citizenship. The OSCE role is best articulated in asserting that its members follow the letter and the—this spirit of their obligations.

As far as the U.S. government, its role is best articulated as supporting a continued open nature of the Internet as well. But as a first step, the U.S. should consider how its policies of Internet freedom will affect local communities as—that they purport to help. It should follow a do-no-harm approach that is sensitive to local concerns and contexts and takes into consideration the personal security and goals of the online activist working in repressive contexts.

In addition to voicing support for access, advocates should consider how to provide multifaceted diverse tools and resources that

help people both to get access to information in restrictive environments and, perhaps more importantly, to help them create, share and preserve, build the tools and resources to be engaged in their—as citizens in their countries. The recent U.S. State Department initiatives to support a wide range of tools in education and information—[inaudible]—creative content in countries that use extensive filtering is an example of the right kind of approach. Narrowly focusing resources only on information access to external information, on the other hand, downplays the importance of locally generated content, information tools—information technology tools and the opportunities for communities in repressive environments to strengthen their own content creation.

While building tools to help people participate freely online, protect identity and privacy and participate freely in the exchange of information is useful, it is ultimately not a substitute for the application of political will on the part of all OSCE member states to foster legal environments and civic cultures of online participation. To ensure that we protect and then grow the Internet for citizens first, rather than for security agencies or corporate interests, in this context, the U.S. has the opportunity to lead by example, whether in supporting open governmental data, as with the recent launch of the Open Government Partnership, or supporting Internet policy principles that represent the interests of citizens as well as corporations and governments in forums such as the OECD, or ensuring that cybersecurity policies do not impinge on the privacy and rights of its citizens, as with ongoing debates over the extensions of the Communications Assistance for Law Enforcement Act to facilitate surveillance.

Finally, governments interested in supporting these commitments should support information access but also focus on the creative capacity, removing barriers to civic participation. A set of tools to respond to restrictive governments removing both economic and political barriers is just the beginning. Governments interested in meeting this spirit of OSCE—[inaudible]—can offer many positive incentives to use and support that kind of participation.

Thank you.

Mr. MILOSCH. Thank you very much, Mr. Sigal. Again, there's a lot to return to there. One thing I would like to return to later—if I—if I forget, please remind me—I think many of us would like to hear more about freedom of expression in Hungary in particular as it touches on the Internet and new laws there.

So now we'll turn to Mr. Charles Lee.

DR. CHARLES LEE, FORMER CHINESE POLITICAL PRISONER

Dr. LEE. OK, thank you.

Thank you very much, Commission. It's my honor and pleasure to be here testifying on what happened in China.

When we look at China, actually, the Communist regime in China is the grandfather of information control. After they took over the power in 1949, they took over all these newspapers and, you know, radio, that kind of things at that time.

And later on, well, Internet came up about 20 years ago. They had a great fear inside the Communist Party because—and that was just after the 1989 Tiananmen Square movement—democratic

movement crackdown, so they are afraid—very afraid of these sentiments in the—inside China. So they—but they know that because they opened their economy, so they cannot shut down the Internet. So they try their best to develop the Internet in the meantime, the controlling system and then the "great firewall." So the "great firewall" prototype was established in China in 1990s already.

But however, the development of this Internet censorship was very much tightened and even more sophisticated after the crackdown on Falun Gong practitioners. Talking about the Falun Gong, you know, just want to mention briefly that what is—Falun Gong is: The use of—is an ancient Chinese meditation system based upon the principles of truthfulness, compassion, forbearance, and they have also five sets of exercises. Combined by the principles of this practice and also exercise is so effective.

So the Falun Gong practitioners—the number of them increased to almost 100 million after the end '98, so the Communist regime started to crack down because they did not want to see any group of individuals who can, you know, think and then do things separate from their system. So they started to crack down in 1999, and then, after that, tens of thousands practitioners have been persecuted—tortured to death.

You know, ultimately because they—you know, they highly control information and, like, Internet is one of the—one of them—you know, the most important one—you have also the TV, radio and the newspapers—they launched a huge campaign against Falun Gong, defaming Falun Gong practitioners in order to incite hatred against the practitioners.

But—[inaudible]—there are a lot of efforts done by the Falun Gong practitioners, especially those people in this country—they have followed a—[inaudible]—Internet freedom consortium, combined with the practitioners from the East Coast to the West Coast. They have developed a lot of very effective technologies that can be used by people inside China.

One of the examples is that Falun Gong practitioners inside China have established about 200,000 material centers. But these material centers, they use these technologies developed by the Falun Gong practitioners outside of the country to get the access to the—to websites out of China and also get the materials—all those materials have been sent out, most of them by the practitioners inside China themselves. So they—[inaudible]—materials and then distribute the truth materials to people inside China.

And also, another issue is that—[inaudible]—thousand material centers, they support an estimate of 40 million Falun Gong practitioners inside China today, even though the Chinese government spends so much energy and time and money to crack down, but there are still so many people inside China continuing to practice and also reveal the truth to the grassroots people in China.

Another aspect is that since the end of 2004, there's a book called "Nine Commentaries on the Communist Party"—was published by the Epoch Times. And since that time, there's a growing wave of—movement which is focused on quitting the Communist Party membership and also their other group—other organizations like Communist Youth League and Communist Pioneers. And the number

of these people who have quit these memberships have reached about 98 million just recently.

So these numbers should tell us how effective these technologies are, you know, in terms of piercing the "great wall," and also for those technologies—you know, Mr.—[name inaudible]—just mentioned that, supported by some of the foreign companies, including Cisco. They have—[inaudible]—technologies. And also, another one is called Golden Shield; it's a system of monitoring and filtering the information, monitoring the information, communication between different people inside China, so they can track down those people's IP address and find out who those people are and arrest them. So these numbers tell people that, you know, it's like an ongoing, continuing war between the Chinese Communist regime and also the—between—and the Falun Gong practitioners who have been developing these technologies and upgrading these very frequently so they make sure these technologies work.

So I just to say, these technologies have also been used by some other countries like those people in Iran, Egypt and also other countries like Vietnam, to get more information on—censored information. So I think this— nowadays, you know, this—one thing is that the Communist regime, they have developed so many confiscated technologies and have it used by other dictatorial countries as well. But on the other hand, we also see hope that people are working on this, piercing these great firewalls and also those Golden Shield systems. So it is important to raise awareness of this ongoing war between this censorship and also these efforts to piercing this censorship. And we should support more of these people who can really bring this technology to—bring the information to the—free information to people in those countries.

Thank you very much.

Mr. MILOSCH. Thank you very much, Charles. I hope—we hope we can return to some of the themes you raise, particularly including the effect that China may have on degrading Internet freedom standards in the OSCE.

As the chairman said before he went to vote, Shelly Han and I will proceed to ask questions regarding your testimony, just as if we were—we were in a hearing while we wait for the chairman to return. Ms. Han, I should say, is on the staff of the Helsinki Commission. She is working on Internet freedom legislation for the chairman, and she organized this hearing. I will begin with a question, then I will turn over to Shelly and we'll go back and forth.

The question that I wanted to start off with—and this is perhaps for—more for David Kramer and Mr. Rohozinski—though, of course, all are welcome—is: Is it correct to see in the OSCE—we've talked about China here—is it correct to see China as the instigator or as the motivating force, inspiration, provider of technology, provider of techniques and apparatuses to countries that are—that are restricting Internet freedom? Or is there—is there—is it—do we tend to exaggerate that? Is there some other driver, perhaps, within the OSCE—would there be within the OSCE a country that plays the role that we often attribute to China of spreading or providing technologies of repression? I'm wondering about Russia and Kazakhstan, but it could be another country.

Please.

Sec. KRAMER. I would—China is an accomplice to it, I would say—in providing technology and know-how. But the motivating factor is insecure, paranoid, authoritarian regimes in the OSCE. They are the ones who are driving efforts to crack down on Internet freedom just as they are responsible for suppressing other kinds of freedom. And what we see are these regimes cooperating with each other.

And in fact, they do a much better job of collaborating, cooperating with each other—sharing technology, sharing, if you'll allow the expression, best practices—at least for what they do, than we do in the democratic community of nations in terms of sharing information and technology and coming together to push back on these challenges that are posed by authoritarian regimes.

If we had included all of Central Asia in our survey we would have seen Uzbekistan and Turkmenistan, as one of my colleagues had mentioned, also in the not-free category when it comes to Internet freedom. And some of these regimes do rely on outside players, such as China, to help them in suppressing Internet freedom in their countries. But I think to be clear, the driving force is the regimes themselves who do not want to see freedom, whether it's on the Internet or anywhere else, in their societies.

Mr. MILOSCH. Thank you.

Mr. ROHOZINSKI. Well, I would add to that, I think, maybe something which is a basic fact. And that is that the OSCE region—countries within that region also belong to other regional blocs; for example, the Shanghai Cooperation Organization or the CSTO. Within those organizations certainly there is collaboration between security forces and security interests around shared agendas. Whether that translates into technical assistance, I think is a fairly far stretch at this point in time. We certainly have not seen in any of the former Soviet states the adoption of identical technologies such are used for securing the great firewall of China. That simply doesn't happen.

We see instead a lot more just-in-time approaches to filtering and blocking, which are built around the specific political agendas of the regimes at stake and generally apply to times when those regimes feel it is necessary to tamp down on inconvenient opposition movements. Certainly China plays a role in terms of supplying technology that builds the physical layer of the Internet. And certainly Chinese operators, particularly in Central Asia, have been vying with Russian telecom operators in terms of becoming the carriers of Internet traffic for those countries in the region.

In fact, when we did a study in Uzbekistan several years ago and compared the censorship regimes on several of the Internet service providers, we found that there was an inconsistency between those that chose to buy their Internet services through Russian providers and those who used China Telecom, where China Telecom's censorship regime had effectively been exported to this particular central Asian country. So at the physical layer obviously Huawei is a major provider of equipment.

And since Huawei also operates in Western markets, all of their equipment conforms to CALEA standards, which essentially means it has the same technologies and protocols built in to give lawful access to interception of Internet technologies as does anybody else.

By that measure we can say that Chinese technology is used to secure censorship means in—[inaudible]—states. But whether that's a direct transfer of technology or something which is inherently built in to the standards of technologies that we all use I think is a more accurate way of putting it. Thank you.

Mr. MILOSCH. Thank you. Anyone else?

Dr. LEE. To talk about little things about—you know, besides the technical aspects is that these countries in the OSCE region, most of them are former communist countries. Yeah, I know they're not right now, but there are still elements of—you know, from the previous communist parties—the mentality and things. And I think it's important to realize the movement I just talked about, the—[inaudible]—Communist Party in China. This is like a de-communization of people's mind and behavior. So this is, I think, is like a broadest, you know, angle to look at these things. And it will truly improve this free information efforts, so for people to realize what is truth. Thank you.

Mr. MILOSCH. Thank you very much, Charles—or, Mr. Lee. We go back a little ways. Shelly?

Ms. HAN. Ms. Mijatovic, I wanted to ask you—your report that you issued last week provides a really important baseline for where we are in the OSCE region in terms of Internet content regulation. And I'm wondering where you see your work going forward on this issue, what kind of support do you need from participating states and how receptive are—what we would call, without naming, but the problem countries—how receptive are they to efforts from your office or other parts of the OSCE or even bilaterally to changing some of the regimes that they have right now?

Ms. MIJATOVIC. Thank you. Well, the report is in a way a step forward in the process of reminding governments of 56 [ph] about their commitments and, as you rightly pointed out in the headline, promises our heads of states made on so many occasions in relation to the free flow of information. It doesn't change, offline or online. The situation within the region and beyond of course—we cannot ignore it—it's not rosy.

The attempts of the governments to further restrict, suppress are visible, almost without any shame. This is done in the process of stopping and silencing the voices. Sometimes we see kind of a sophisticated way of suppressing free speech. But in the cases we see more and more and—colleagues today and—mentioned several countries where we see the problems, which is now increasing particularly in relation to Facebook—social media. So that is seen by—and I would dare to say—unstable governments as another threat in the process of establishing more and more borders.

And I really liked what Rafal said about digital curtain. What they are trying to do, they are trying to build a curtain within their own countries. But again—and I would repeat myself once again, it's a lost battle because in the offline world history taught us that no matter how much the regimes try to suppress free speech or human rights in general, people will always find ways to reach for those rights. It's not an easy task; it's not an easy job for my office and for the mandate that I have. I must say that the cooperation is there, but sometimes I have a feeling that some of the documents—some of the most important documents we have within the

OSCE are just empty words on paper because they are not complied with, they are not honored and they are not implemented.

My job in this process is to remind the governments, but today we also heard from a distinguished commissioner at the beginning, do we need a hammer? I do not think so because all the tools that the OSCE has at its disposal, because of comprehensive and consensus-based nature—all those tools are of democratic nature. And those are the only tools we use in this process in order to build more trust.

It's not something that happens overnight, but the cooperation is there. There is more need for coordinated approach by different international organizations in order to make changes. Belarus was mentioned on so many occasions. The only thing we can do is to continue raising our voices and trying to change the situation there and to help people that are really suffering tremendously just because they have differing views or they tried to express their opinion.

Also the countries that were mentioned and they're all the time on the very top of my agenda. Hungary, you mentioned, is of great concern for my office. I raised this issue first time in June, 2009. And we are at the moment monitoring the situation there in order to see in which direction this will go.

You also ask, what are the ways we can help and we can change the situation? We can offer legal analysis of certain laws, articles we send with recommendations to the government. We did it in the case of Hungary. Unfortunately, the recommendations and everything that was put forward was not accepted as valid for certain changes. But we do continue dialogue because that's the only way. And from the Hungarian government's side there is cooperation, in a way that they do listen. But unfortunately still there are no changes, even though I do expect that those changes will—we will start working on it soon.

Turkey as well it was mentioned—and I think it's important in this because we mentioned several Central Asian countries and post-communist countries. Turkey is in a way a very particular case. We have two issues that are burning: imprisonment and Internet freedom. But I think that would deserve a longer time in order to explain it. We do work with the Turkish government very openly.

I'm invited by the authorities for the first visit since I was appointed in September. I welcome this step forward very much, and I do hope that we will come to some conclusions which will change the Internet law that in a way needs to change if you want to see any positive movements. But at the moment, the situation doesn't look very promising.

Mr. MILOSCH. Ms. Mijatovic, could you characterize the Hungarian law and how it affects Internet freedom so that we all have an idea?

Ms. MIJATOVIC. Well, it's almost impossible—[chuckles]—at this occasion because the law—it's one of the—it's thousands and thousands of pages that were adopted overnight, no public consultations. It is very much related to the whole media package, so it's not just the Internet freedom. We heard that—there were many issues mentioned today, but in relation to Internet particularly—

Internet is seen as just another media that needs to be regulated in the old traditional way.

Media Council—Media Authority, which is the regulatory authority, is composed of members with the mandate of nine years renewable, which is not seen in any of the EU member states. They have full power to regulate electronic media, Internet and press, which is also something that is not seen in—within the EU member states' legislation. Internet is a chapter that we also analyzed, and we offered the analysis to the Hungarian government in order to change the law before it was adopted, but as I said, that was not accepted. And the only changes that were made were changes—I would call them of a cosmetic nature—that were made were changes in relation to the request from the European Commission that were related to different issues than Internet freedom.

Mr. MILOSCH. Thank you. Thank you very much. You know, it's very tempting to ask each of you now to rate the five worst countries in the OSCE region but I think we've brought that out already and Freedom House has, by the way, been working on that and done that for us. So I'll ask another question here. Can you give me an idea how the technologies used in Internet repression are changing?

In 2006, we tended to think of Internet repression generally in terms of blocking sites and putting surveillance on users. I have this sense, but don't know exactly, that in fact there are now a lot more things going on, and while blocking and surveilling are still issues, they're no longer 80 percent of the games or 60 percent of the game, but are becoming—are diminishing in their relative importance as many other nefarious tricks and devices have come into play. Can any of you—all of you elaborate on that or respond?

Mr. ROHOZINSKI. Permit me to make the first remark. I think there's a—that there's an essential fact here that has to be recognized and that is that the technologies that are used for limiting access to information or targeting and identifying individuals are the very same technologies that we have demanded to be built into the Internet in order to tackle the problem of cybercrime, cyberespionage, and cyberinsecurity. In fact, some of the most significant technological changes, which will transform the Internet, are being brought about by our concern of securing our national networks from these parasitic and ultimately what we see as negative occurrences.

Now, that having been said, it's also quite clear that regimes have become well versed in the art of information operations—that is, how to create, shape and influence actors on the net using a variety of different tools, including legal tools, including tools that effectively try to drive opposition movements out by flooding their dialogue with a counter-discourse that effectively confuses users; by using shaping through the turning on and off of different parts of networks available on a national level in order to sow doubt, so fear that technologies don't work or that are in, effect, working against the very activists that are using them.

That, I would say, is one of the fundamental trends which we have laid out as second- and third-generation filtering, and ones which, as I say, are being propelled by our own concerns about securing cyberspace from cyber-crime and cyber-espionage.

Now, I agree with my colleague from the OSCE that in some respects, it is human agency, the willingness of people to put themselves at risk, that ultimately drives social change and net technologies. But it's also undeniable that these technologies have made the work of activists and others who care about their communities much easier, much quicker and much less bloodless.

I fear that as cyberspace becomes closed down as an environment, as a domain for legitimate political action, we will be moving from the relatively bloodless jaw-jaw [ph] of activists to the war-war of rebellion. And I, for one, would much rather live in a world where the revolution can be tweeted than when it's belched from the barrel of an AK-47.

Mr. MILOSCH. Thank you. Others? Shelly?

Ms. HAN. We've mentioned a couple times the concept of a—of a regional or national Internet as a way for countries to control information. Recently, Google blogged on their blog about Kazakhstan's request to them to only route information through google.kz, which would mean that in effect, they would be creating almost their own national Internet.

And Google—you know, demurred and asked that—you know, to reconsider that. And I think that they were somewhat successful to—but they—there are still—like, I think future domain names that are added to google.kz will still come under this restriction.

So can we talk a little bit about the technology behind that? How does that work versus blocking? And is that sort of the future for countries—I think Cuba basically already has something similar to that. But is that the future for countries that want to sort of take themselves off what we would consider the global Internet and then create their own version? And how does that work, and why should we be afraid of that?

Mr. ROHOZINSKI. Well, let me take that question. The latest, and I think the headline-grabbing aspects of Kazakhstan wishing to use control of its top-level country domain as a means of creating a national intranet is actually a bit of an old story. Effectively, in Tajikistan and Kazakhstan, national intranets based upon an Internet which is accessible only within the top-level country domain has existed for at least the last three or four years.

In fact, I would say that this is one of the emerging forms of censorship, where economic discrimination or economic means are used as a way of effectively creating a two-speed Internet for citizens of these countries.

So the way that it's worked in Tajikistan and the Kazakhstan previously is there was a different tariff put against someone who wanted to access the Internet that was restricted to domains existing within .tm or .kz and those that gave access to domains outside of that. The difference now that's being made is that that kind of virtual bubble built around tariffs and access to domains are starting to be applied to services which exist on a more planetary level, like Google.

We fully anticipate that both the repatriation by most states in the region, and in fact globally, of top-level domains, which effectively gives them control over the domain-name system within their countries, combined with requests to, for example, register international media carriers as local media, making them subject

to media laws, are the emerging, front-leading edge of what we'll see as control regimes that exist.

We are already starting to see similar kind of efforts, for example, being put in place in Iran—the creation of a national intranet, again, which segments itself from the global Internet. And we fully anticipate that economic, i.e., tariff means, are going to be as effective in creating and making that an effective means for containing populations as will any physical means put over trying to restrict access to the global Internet.

And again, I would say that that is one of the issues in terms of what Department of State and U.S. government should be looking at in terms of addressing the problem of keeping the Internet commons, that simply funding circumvention technologies is not enough. It's going to take a lot of policy work to crack this particular nut. Thank you.

Ms. HAN. But before I let other people comment, how exactly would the State Department address that? You know, because it seems that now, because of the way the Internet governance is established now, it—there is no government-government mechanism for doing that—unless I'm mistaken. But I'm just curious if you had some thoughts on how to address that.

Mr. ROHOZINSKI. No, it's very true. The part of the—one of the benefits of the way that Internet governance has worked up to now is the fact that it's diffuse and multipolar and controlled by a variety of different actors, including commercial, private, self-governing, self-constituting bodies.

What has happened, and what is a trend outside of the OSCE as an organization, OECD as an organization, basically those which conform to our, let's say, similar normative characteristics, is that you are seeing regional bodies start to look at the issue of Internet governance as a strategic priority; harmonize amongst themselves, such as for example within the SCO; use and leverage international organizations as a way of shifting and centralizing intergovernance—Internet governance into organizations that are collective national—or, sorry, international and subject to majority vote.

So the danger is that because the simple majority exists, there is a danger that in effect, those rules will start to be changed. And I think it's extremely important for both the OSCE, at least in terms of its members from Europe and the Euro-Atlantic alliance, and certainly the U.S. in terms of its international engagement, to realize that strategic lobbying and building a coalition of the willing around a concept of a free, open global Internet commons is extremely important as an idea to push cultivate, and support.

Thank you.

Dr. LEE. I want to comment on the situation in China. [Inaudible]—the Chinese government has been tempted to build a national Internet for a long time, but because China's economy is so heavily relied on in foreign trade and you know, there are a lot of foreign business in China, so if they did that, there would be a disaster for the economy, so they couldn't.

So they're trying to tailor—you know, if they could build up a national Internet for the Chinese people or something like that. But technically, it's very difficult. So I don't see this in the near future that can happen. Thank you.

Mr. MILOSCH. I'd like to ask a question of Mr. Rohozinski and also Mr. Lee. I'm—and of course, again, to anybody who interested in commenting. But it would be very helpful if somebody could explain the difference between second—the notion of second-generation technologies in fighting Internet restrictions or these—the second generation of Internet-restriction technologies and how that's changed from what we were dealing with about five or six years ago.

And related to that, I'd like to hear people's opinions on firewall-busting technologies versus—or, circumvention technologies versus other means of—other technical means of promoting freedom on the Internet. I guess we start off with Charles.

Dr. LEE. I feel this is like—like, as I imagine, it's ongoing war, because the—for the next Internet-censorship technology—[inaudible]—upgrading and also, the people, you know, in this country, I mean, Falun Gong practitioners, they also have upgraded these technologies constantly. So I don't have any clear answer for this, you know, generations for—per se, because myself is not a technical person.

But I want to add that, you know, the way of controlling the Internet is—you know, there's a lot of ways for the communist regime. [Inaudible]—very interesting thing in China is that they have hired millions of people, you know, who are unemployed to post the comments in the Internet, to—trying to mislead people's opinions. This is one of those things they do.

I'd just say, on the side of, you know, the technical question—they pay these people like 50 Chinese cents for a post they do, so—which is very good money for them. They—you know, this—you know, they use these resources in China to control the Internet contents. Thank you.

Mr. ROHOZINSKI. So this is outlined actually in the written testimony that's been submitted to the Commission, but I'll restate it here in simpler terms just so we can have a criteria for it.

Mr. MILOSCH. Please.

Mr. ROHOZINSKI. So first-generation filtering essentially relies upon lists that enumerate sites or content that should be blocked and creates a firewall, or a physical barrier that simply does not that let that through. Now, this takes on various technical characteristics, but ultimately what it means is that you are creating a wall that stops certain content from being accessed. It exists all the time. It is constantly upgraded. It effectively enumerates as you go along and in some cases has become much more anticipatory in terms of what content should be blocked. This is what we referred to as the "great firewall of China."

There are very few countries in the world that practice the "great firewall in China"-type approach. And in fact, the number of countries practicing that particular approach is falling.

Mr. MILOSCH. So I take it that no OSCE countries—

Mr. ROHOZINSKI. OSCE countries, we see Uzbekistan, we see Turkmenistan certainly using those kinds of technologies where there is a constant block list, constantly applied.

Mr. MILOSCH. Thank you.

Mr. ROHOZINSKI. We're starting to see selective blocking on a much less—lower level in places like Kazakhstan and elsewhere.

However, the vast majority of what we're now starting to see as online censorship are what we call second-generation techniques. These may apply the same kind of blocking, but it doesn't do it consistently and doesn't do it over time. What it does instead is applies them when those sites or when that information is most needed.

So for example, in 2006 during the Belarus elections, selected sites were blocked, but only for a three-week period. Other than that, they were available. Other second-generation techniques include more active measures taken to shut down sites. Rather than to filter them, they are attacked through denial-of-service attacks, essentially rendering them inaccessible to anybody on a planetary level.

There are also hacking attacks which deliberately manipulate or change the content on those sites themselves. Some of them are quite crude, simply defacing or bringing down the site. Some of them, such as we have seen in Kazakhstan, can be quite elaborate, or in effect, what happens is, content is injected into a legitimate site, only changing small aspects of it rather than entirely blocking the site or entirely changing or defacing the site in a way that it's not effective.

Secondly, second-generation techniques also include the use of surveillance and selective prosecution and the designing of laws that create harsh barriers for someone wishing to either use certain technologies or access certain information, effectively criminalizing it or creating high-level finds that cow people, creating fear and doubt and actually wanting to go outside of this.

Third-generation techniques take it a step further. Those include, for example, the use of malware, computer-virus based attacks against human-rights groups, opposition groups and others in order to pollute their information flows, disrupt their communications, effectively turn members of the organizations against each other if possible.

They include the use, as Charles said, of 50-cent armies, effectively hiring large numbers of counter-bloggers who engage opponents in an online dialogue or simply overwhelm their information flows through the creation of alternative information. Now—

Mr. MILOSCH. Do any OSCE countries do this?

Mr. ROHOZINSKI. Yes. We've seen this very effectively used in Belarus. We've seen this used during the Russian elections. We—in fact, we see this used in just about every OSCE country east of the Elbe.

Denial-of-service attacks are used constantly against independent media, opposition parties or, in effect, a lot of very inconvenient information that exists even out there in the wild that may be specific to any one politician.

In fact, a few years ago, if you had opened a Russian online newspaper, you would have openly seen adverts where people would hire out botnets to carry out denial-of-service attacks against anyone who had the money to pay them the $200 or so to carry these things out. We obviously saw denial-of-service attacks being used very effectively in 2007 against Estonia and later in the Russia-Georgian war as well.

Now, what I would point out, and I would—here, I would put my cards on the table: As an operator of a circumvention technology, it's that dealing with second- and third-generation type attacks is extremely challenging. And none of the tools that are being created, either by our colleagues at the Falun Gong or anywhere else, can effectively get a site back up, circumvention tools, when it comes under denial-of-service attack or encourage people to use online tools where they may fear doing so instead of prosecution or defend them against malware-based surveillance or other kinds of techniques that are being used.

So these are hard challenges which don't have solutions in the purely technological realm.

Mr. MILOSCH. This is very discouraging. I'm getting a picture here of an increasingly broad arsenal of the—of the repressive governments.

Ms. Mijatovic?

Ms. MIJATOVIC. Just a brief comment, but in the OSCE region, unfortunately, you don't need to be very technologically advanced in order to see how the Internet freedom is suppressed on a daily basis. You do not need second or third generations. You just need a young Facebook activist who has a differing view and who is the next day arrested on dubious charges and put in prison for it. So those are also the ways of, in a way, very basic ways of suppression and restriction.

In Azerbaijan, two young bloggers were in a prison for almost two years because they just put a video clip on their website that was critical of the government. They are finally outside the prison, but there was no need for the government to use any advanced technological means in order to put them in prison and to have this enormous chilling effect that is continuing in Azerbaijan, because now there are two more Facebook activists in the prison just because of differing views, again, on dubious charges.

And when I write to the governments, what I hear from them that it's absolutely nothing to do with freedom of expression, it's because of drug-dealing, that's mostly the case that it's used, drug-dealing or hooliganism as an explanation of suppressing people's rights to express their views on the Facebook. And that is becoming more and more problematic, especially in Central Asia, because it's seen as—especially after African Spring—as another threat to the governments', in a way, will to suppress any critical voices in their countries.

So just the point was that you do not need advanced technology in order to continue this agony, in a way, of trying to suppress people's voices.

Mr. MILOSCH. Point taken. Mr. Sigal?

Mr. SIGAL. I'd just like to point out that this trend—we're talking about it as if it's new, but in the former—in many countries in the former Soviet Union, this is something that's been occurring for 15 years. And if there are additional tools in the arsenal of repressive regimes today, it does not diminish the basic strategy that they've employed for a long time, which has always been a mix of tactics designed to intimidate, to restrict, to suppress, to propagandize, to create disinformation or misinformation around a particular set of ideas.

If, in 1996, the response of—the way to take out an independent newspaper in Kazakhstan was to throw a firebomb into a printing press, today there's a similar mechanism. And I think we shouldn't be discussing this issue as if there's some kind of essential change in the way—the approach that's—that we see here.

There are websites that were altered, hacked and altered around—opposition websites that were hacked and altered in Kazakhstan 10 years ago so that that second-generation technology that Mr. Rohozinski is speaking of is—has been occurring in Kazakhstan for 10 years.

So it is not—it is—again, the intent is to focus on internal voices that have an effect not just of receiving information and listening passively, but are actively trying to produce content information or create a voice that are a threat to the legitimacy or threaten the authority of regimes around very specific issues. And security ministries in many of the countries we've been discussing are—have active strategies about how to combat or pinpoint those kinds of issues. And I think that's the—the proper framework for understanding the problem.

Mr. MILOSCH. Thank you. Mr. Kramer?

Mr. KRAMER. Could I just quickly add—picking up on some of what's been said—it is important to recognize, I think, that the technology can have a negative impact on the state of human rights and freedom in the world, and certainly in the OSCE region. The OSCE is no exception.

In the recommendations and the testimony I've submitted I suggest that companies conduct transparent human rights impact assessments so that they determine how American-made technology might adversely affect the privacy of citizens in the OSCE region that could severely restrict freedom. And in light of the European parliament's passing an export control regime of products that have a negative impact on Internet freedom, I would suggest that the Congress also look at the possibility of such a regime.

And then, in picking up on a point that Rafal had made and going through the different generations of technology that these regimes use, as critically important as busting through the firewalls is, there are other anti-censorship technologies and assistance and advice that can be provided. And those include training so that activists are aware of and recognize the threats that are being posed—they reduce their vulnerabilities; security, so that they have the support necessary to fight against the various cybersecurity threats that they face on a daily basis; and then thinking about urgent response mechanisms so that if in urgent need they have places that they can go and networks that they can rely on.

Thank you.

Mr. MILOSCH. Thank you.

Ms. HAN. One more question?

Mr. Sigal, I wanted to ask, and I'd like others to chime in if you'd like too, but really what is the role for citizens? I mean, Global Voices is a forum for users in a lot of different countries. But how should citizens be working? I know we're focusing here on government policies and what governments are doing but, you know, I'd like to look at—talk a little bit more about what private companies—the technology companies that are expanding the, you know,

either the social media or the infrastructure itself—what should be their role? But then also, what about users?

Ethan Zuckerman famously coined the cute-cat theory of, you know, sort of harnessing the number of users and the interest in the Internet for watching cute cat videos; how do you then translate that into users who are really—how should I say this—that are interested in how they're getting their information and what information they're getting? You know, how do we make that leap from people who just randomly want to go on and watch YouTube videos to people who actually care about how their government is controlling or blocking their Internet? I wondered if you had any thoughts on that, and others as well.

Mr. SIGAL. Well, this—the fundamental structure of online communities in a network media society is webs or circles of individuals who have multiple links through their communities that are focused around common interest, if you're talking about citizen media space. So if—for instance, a very simple example, if I have blog and I write about cats, and I will put a list of links in my—within my blog to other people who also write about cats. That constitutes a community.

Once a community is formed, it continues to focus on its subject or its issue but it has become potentially an active space for other contexts—other conversations. If we look broadly speaking at the way that online communities have moved in regard to, say, Arab Spring movements, we see that the function of the Internet is very much an accelerator. It is very useful at bringing together a cross of categories, that is people who—people who like cats, and networks—that is, people who are involved in another and happen to live for instance in the same physical space. And there's a sociological theory around this that's called Catnets, which is not the same theory as the cute-cat theory.

On the Internet it becomes much easier to create, to raise a flag such as an image or a concept or an idea, and rally people around that idea. And the formation of those groups can be—is much more rapid. Whether or not that leads to some kind of actual social change is a different question. But if we look in Egypt, for instance at the We Are All Khalid Said movement, we see a simple event which is difficult but an event, which is the arrest and then eventually the killing of an individual, that served as a flag or a concept around which people could rally.

As I said, as a social movement it is not different, necessarily, from earlier kinds of social movements except in terms of its accelerating potential. And when we follow how social movements track, not just nationally but around the world, we see the potential for communities to gather quickly around a concept rather than around an individual—are greatly enhanced. And one way of thinking about it is that we should be thinking about how ideas move through people and networks rather than finding or focusing specifically on charismatic leadership or on traditional hierarchies of organizing in opposition movements, which is not to say that organization is not important. I think anybody who works in the digital media activism space would say that you still have to organize people if you want to get them onto the street.

It's not technological determinism to say that these are tools that are effective in creating and driving change. It's more of the—more the point that there's a different kind of organization. And if you're thinking about how communities do organize, they—it's a matter of choosing the right tool and the right tactic for the event.

So in Tunisia, Facebook was really important. And it was important because so many other user-generated content services and blogs were blocked, but the private networks within Tunisia were able to focus on work in the Facebook space. But that didn't reach a large audience; it reached a very narrow audience. For them to be effective, they had to be translated, taken out of the Facebook community, put into blogs, put into other contexts, and then ultimately broadcast by Al Jazeera. And then they were effective at a national scale.

Mr. ROHOZINSKI. I'd just like to comment on something that Ivan said because I think it's a very essential point here. The character of opposition movements—how they coalesce, how citizenry can, in effect, mobilize itself for social change—has been transformed by technology. You know, whereas previously movements required long gestation periods, different organizational structures, now it is possible to create a "Facebook revolution" essentially because of the means of being able to bridge commonality of interests and create an emotive spirit to get out on the streets and carry out social change in ways that simply isn't possible when you have an organization that's dependent on leadership. You can have leaderless resistance.

However, and I think this is an important point, just to come back to something that you had mentioned as one of your questions, I don't—certainly don't want to leave the impression here that circumvention tools or technologies are not important to be supported in their own right. I think they're an essentially a very important tactical tool for promoting openness and the possibility of social change. They're not a substitute for a strategy.

And I think that's where, in the past, debates have unfortunately fallen into—that somehow we can design something that will meet our objectives or create our objectives. Let's not forget, fax machines did not lead to the Polish revolution; Solidarity did. Much in the same way, it'll be the work of the Falun Gong or concerned Chinese citizenry that will effect social change and not TOR or not GIFC or not Sai-Fon [ph].

Thank you.

Mr. MILOSCH. I'd like to switch gears for a moment here. Just as most of you or all of you represent groups that are about change, that the Helsinki Commission is also about change. And it's of course very helpful to get your assessment of the situation and the problem. I'd like to talk about what we can do going forward.

My first question would be for Ms. Mijatovic. The Helsinki Commission, of course, was created to interact with the—with the OSCE. Do you have any suggestions on what the Commission and congressmen who are interested in the OSCE can do to promote those—the Internet freedom agenda to promote freedom on the Internet within that organization? What kinds of things—and you can be very particular, very specific—would be helpful to move this

issue onto the agenda in an effective way within that—within that group?

Ms. MIJATOVIC. Thank you for this question, it's very relevant. And I would also like to use this opportunity for us to thank the Commission for constant interest and involvement in the work of my office and its support, which in a way presents an enormous energy that is given to us when we see that participating states through their commissions and different other bodies are trying to engage more in all the issues that we are discussing in order to promote and to implement the commitments.

What can be done in order to enhance this cooperation and in order to make those states that are not actually honoring the commitments? I think what we have as a problem in certain regions—but in certain countries of the OSCE region—is something that is almost in a modern, digital world something that is, you know, not understood well. It is the problem of telecommunication infrastructure, a very low level of penetration of the Internet, and ultimately a lack of Internet literacy education.

So I think, in a way, in order to promote freedom there is more need to continue talking about it on different levels and in different countries because I always said in my work it is almost impossible to do anything from Vienna. In order to change things, you need to go to certain countries in order to promote the commitments and in order to engage with civil society and with the authorities.

Sometimes it's a struggle, but in this process the Commission and all other bodies that are interested in working with the office can do more on promoting trainings and education in certain regions of the OSCE so we can move to a different level when we talk to people and we try to help them, because some of the issues that we tackle today in some of the countries would be almost impossible for people to understand in order to know their rights. So in those countries it's very easy to manipulate people's minds and their decision-making process because they do not know enough for a different reasons.

Maybe it's a legacy from the old systems, as we heard before, but maybe also the restriction of information that is seen as a tool of suppressing their views, not to mention any critical views. So the chilling effect is another thing that we see as a huge problem. I do not have a formula how to tackle—I do not have a formula how to tell Commission in order to engage in this process.

But I think what we have already—the cooperation with the NGOs and different other organizations in order to promote Internet freedom and to actually explain what does it mean and why it is so important so it's not seen as some kind of monster behind a closed door that is going to destroy, as I hear on many occasions, tradition, culture, and sensitivities of certain societies, which is not the case. So I would just encourage you to do more and more of hearings of this kind in order for us to be able to talk to the audience but also to engage in the projects that would promote Internet literacy within the OSCE region.

Mr. MILOSCH. If I could follow up, because I have a very closely related second question, and that is, if the first one was about how the Commission can interact with the OSCE to move this issue for-

ward, what about what Congress can do to move this issue forward in the OSCE and in the broader world?

I think I've already mentioned that the chairman is working on long legislation on Internet freedom. It'd be very interesting to hear from each one of you your thoughts on the traps that legislation—that it could fall into, the directions we should go, your thoughts and reflections on emphasis, the success or failures of previous iterations of Internet freedom legislation and, you know, how the issue is changing and how we need to be changing our thinking about it in order to, as I said, promote change—what about change?

Ms. MIJATOVIC. Well, if I may, I said at the end of my statement that one of the humble suggestions of mine would be to make an Internet a human right, like, for example, Estonia or Finland did. So I think if more and more countries would engage in making it a human right and enshrine it in their constitution, that would probably bring long-term changes in people's mind on how important it is to have access to Internet.

On a more practical level, I think Dan mentioned it during his testimony, this year towards the end we will have a ministerial conference in Vilnius. And Lithuanian chairmanship made freedom of the media and freedom of the Internet, of course, as one of their priorities. I know that the chairmanship is aiming to adopt a ministerial decision in relation to Internet freedom.

And the support from the Commission and the Congress and the U.S. government in this particular issue would make a great impact and a great change in order to make this happen because I think it would be, in a way, not a new commitment but rolling over what we have already into a new reality, which is Internet reality. And it would present a political view on the importance of Internet freedom within the OSCE region.

And I do hope that 56 will have enough courage and wisdom to adopt such an important decision at the end of the year. So, you know, we will be open—my office of course doesn't play a role in their decision-making process, but we would assist and help as much as we can, because because I think for Internet users and for citizens within the OSCE region this would present an enormous step forward.

Mr. MILOSCH. Thank you very much. Fifty-six—that is the tough part, the 56 member states. David?

Mr. KRAMER. Just very quickly—the three points. One, the Commission and members of Congress really can't stress enough the importance of open access to the Internet. That this is, as Dunja had said, this is a fundamental freedom— it's freedom of expression. Having hearings like this, having hearings specific about certain countries and abuses that governments are responsible for, I think, is very worthwhile.

Second is to call out member states that are not complying with these fundamental freedoms—naming and shaming. It is tough to do in an organization that is based on consensus. But some member states have to stand up and take a principled position when there are such abuses taking place and trodding on fundamental freedoms.

The third point is to support in the strongest way possible the Office of the Representative for Freedom in the Media. It's critical. It's not an easy job. And it deserves full support from members of Congress, from the Commission and from the U.S. government.

Thank you.

Mr. MILOSCH. Please?

Ms. MIJATOVIC. A quick note on this. And thank you very much, David. You said it, so I didn't have to say it—[chuckles]—myself. But support is there and it's extremely important to have this support because it gives more energy and more courage for us fighting for free speech around the world.

But I think we are criticizing a lot of 56, but I think also this is a good moment to remember that the office was created by 56. And the office is the only intergovernmental media watchdog in the world. It is unique, and I think this uniqueness and in a way the beauty of the mandate is that the 56 created an institution to name them, shame them and blame them for not complying with the—with what they agreed on a voluntary basis.

So that's actually my job. It's not any easy one. It's a very sensitive and very responsible task. But I do not hesitate to explore the mandate and innovate to bend it and stretch it when there is a need to remind the participating states. But if there are more voices joining from the NGO side and from the authority side, of course, the impact and the results are much greater.

Mr. MILOSCH. That's a very true observation. Pardon my flash of cynicism on the number 56.

Please, Mr. Rohozinski.

Mr. ROHOZINSKI. Well, as a Canadian citizen, I find myself in the funny situation of being asked to advise the U.S. Congress when my own parliament has yet to hold a single hearing on this particular issue.

That having been said, let me summarize a few points as takeaways. One, I think it's really all about leadership and moral courage. We have to recognize the centrality of cyberspace to everything that we do. There is no separation between domestic policy, in terms of how we choose internally to regulate the Internet or provide means for providers in the U.S. and how those means will be interpreted and used, whether in the OSCE or globally.

Along with that comes a very important task of recognizing cyberspace as a global commons, a global commonwealth that requires a joint stewardship. It's not simply about the Internet. It's not simply about a domain. It's about something which we collectively have to tend to as a global society in order to ensure that those flickers of freedom that have emerged over the last two decades globally continue to burn rather than to wink out into a new era of darkness.

Three, we need to recognize that there is a basic contradiction between the way we are currently addressing the insecurity, cybersecurity and the militarization of cyberspace and some of the values and principles that this panel has raised. There is a cost to maintaining an accessible and open Internet. And that may mean being able to absorb the friction of the inconvenience of groups like WikiLeaks, which put our secrets out for everyone to see, and pro-

vide transparency which is perhaps slightly more radical than most commercial and public bodies are willing to see.

Three—or, four—in terms of addressing the hammer that one of the members of the Commission raised, access to content, access to information should be raised as a trade issue, as one on limitation of trade. I think that's an avenue for combatting censorship, which has not been fully exploited by anyone and where the U.S. has a unique position as a major trading partner to actually exert some authority.

Fifthly, governance: We must preserve the multi-stakeholder approach to Internet governance. That means ensuring that the centralization of governance is not concentrated in institutions where values through simple majority vote may shift it into a direction which is inimical to the principles of freedom and choice that we have enshrined and that we all support. Thank you.

Mr. MILOSCH. Thank you very much. Mr. Sigal.

Mr. SIGAL. I very strongly support and echo the concept of a global commonwealth within the space of Internet and cyberspace. I think that the notion that we have the—a potential future where all of us are interlinked, connected and can actually—can exist whereby any individual in the world can talk to, communicate with any other single individual, groups of individuals is a vision for a future of a borderless world which I'd like to participate in.

And I think that the legal principles that make that possible already exist within the frameworks that we have. In making legislation, I would urge that we be careful about focusing on today's technologies to the detriment of thinking about the future of where our technologies will take us because as we've seen, the communications tools and platforms that we are using today were tools that we didn't envision 10 years ago.

And we may find that—we know that technology moves faster than law, faster than regulation. And we may find that we're building systems that aren't able to accommodate—building legal systems that aren't able to accommodate the technological changes, or worse, that we'll be creating eddies or restrictions that force technologies to grow in a way other than they would if they were living in unfettered and global commonwealth of ideas.

I'd also like to point out the concept of a free movement of ideas and how some of our trade laws and corporate and commercial laws potentially act as restrictions to those kinds of ideas, whether it's things like the commercialization of human biology or the effects of the entertainment industry on copyright.

In the space of a cultural commons and a global commonwealth of ideas, innovation comes through the potential to have access to other concepts and other communities of ideas. And just as the technology has walls, we also have the potential to put walls on our culture and walls on our concepts. And I would urge that we think very carefully about not creating those blockades in the process of responding to special interests that may exist in this country or in other countries in the OSCE region.

Lastly, I think that from the U.S. perspective, it's very important, again, to lead by example. So we have the potential ourselves to create in this country a set of—a basis for an open and

participatory network of communications. And that, in itself, is potentially under threat.

So we see ongoing discussions about net neutrality, about tiered systems for access. I'm not saying that those discussions are necessarily clear in terms of what is right or what is wrong. In some cases, policy is really unclear as to what a best solution is. But the principle should be the guiding—the guiding principle that each of us has equal access is very, very important to sustain.

And lastly, as regards international engagement and the question of legislation, I think it's very important to look closely at the potentially contradictory roles that the State Department and Commerce Departments and other kinds—other departments and the military as well will play when thinking about how we should be shaping the Internet. We aren't necessarily, even within the United States government, in accord. Thank you.

Mr. MILOSCH. Thank you very much. Mr. Lee?

Dr. LEE. Thank you. I'll say that I think conclusion statement that the Chinese people has been waiting for a, like, commonwealth of the world for a long time. There have been more than 160,000 uprising events in China last year against the Chinese communist regime. It's horrifying, you know, in the sense that so many people are living in such misery.

As to the U.S. government, I believe that U.S. has the moral authority to lead the world to the land of freedom. And I hope that when the U.S. government deal with the communist regime in China, they don't forget this role.

And for—and also, I just want to echo on the—Mr. Rohozinski's comments on the people's power because it's often the people who can have the right value, the right sense of judgment and what is right or wrong to lead world toward freedom.

The "Quitting the Communist Party" movement actually has led into this direction because, as I mentioned, these countries in the—East European countries, mostly they are former communist states. The technologization [ph] is extremely important in these areas to really have a nice sense of, you know, free—what is freedom.

So I hope that—actually, I want to just mention over here that the day before yesterday, the U.S. Senate has introduced a Resolution 232, which supports this —[inaudible]—the "Quitting the Communist Party" movement and supports the human rights in China. So—[inaudible]—the U.S. government can play a great role in supporting these peoples' power and the move to the right direction in those dictatorship countries.

And also, for the global freedom—Internet Freedom Consortium, it needs more support because a lot of people know they're doing great things, but they left the resource—actually, that Chris—Mr. Smith asked this question to the first panelist already. So I—you know, this is my hope, that things—actually, I believe that things will move to the direction we want to see. Thank you.

Mr. MILOSCH. Thank you very much, Charles. Well, it looks like the chairman is not going to make it back before the room reservation expires. I would—I would just ask any of you if you have some final comment that you'd like to make, some point you've not been able to make yet in the hearing?

If not, then I will thank very much the witnesses for coming and to everyone who joined us today. We're adjourned.

[Whereupon, at 12:30 p.m., the hearing was adjourned.]

A P P E N D I X

PREPARED STATEMENTS

PREPARED STATEMENT OF HON. CHRISTOPHER H. SMITH, CHAIRMAN, COMMISSION ON SECURITY AND COOPERATION IN EUROPE

Good morning, and welcome to our witnesses and to everyone joining us this morning.

Sadly, online censorship, surveillance, and the intimidation of online speech is not restricted to countries where it's commonly reported, like China and Iran. It is increasingly common in member states of the Organization for Security and Cooperation in Europe—broadly speaking, in Europe and the former Soviet Union.

With this hearing, we seek to draw the world's attention to the arrest of bloggers, to the blocking of Web sites, the surveillance and intimidation of peaceful political activists, to aggressive denial of service attacks, and to violent intimidation by some OSCE member states. For example, Belarus is blocking social networking sites as Twitter and Facebook and temporarily shutting down opposition Internet sites. Turkey is set to require a mandatory, nationwide Internet filtering system on August 22—unprecedented in scope in the OSCE region and compounding the already aggressive blocking of around 14,000 Web sites and broad restrictions on content. Kazakhstan, which already blocks a number of popular blogs and media sites, is also in the process of creating a national Internet, having recently decided that all .kz domain names will have to operate on physical servers within its borders.

No less disturbing is the violent intimidation of dissent in Russia. Though Russia does not aggressively censor terms or significantly block access to information on the Internet, it has its own crude but effective methods for controlling the Internet: mafia thugs in league with the government beat people and instill fear in Russian bloggers and journalists. According to the Committee to Protect Journalists, "Online journalists in Russia and throughout the region—whose work appears on the Russian-language Internet known as the Runet—have faced physical intimidation, attacks, and threats for far longer than has been widely noted in either Moscow or the West."

In a report issued by the Open Net Initiative, the authors (one of whom is here with us today), concluded that Internet controls in the Commonwealth of Independent States have evolved "several generations ahead" of those used in other regions of the world. Runet controls are not only mirroring past oppression, the authors said, they're foreshadowing the future of Internet control worldwide. The prospect of the Internet environment deteriorating to that level is frightening, and surely is a call to action.

At the signing of the Helsinki Final Act in 1975, President Ford stated that history will judge the signatories, "not by the promises we make, but by the promises we keep." This is as true now as it was then. All 56 OSCE states have agreed to respect their citizens' human rights and fundamental freedoms, including the freedom of expression. But some do not do so—and are not only not improving but even backsliding. I look forward to a conversation on what we can do to turn this around.

PREPARED STATEMENT OF HON. BENJAMIN L. CARDIN, CO-CHAIRMAN, COMMISSION ON SECURITY AND COOPERATION IN EUROPE

Mr. Chairman, the issue under discussion today is of great importance, both for the present and the future. The Internet has played a critical role in the events we've all witnessed in the past few months in North Africa and the Middle East—it has become an enabling tool for citizens to seek redress and seek change. When governments tried to stop the protests by blocking or, most notably an alarming Internet 'shutdown' in Egypt, netizens found ways to get around the obstacles and got their message to their countrymen, and to the world.

The fundamental reasons behind the protests and the uprisings are age-old, but the incredible communication and information tools provided by the Internet to combat these problems is brand new. But there are worrying trends where we see the incredible promise of the Internet being thwarted by government intervention. It has become clear that we as citizens and as governments must work to keep these powerful tools in the hands of those who want to use it for freedom, not suppression.

So as we discuss oppression on the Internet, I also hope we can talk about the solutions—what are the best practices countries and citizens can follow to keep the Internet safe for democracy? And how do we accomplish that and also keep the Internet secure? From Wikileaks to Anonymous, hackers exposed the weak links, both human and technical, in our nation's information security web. These incidents beg the question, "how can we maximize our nation's cybersecurity without sacrificing our citizens' Internet freedom?" The reconciliation of user privacy with effective cyber-security measures is certainly an important question, but I believe they can be complementary. I introduced a bill earlier this year, the Cybersecurity and Internet Safety Standards Act, which would require our government and the private sector to work together to develop minimum safety standards for Internet users, with as few restrictions on personal freedom as possible.

Any increase in Internet regulation and security there will follow, however small, a decrease in the level of privacy, which imposes a responsibility not to abuse the public trust for its own gain on the government. As demonstrated in the former CIS countries, the government's abuse of its regulatory power for often murkily-defined security reasons often serves as a smokescreen for political repression and comes at the expense of the rights and freedoms of its citizens. We are vigilant against that here in the United States—and must remain so—but with any regulation, there is the potential for abuse of the public trust. And that is something that we have seen happen in some OSCE countries, where governments employ many tactics, both visible and covert, to stifle opposition and free speech. These range from selectively enforced, ambiguous defamation laws to collection and retention of sensitive user information and data to large-scale hacking attacks on domestic and international targets. As participating States of the OSCE, these governments pledged to uphold a higher standard of human rights. Their open neglect of these responsibilities raises serious concerns, and I look forward to discussing these with our witnesses today.

I'm particularly pleased with our panel of witnesses today, as many of them have contributed significantly to this debate by shedding light on some troubling trends, as well as providing solutions for us to follow. For example, the OSCE Representative on Freedom of the Media has made extensive recommendations on best practices through a system of transparent governance in Internet regulation. One of the ways identified is to involve competent partners from civil society in order to expand the responsibility of regulation and consolidate the diverse, high level knowledge and competence required to do so.

I'm looking forward to hearing her thoughts, and others as well, on where we stand today in the OSCE on this issue. Thank you.

PREPARED TESTIMONY OF DR. DANIEL BAER, DEPUTY ASSISTANT SECRETARY FOR DEMOCRACY, HUMAN RIGHTS AND LABOR, U.S. DEPARTMENT OF STATE

Thank you, Mr. Chairman. Distinguished Members of the Commission, I appreciate the Commission's affording me the opportunity to address an issue with profound implications for the exercise of human rights in the OSCE region and across the globe: ensuring a free and open Internet. Your focus on this critical subject is emblematic of the Commission's strong defense and dedicated promotion of human rights principles enshrined at the core of the Helsinki Final Act and UN Universal Declaration of Human Rights. States have an enduring responsibility to respect these principles and their responsibility extends into the Digital Age. In the 21st Century, men and women everywhere are increasingly turning to the Internet and other connection technologies to exercise their human rights and fundamental freedoms.

I have valued the opportunity to work with Members of this Commission and your superb staff. The Commission's efforts greatly strengthen my hand and that of Assistant Secretary Michael Posner and our colleagues in the State Department as we work with other governments, civil society advocates and the private sector to defend and advance human rights and democratic government. The defense of Internet Freedom is integral to our efforts.

If I may, Mr. Chairman, first I will describe the Obama Administration's global policy of support for Internet Freedom. Then, as you have requested, I will highlight key trends and concerns regarding a number of countries in the OSCE region. Finally, I will describe what we are doing institutionally within the OSCE to ensure Internet Freedom.

The U.S. Champions a Rights-Based Approach to Global Internet Freedom

The United States champions Internet freedom because it derives from universal and cherished rights—the freedoms of speech, assembly, and association. An open Internet gives people a neutral platform from which to express their legitimate aspirations and shape their own destiny. We believe that people in every country deserve to be able to take part in building a more peaceful, prosperous, and democratic society. In the 21st century, technology is a powerful tool with which to exercise human rights and fundamental freedoms. In turn, ensuring Internet freedom helps create the space for people to use technology to "know and act upon" their rights.

As Secretary Clinton has emphasized: "The rights of individuals to express their views freely, petition their leaders, worship according to their beliefs—these rights are universal, whether they are exercised in a public square or on an individual blog. The freedoms to assemble and associate also apply in cyberspace. In our time, people are as likely to come together to pursue common interests online as in a church or a labor hall."

As we all know, the Internet and other new technologies are having a profound effect on the ability to organize citizen movements around the world. And because repressive regimes understand the power of this technology, they are redoubling their attempts to control it. It is no coincidence that authorities who try to restrict the exercise of fundamental freedoms by their people, impede the work of human rights defenders and civil society organizations, control the press and obstruct the flow of information, tend to be the same authorities who try to restrict, impede, control and obstruct their citizens' peaceful use of these new connective technologies.

Governments that respect their citizens have no reason to fear when citizens exercise their rights. And governments that respect the rights of their citizens have no reason to fear a free Internet. As President Obama has said: "suppressing ideas never succeeds in making them go away."

Recently, in Vilnius, on the margins of the Community of Democracies ministerial meeting, Secretary Clinton and I met with activists-including several from the OSCE region—who spoke of the surveillance, hacking, and harassment they face every day.

Mr. Chairman, we are not cyber-utopians who believe that the Internet is the magic answer to the world's human rights problems. Technology does not change the world; people must. Some governments are using advanced technologies to chill free expression, to stifle dissent, to identify and arrest dissidents. Through our diplomacy and through direct support for embattled activists worldwide, we are helping people stay one step ahead of the censors, the hackers, and the brutes who beat them up or imprison them for what they say online.

At the same time, we will continue to speak out about the regimes that resort to such behavior. And we will continue to point out that cracking down on the Internet only undermines the legitimacy of a government in the eyes of its own people—particulary young people. Those who have grown up in the Internet age understand

how critical it is that all people everywhere can join in the global discussion and debate. These young "digital natives" understand intiuitively the dangers of an online world where citizens in one country receive only censored information and so form a stilted view of the world. And they understand intuitively the need to protect the promise and the potential of a truly free and global Internet.

Around the world, our embassies and missions are working to advance internet freedom on the ground. We are building relationships with "netizens" and advocating on behalf of imprisoned and arrested online activists. Internet freedom is now a core part of many of our bilateral human rights and economic discussions with a broad range of countries. Fostering free expression and innovation is a core element of the President's International Strategy for Cyberspace, released in May of this year. As Secretary Clinton said in the rollout of the strategy, cyber issues are a new foreign policy imperative. Accordingly, we are integrating Internet freedom into our engagements on the broader range of cyber issues.

Since 2008, the State Department and USAID have committed $50 million in direct support for activists on the front lines of the struggle against Internet repression. By the end of 2011, we will have allocated $70 million toward these efforts. Our programming responds to the most urgent priorities we hear from activists on the ground—including embattled democracy and human rights activists from OSCE countries. A critical part of our efforts is support for circumvention technology, to enable users to get around firewalls erected by repressive regimes. But circumvention alone is not enough. Users do not just need access to blocked content; they also need to be able to communicate safely with each other, to organize, to get their own messages out. For this reason, we are funding the development of better communication technologies, including secure tools for mobile phones, to empower activists to safely organize themselves and publish their own material. We are funding trainings on cyber self-defense, to train activists in person about the risks they face and how to protect themselves online. And we are committing funding to research and development, so that we stay ahead of the curve in understanding evolving threats to Internet freedom.We also are working with the private sector, to define the steps that governments and businesses need to take to protect and respect human rights and fundamental freedoms at a time when the technology and its implications are changing constantly.

And, through our multilateral diplomacy, we are playing a leading role in building a global coalition of governments committed to advancing Internet freedom. To that end, we are working at the UN Human Rights Council, in UNESCO, in the OECD, and, of course, within the OSCE.

OSCE as a Pioneering Regional Platform for Human Rights and Fundamental Freedoms in the Digital Age

Mr. Chairman, as you know, OSCE was the first regional organization to recognize that respect for human rights, pluralistic democracy and the rule of law are prerequisites for a lasting order of security and prosperity. And OSCE was the first regional organization to acknowledge the vital importance of civil society. The Helsinki process must continue to be a pioneer for human dignity, civil society and democratic government in the Digital Age.

Challenges to Internet freedom in the OSCE region are illustrative of the issues we are addressing across the globe in our efforts to support an open Internet. Let me now address trends and concerns related to Internet Freedom in a number of OSCE participating States:

Belarus

In mid-2010, Belarusian authorities announced a new legal regime designed to restrict freedom of speech on the Internet, and to harass and intimidate individuals and organizations to deter them from expressing their views through Internet postings, email and websites. The law requires all website owners to register with the authorities, and further requires them to maintain their sites on the government-controlled *.by* domain. Citizens seeking to use the Internet at public locations including Internet cafes must present their identity documents, and Internet cafes are responsible for maintaining lists of users and the websites they visit. Authorities routinely monitor emails and Internet traffic, and at times block access to websites linked to opposition political parties and independent media groups. On December 19, 2010, the day of the presidential election, authorities also blocked access to popular global sites, including Twitter and Facebook. The same day, denial of service attacks led to the disabling of over a dozen popular Belarusian independent media websites.

In recent days, Belarusian citizens have mobilized via the Internet to organize a series of "silent" protests designed to highlight the government's continuing repres-

sion, the lack of freedom of speech, and the country's deteriorating economic situation. Since June 8, such protests—in which participants gather silently and clap their hands—have taken place in at least 43 cities and towns across the country. Authorities have responded by dispersing gatherings via heavy-handed tactics and by detaining hundreds of people. Police have ordered the closure of at least seven websites, and reports of denial of service attacks and spear-phishing attacks have also increased. Finding themselves unable to completely suppress free expression via the Internet, Belarusian authorities have created their own Twitter accounts to threaten protest participants, and have flooded the most popular Belarus-focused news feeds with misinformation designed to disrupt plans for further protests.

Yet the protests continue and demonstrators continue to express themselves online. Over 216,000 people joined a group on Vkontakte (the Russian-language equivalent of Facebook), calling for "Revolution via the social networks" in Belarus. The page was shut down on July 3, but a replacement page gained 20,000 members in two days. Bloggers and Internet journalists have continued to post videos of police beatings and harassment of peaceful demonstrators on YouTube. During a recent public protest on July 3, police reportedly arrested nearly 200 people; at least 15 journalists were also detained. During protests on July 13, authorities blocked access to Vkontakte for several hours, but hundreds of demonstrators still turned out to silently protest in locations around Minsk. As Secretary Clinton has made clear, we will continue to press for the human rights and democratic aspirations of the Belarusian people. And we will continue our staunch support for those struggling to make their voices heard both online and in the streets.

The Participating States of Central Asia

In the Central Asian region, we continue to be concerned by governments' efforts to block websites, particularly when information or opinions are expressed via the Internet that are critical of government officials or policies. Media laws and registration requirements are also used to target independent activists and dissidents, which does not accord with the commitments that OSCE participating States have made to ensure freedom of expression. Internet censorship further aggravates the constraints on freedom of expression and other fundamental freedoms that impede progress and development in the Central Asian states. In order for the Central Asia region to prosper, 21st century new media technologies must be harnessed to facilitate citizens' vibrant ideas and contributions, not governments' repression.

In Kazakhstan, we have long expressed our concern that the Respublika news portal remains inaccessible to users of Kaztelecom, the government-owned Internet service provider, along with dozens of other independent sites that are intermittently blocked. In Tajikistan too, we have seen the blockage of websites disseminating independent or critical views. And in Turkmenistan and Uzbekistan, heavy monitoring of Internet content and registration requirements continue to impede free expression. In Kyrgyzstan, despite an end to official restrictions on, or monitoring of, the Internet after the April 2010 change in government, we were concerned by the Parliament's recent resolution calling for the Fergana.ru site to be banned on grounds that it is inciting ethnic hatred. We believe that full respect for freedom of expression, including via the Internet, can undergird efforts at reconciliation and accountability in Kyrgyzstan.

Russia

We welcome the Russian President Medvedev's statement at the World Economic Forum in January that: "Any attempts to limit the Internet or stifle innovation will lead the world to stagnation. Russia will not support initiatives that put Internet freedom in question." The spread of the Internet undoubtedly has had a positive effect on Russian civil society, providing new opportunities for grassroots organizations to connect with citizens and new platforms to voice alternative viewpoints and hold government accountable. However, problems associated with press freedom for print media have begun to migrate to online media as well. Russia is one of the countries "under surveillance" in the 2010 Enemies of the Internet report by the Committee to Protect Journalists.

Even when technical blocks or filtering are not deployed systematically, if people are punished physically or through legal action for peacefully expressing themselves online, Internet freedom is constrained. The threats to Internet freedom in Russia range from attacks on bloggers to criminal prosecutions of bloggers for 'extremism', to the blocking of specific sites by local service providers, denial of service (DDOS) attacks on sites site of opposition groups or independent media, and attempts by security services and some regional authorities to regulate Internet content. For example:

In November 2010, journalist and blogger Oleg Kashin was brutally beaten outside his home in Moscow. Leading human rights organizations in Russia connect the attack with material he had published on his blog.

The independent newspaper *Novaya Gazeta*came under a DDOS attack in April, while a wide-scale March DDOS attack on LiveJournal, a blog hosting site, began by targeting the blog of prominent anti-corruption activist Alexei Navalny. Navalny has also been targeted for prosecution for criminal charges alleging that he had facilitated a 2009 bad investment for a regional government in his capacity as a legal advisor. Rights groups in Russia believe that the charges are politically motivated.

Regional authorities have acted to block sites or prosecute those who produce content that they deem politically undesirable. Bloggers in Oryol, Marii El, Syktykvar, and other areas of Russia have have faced prosecution for posting insults to Prime Minister Putin or other official persons in online forums. Local authorities have acted in multiple cases to compel local service providers to block certain sites that contain materials listed on the Federal List of Extremist Materials—a problematic and expanding list of over 700 publications. Regional providers have also temporarily blocked sites of the political opposition, such as the site of the Solidarity Movement and Kasparov.ru, and independent publications like the *New Times.*

Whistleblowers also face legal retaliation. For instance, Yuri Yegorov, a blogger from Tatarstan and a former employee of the regional government, received a 6-month suspended sentence in May for libel after he alleged corruption and embezzlement on the part of Tatarstan human rights ombudsman Rashit Vagizov. His reports of corruption were later supported by other witnesses' testimonies, which were ignored by the court.

Turkey

We are increasingly concerned by the restrictions that the Government of Turkey places on Internet freedom. Turkish authorities have blocked over 5,000 websites, many with content on sensitive social and political issues. Much of this blocking is done in accordance with Turkey's 2007 Internet law, which allows the government to prohibit a Web site if there is suspicion that the site is committing any of eight crimes. These restrictions have been criticized by prominent officials within the Turkish government itself, including President Abdullah Gul.

This year has brought two new proposed restrictions on Internet freedom. Turkish authorities announced a new ban on Internet domain names that contain 138 words deemed offensive based on vague criteria. In addition, the government announced that it planned to introduce a nationwide filtering system to be implemented by Internet Service Providers. The proposal was met with widespread criticism, from the international community and from within Turkish civil society. Although some Turkish Internet associations indicate this decision may be postponed, yet the regulations are still scheduled to take effect August 22. While we understand these restrictions are allegedly designed to protect children from harmful content on the Internet, banning words in an attempt to eliminate undesirable content from the Internet cannot succeed. Major international Internet companies have voiced concerns over operating in Turkey under such regulations. If Turkey is to ensure a modern, prosperous, and peaceful society, it cannot continue to constrain the potential of the Internet for the exercise of human rights.

Azerbaijan

In Azerbaijan, Internet access is not restricted. For example, the government does not restrict web sites such as You Tube or Facebook, both of which are very popular. The government's release of young blogger-activists Adnan Hajizade and Emin Milli last fall and newspaper editor Eynulla Fatullayev this spring were positive developments.

We are concerned, however, that government officials appear to have monitored certain types of online activity, including postings on social media sites, in order to restrict freedom of assembly, specifically the activities of youth and opposition organizers who used these sites to organize anti-government demonstrations in March and April. Several of these activists—presumably identified from internet postings as organizers—were detained or imprisoned following these events. For example, youth activists Bakhtiyar Hajiyev and Jabbar Savalanli were arrested earlier this year after using the Internet for pro-democracy activism. Hajiyev, a candidate in last November's parliamentary elections, was detained on draft evasion charges pending since 2010 after he was associated with Internet postings related to March 2011 protests. International and domestic observers have alleged that the authorities prosecute draft evasion selectively, and have singled out Hajiyev because of his political activities. He was convicted on May 18 of draft evasion and sentenced to two years imprisonment. This is not the first time Hajiyev has encountered prob-

lems with the government after utilizing the Internet for social activism; in 2007 the authorities arrested him after he established a web site to protest price increases. Savalanli, a young opposition Popular Front Party activist, was convicted on May 4 and sentenced to two and a half years in prison on drug charges considered to be spurious by human rights groups.

Enduring Freedoms, New Apps

Mr. Chairman, as you know, in the past, the Helsinki process was a major international platform for defending citizens expressing dissenting views via samizdat and for protesting the jamming of radio broadcasts. Two decades ago, in response to efforts by the Ceausescu regime to restrict citizens' access to Xerox machines, an explicit commitment was included in the OSCE's Copenhagen document pledging that "no limitation will be imposed on access to, and use of, means of reproducing documents of any kind." Today, email, social networking and text messaging are new forms of samizdat as well as indispensible tools of commerce, education, and global communications.

As the United States has done since the inception of the Helsinki Process, so, too, in this new century, we stand with those in the OSCE region who seek to peacefully exercise their fundamental freedoms and promote and protect human rights, including via new technologies.

I commend Lithuania, which has made key themes of its Chairmanship media freedom via old and new technologies and the safety of journalists. We are particularly grateful for the tireless efforts of the OSCE Representative on Freedom of the Media Ms. Dunja Mijatovic and her dedicated staff to ensure that fundamental freedoms can be exercised via digital media, and I am delighted that she is here with us today. Last week, she co-organized with the OSCE Office for Democratic Institutions and Human Rights a Supplementary Human Dimension Meeting on Promotion of Pluralism in New Media. Her office is working on a matrix representing Internet laws and policies in the OSCE region to identify and encourage best practices and adherence to OSCE commitments on freedom of expression. Additionally, her office provides critical training to journalists in Central Asia and the Caucasus, as well as legal reviews of OSCE participating States' legislation, to advance broader respect for freedom of expression norms. Perhaps most critically, Ms. Mijatovic has been a voice for bloggers, journalists and other activists who are harassed or imprisoned for their work to disseminate independent information that is essential for democratic development.

Mr. Chairman, the Commission has long supported the vital role that non-governmental organizations play in the OSCE process. I am pleased to say that we are exploring creative ways that we can help connect human rights and democracy activists across the OSCE region through new technologies in order to enhance their ability to network with one another and leverage the contribution of their ideas and insights to the work of the OSCE. On her trip to Vilnius last week, Secretary Clinton spoke at a "tech camp" we organized to help civil society groups from the OSCE region and beyond use these new technologies most effectively.

I want also to emphasize, Mr. Chairman, that cyber issues are relevant to all three dimensions of the OSCE. As we partner with other governments, civil society and the business sector on ways we can safeguard against very real cyber security threats, we do so ever mindful that the measures we take must be consistent with our human dimension commitments to respect the exercise of human rights and fundamental freedoms.

Mr. Chairman, last year, in the run-up to the OSCE Summit in Astana, the U.S. advanced language for inclusion in the Summit Action Plan stating that the participating States, in fulfillment of their longstanding OSCE commitments, will permit their people to peacefully exercise their rights to freedom of expression, peaceful assembly and association through Digital Age technologies. The language did not aim to create new commitments; rather it was designed to reinforce the message that existing commitments to respect human rights and fundamental freedoms apply in the Digital Age. The language represents a conceptual breakthrough in that it recognizes that individuals and members of civil society organizations utilize digital technologies not only to exercise freedom of expression, but also to connect, network, form organizations, and gather in both virtual and real space. The language also highlights a key human dimension priority: defending and supporting the vital role of civil society in human rights protection and democratic development.

In Astana, our negotiators worked to advance our Digital Age language along with highly compatible language from the European Union related to freedom of expression.

As you know, Mr. Chairman, the Astana Summit did not adopt an Action Plan. We intend, however, to renew our efforts to advance our language on Human Rights

and Fundamental Freedoms in the Digital Age with a view to its adoption at the OSCE Ministerial in Vilnius this December. OSCE's adoption of the Digital Age language would, I believe, mark the first time that any regional organization formally recognizes that respect for the full range of human rights and fundamental freedoms must extend to the use of new technologies.

The United States will take every opportunity to work with the Lithuanian Chair, the EU, other participating States and civil society to ensure that the OSCE sends a clear message from Vilnius on Internet Freedom. If I were to distill that message into a tweet to the world, it would be: "Enduring Freedoms, New Apps."

Mr. Chairman, when he signed the Helsinki Final Act 35 years ago, President Ford famously said that: "History will judge this Conference not by what we say here today, but by what we do tomorrow—not by the promises we make, but by the promises we keep." He was right then, and his statement is even more true today. In this Digital Age, keeping our promises greatly depends on ensuring that the Internet is open and free.

Thank you, Mr. Chairman. Now I would be happy to answer your questions.

BIOGRAPHY OF DR. DANIEL B. BAER

Term of Appointment: November 23, 2009 to present

Daniel Baer was sworn in as a Deputy Assistant Secretary for the Bureau of Democracy, Human Rights, and Labor on November 23, 2009.

Dr. Baer's portfolio for the Bureau of Democracy, Human Rights, and Labor includes the Office of East Asian and Pacific Affairs, the Office of African Affairs and the Office of Multilateral and Global Affairs.

Prior to joining the Department of State, Dr. Baer was an Assistant Professor of Strategy, Economics, Ethics, and Public Policy at Georgetown University's McDonough School of Business, where he taught business ethics to MBA and undergraduate students. In 2007–2008 he was a Faculty Fellow at the Edmond J. Safra Foundation Center for Ethics at Harvard University.

From 2004–2007, Dr. Baer worked at The Boston Consulting Group where he was a Project Leader and provided strategic advice to leaders in the corporate, government, and non-profit sectors.

A Colorado native, Daniel Baer holds doctoral and masters degrees in international relations from the University of Oxford, where he was a Marshall Scholar. He received his undergraduate degree from Harvard University in social studies and African American studies.

PREPARED STATEMENT OF DUNJA MIJATOVIC, REPRESENTATIVE ON FREEDOM OF THE MEDIA, OSCE

1. Introduction

For centuries, the right to be heard has been seen as the cornerstone of democracy—it enables other rights to exist. In the age of the borderless Internet, the protection of a right to freedom of expression *"regardless of frontiers"* takes on new and more powerful meaning. The argument for freedom of expression on the web is a double-edged sword and is a hotly debated issue. On the one side it is upholding civil rights and on the other allowing governments and censors to question people's own judgment. The Internet, at its best, is a cyber experience on every single topic imaginable from personal pages detailing the life and thoughts of a school child to multinationals promoting their wares online.

Governments, however, have already begun to impose controls on the Internet, threatening the potential of this new medium. As an international community of users and providers of information, we are at a dramatic turning point. The Internet will change the way people live: it offers extraordinary opportunities for enhancing creativity and learning, for trading and relating across borders, for safeguarding human rights, for realizing democratic values and for strengthening pluralism and cultural diversity. The change holds promise and it holds challenges. One of the major challenges is to confront ways in which to spread access to the Internet so that the whole world can benefit, rather than creating gaps between the information rich and information poor.

The individual decides what he/she does not want to see, not the authorities. In a modern democratic and civil society, citizens themselves should make the decision on what they want to access on the Internet; as the right to disseminate and to receive information is a basic human right.

The exploration of cyberspace can be a civilization's truest, most challenging and also very controversial calling and adventure. The opportunity is now before the mankind to empower every person to pursue that opportunity in his or her own way. However, the exploration of cyberspace brings both greater opportunity, and, in some ways, more difficult challenges, than any previous human adventure.

The internationally distributed and interactive nature of the Internet means that any attempt to deal with the Internet in isolation from other countries will be very difficult to accomplish. National actions must fit into a pattern of international understanding on the best ways in which to deal with Internet content issues.

The Internet is the fastest growing medium ever. While it took the United States, for example, 38 years to reach 50 million radio users and 10 years to reach the same number of television viewers, it only took 5 years in the case of the Internet. [1]

We already live in the digital age, a time in which we can create truly democratic cultures with participation by all members of society; and in only a few years from now this participation will virtually include most of the world's citizens.

It will not be enough to provide citizens, particularly in rural or less-developed parts of this world, with a connection and web-compatible devices. For consumers to become what we now call "netizens" it is indispensible to understand the information, and subsequently know how to critically assess, how to process and how to contextualize it. The technological advancement in order to reach out to all has to go hand-in-hand with education, with programs on media literacy and Internet literacy.

But it remains true, that in our globalized world where education, information, personal development, societal advancement and interaction, and participation in political decision-making are to a great extent realized through the Internet, the right to access the web becomes a cornerstone for the fundamental right to freedom of expression. The right to seek, receive and impart information not only includes the right to access but presupposes it.

So, despite progress, some challenges and preconditions remain. The first one is surely *access to the Internet.* Without this basic requirement, without the means to connect, and without an affordable connection, the right to freedom of expression and freedom of the media become meaningless in the online world. The second one is *restricting free flow of information* on the Internet. I would even go so far to say that the free flow of information is oxygen of cyberspace! Without it the Internet becomes a useless tool.

Why do certain Governments try to block, restrict and filter this flow? To protect us from terrorism, extremism, child paedophilia, human trafficking and other forms

[1] Source: Morgan Stanley: The Internet Retailing Report, at: http://www.morganstanley.com/institutional/techresearch/pdfs/inetretail__1997.pdf

of threats, and make our societies more secure? All mentioned are legitimate reasons that should not be challenged by anyone.

But to protect us from criticism, satire, provocative and shocking comments, differing views, tasteless and controversial content? For that they do not have permission. We as citizens that voted for them never asked or obliged them to shape our minds and opinions.

There is no security without free media and free expression and, no free expression and free media without security. These two terms should come hand in hand and not fight each other like we see in so many parts of the world; and there is no better place to discuss and fight for both than in the OSCE. Security and human rights are both at the heart of the Helsinki Process and the Astana Commemorative Declaration as well as the OSCE principles and commitment that we share. So, why do we still struggle and why are we afraid from words? Where dos this fear from words comes from?

The Internet epitomizes the tremendous changes media has undergone in the last few decades. Dramatic technological changes have resulted in an unprecedented increase in the number of outlets and channels, a dramatic reduction of distribution costs and even the emergence of entirely new forms of journalism.

On the other hand, the very same technological changes that are manifest on the Internet seem to undermine the traditional ways print media use to finance themselves, erode the quality of journalism and challenges readers, viewers and listeners to rethink their views on what is quality media.

One requirement however, has not changed, namely the OSCE obligation of governments to guarantee freedom of the media.

It is therefore important to recall the major OSCE Commitments regarding pluralism, the free flow of information and the Internet, including the Budapest Summit 1994,[2] the 1999 Charter for European Security,[3] and the OSCE Permanent Council Decision No. 633 of 2004.[4]

Our common goal of achieving the promises we made should be a free, open and safe Internet. Very simply, when services are blocked or filtered, users of Internet platforms everywhere cannot be served effectively. While many governments have welcomed this trend, some have recoiled at the new openness—and are doing their best to make sure that the Internet is a restricted space.

Today, many governments disrupt the free flow of online information. Popular tactics include incorporating surveillance tools into Internet infrastructure; blocking online services; imposing new, secretive regulations; and requiring onerous licensing regimes.

And with the development of the Internet, some new features never considered before, such as blogging and citizen journalism have now arisen. With this in mind, let me now give you an overview of the situation regarding Internet freedom in the OSCE region.

2. Freedom of the Internet in the OSCE Region

There are an estimated 2 billion Internet users worldwide, 750 million of which live in the OSCE region. In order to bring more light on Internet regulation across the region, my Office commissioned a report by renowned Internet and media lawyer, Professor Yamam Akdeniz of Bilgi University in Istanbul.

This first OSCE-wide study on content regulation was launched on July 8 and it revealed, *inter alia,* the following:

1) A number of participating States introduced policies which could be used to completely "switch off" Internet access during times of war, in a state of emergency and in response to other security threats. Although these countries, Azerbaijan and Bulgaria, for example, have not made use of this legislation, it is, nonetheless, a

---

[2] At the Budapest Summit in 1994, the participating States reaffirmed *"...that freedom of expression is a fundamental human right and a basic component of a democratic society. In this respect, independent and pluralistic media are essential to a free and open society and accountable systems of government. They take as their guiding principle that they will safeguard this right."*

[3] In the 1999 Charter for European Security, the participating States reaffirmed *"...the importance of independent media and the free flow of information as well as the public's access to information. We commit ourselves to take all necessary steps to ensure the basic conditions for free and independent media and unimpeded transborder and intra-State flow of information, which we consider to be an essential component of any democratic, free and open society."*

[4] In OSCE Permanent Council Decision No. 633 of 2004, explicitly including the Internet, the participating States pledged to: *"...take action to ensure that the Internet remains an open and public forum for freedom of opinion and expression, as enshrined in the Universal Declaration of Human Rights, and to foster access to the Internet both in homes and in schools." "...to study the effectiveness of laws and other measures regulating Internet content."*

cause for concern that these "Internet kill switch" laws COULD be used to suspend communication services for parts of or entire populations.

The "Internet kill switch" idea was also considered by the United States, allowing the president to shut down critical computer systems in the event of a national cyber emergency. I welcome the fact that the U.S. Senate DID NOT act on the proposed measure.

2) Some governments already recognize access to the Internet as a human right. This trend should be supported as a crucial element of media freedom in the 21st century. Access to the Internet remains the most important pre-requisite to the right to freedom of expression.

3) That freedom of expression and freedom of the media principles equally apply to Internet-related content is not recognized by most participating States. However, laws criminalizing content are applicable to all media, including the Internet. Therefore, criminal sanctions can be used to regulate online content and conduct. Content regulation developed for traditional media can not and should not simply be applied to the Internet. While rules and boundaries still exist, enforcement of existing laws, rules and regulations to digital content becomes evidently complex, problematic and at times difficult to enforce.

4) In several participating States a legal remedy provided for allegedly illegal content is removal or deletion of the offending material. The new trend in Internet regulation seems to be blocking access to content if state authorities are not in a position to reach the perpetrators for prosecution or if their request for removal is rejected or ignored by foreign law enforcement authorities. In some participating States, such as in Belarus and the Russian Federation, "prohibited information lists" exist, allowing blocking if such information appears on the Internet. Some countries, including the Czech Republic, Moldova, Switzerland and the United Kingdom also have developed state-level domain name blocking or seizure policies. State-level blocking policies undoubtedly have a very strong impact on freedom of expression. Participating States should refrain from using blocking as a permanent measure, solution or as a means of punishment. Indefinite blocking of access to websites and Internet content could result to "prior restraint". Turkey provides the broadest legal measures for blocking access to websites by specifying 11 content-related crimes. Turkish authorities have not revealed the number of websites blocked using this legislation.

5) There are definitional problems when it comes to terms such as "extremism", "terrorist propaganda," "harmful content" and "hate speech". These terms are vaguely defined and may be widely interpreted to ban speech that Internet users may not deem illegal. Clarifications are needed to define these terms.

6) The development of so-called "three-strikes" measures to combat Internet piracy in a number of participating States is worrisome. While the participating States have a legitimate interest in combating piracy, restricting or cutting off users' access to the Internet is a disproportionate response which is incompatible with OSCE commitments on freedom to seek, receive and impart information. Participating States should steadfastly refrain from developing or adopting measures which could result restricting citizens' access to the Internet. Also, an international discussion on whether or not the current standards on copyright are up to date in our information society might be necessitated.

7) Network neutrality is an important prerequisite for the Internet to be equally accessible and affordable to all. It is, therefore, troubling that more than 80% of the participating States do not have legal provisions in place to guarantee net neutrality. Finland and Norway stand out as best-practice examples with Finland having anchored network neutrality in its laws while Norway, together with the industry and Internet consumers, developed workable guidelines.

8) A considerable number of participating States have yet to decriminalize defamation. Harsh prison sentences and severe financial penalties continue to exist in defamation suits. In the Internet age, decriminalization of defamation becomes a prerequisite for free media to report without fear of criminal prosecution about issues of public importance—beyond national borders and jurisdictions. In countries where a free media scene is yet to be established, it is often foreign correspondents who assume the watchdog function. If, however, journalists face criminal charges for online publications where their stories have been read or downloaded, the ability to report freely and unhindered will be severely hampered.

9) Some participating States had problems submitting information because applicable regulatory provisions or relevant statistics were not easily retrievable. This lack of clarity makes it difficult for users and legislators to understand Internet regulation regimes. Often information, particularly pertaining to questions on blocking

statistics, was not available. Sometimes different governmental institutions and ministries are responsible for the different aspects of the Internet, hence internal co-ordination becomes complicated. Almost no participating State had an institutional focal point on Internet matters to fall back on. For the purpose of streamlined national co-ordination, the avoiding of duplicated or contradicting legislation, my Office proposes the introduction of governmentally independent national Internet focal points. This might also facilitate the maintenance of reliable information and statistics about laws and regulations, their implementation and consequences related to freedom of the media and the free flow of information.

3. Conclusions

Blocking access to the Internet or banning certain content has proven to be ineffective. Even by trying to establish "regionalized" networks it will not be possible to gain full control over the communication exchanged and information shared on the web. Any attempt to hinder the free flow of information, to disproportionally restrict the right to free expression, to block dissenting opinions or to prevent critical voices from being heard will prove to be short-sighted because a free Internet and independent media are a means and not an end in itself.

I hope that the OSCE report on freedom of expression on the Internet will serve the OSCE participating States as a valuable reference tool in advancing free speech, media freedom, and media pluralism online.

Internet as a source of pluralism:

The level of pluralism in the media is one of the major indicators of what the OSCE stands for, namely promoting pluralistic societies with democratic decision making processes, which by definition need pluralistic views and opinions to be presented freely, especially, but not exclusively, during election cycles. In this respect the Internet is an achievement and a utility which needs protection, as traditional media do. The relevant provisions and international standards, such as Article 19 of the UN covenant on Civil and Political Rights, Article 10 of the European Convention on Human rights and the OSCE Commitments regarding freedom of the media are applicable to content on the Internet. Often however, we see a trend in the opposite direction, which includes targeted and specialized legislation to address and restrict content on the Internet.

Access to Internet as a constitutional right:

Finland and Estonia introduced pioneering legislation which established the access to Internet as a constitutional right. In France, the constitutional court ruled in a similar way. In order to pay tribute to the unique contribution the Internet has given to participatory democracy, to freedom of expression and to freedom of the media, it is only fitting to enshrine the right to access the Internet on exactly that level where such rights belong, as a fundamental right with a constitutional rank. Perhaps the time is ripe to turn a new page in the history of fundamental rights and establish access to Internet as a universal human right.

It would be promising indeed to see the number grow of OSCE participating States which recognize this principle on a constitutional level.

The Internet is a fantastic resource that has fundamentally changed our societies for the better. It will continue to have a positive impact—if we allow it. The lesson is simple: The Internet must remain free.

BIOGRAPHY OF DUNJA MIJATOVIC

Dunja Mijatovic of Bosnia and Herzegovina has been appointed as the OSCE Representative on Freedom of the Media.on March 11, 2010 succeeding Miklos Haraszti of Hungary.

Mijatovic is an expert in media law and regulation. In 1998, as one of the founders of the Communications Regulatory Agency of Bosnia and Herzegovina, she helped to create a legal and policy framework for media in a complex post-war society. She also was involved in establishing a self-regulatory Press Council and the first Free Media Helpline in South Eastern Europe.

Mijatovic was appointed Chairperson of the European Platform of Regulatory Authorities in 2007, the largest media regulators' network in the world. She held this post until her appointment as the Representative.

From 2005 to 2007, she chaired the Council of Europe's Group of Specialists on freedom of expression and information in times of crisis. In that role, she was instrumental in steering a Declaration on the protection and promotion of investigative journalism through the Council's Committee of Ministers. She also played a key

role in developing guidelines on protecting freedom of expression and information in times of crisis.

Mijatovic has written extensively on "new media" topics. She also has served as a consultant on projects relating to media regulation and new technologies in Europe, North Africa and the Middle East.

She is a graduate of the University of Sarajevo, the University of Bologna, University of Sussex and the London School of Economics.

PREPARED STATEMENT OF SEC. DAVID J. KRAMER, PRESIDENT, FREEDOM HOUSE

Mr. Chairman, Members of the Commission, it is an honor to appear before you today for a very timely discussion on Internet freedom in the OSCE Region. As a former member of the Commission myself when I served in the State Department as Assistant Secretary for Democracy, Human Rights, and Labor, I always appreciate the opportunity to return to this Commission and participate in its important work.

Before delving into today's topic, Mr. Chairman, I'd like to commend you for your leadership in securing passage last week by the U.S. House of Representatives of the Belarus Democracy and Human Rights Act of 2011. This is an extremely important bill that will reinforce efforts of the Administration to pressure the Lukashenka regime and support the opposition forces and civil society. The role you personally have played on Belarus over the past decade, along with a number of your colleagues, including Senator Cardin, has been critical to showing solidarity with those who are trying to bring about democratic change and an end to Europe's last dictatorship. Lukashenka is unquestionably on the thinnest ice of his political life, and we may be celebrating his departure from power—hopefully sooner rather than later. Freedom House could then conceivably move Belarus out of the "Not Free" category that we use to rank countries around the world. More on Belarus shortly.

Mr. Chairman, whether in Belarus or elsewhere in the region, Internet freedom, like many other freedoms, is under duress in a number of countries. Before the information revolution, regimes in the region focused their efforts at maintaining control over television first and foremost, but also newspapers, radio, and foreign broadcasting. The Internet poses the latest and most promising challenge to break through the iron grip that some regimes in the area seek to maintain. By its very nature, the free flow of information poses a threat to such regimes and challenges the very essence of who they are and how they preserve control. Thus, whether via TV before or the Internet today, repressive governments show their stripes online or offline; the tactics may change, but the intent of such governments remains the same. Not surprisingly, countries that rank "Not Free" in Freedom House's *Freedom of the Press 201* report receive similar scores when it comes to Internet freedom. Their efforts to control and suppress information through more traditional means extend to the newer forms of communication as well. At the same time, it is worth noting that in most cases, countries, even those ranked "Not Free", perform better in Internet freedom than in press freedom-at least when we look at the actual scores-in large part due to the fact that many governments still have not started restricting online content to the same level they do traditional media. This is slowly changing, however, and something worth keeping an eye on.

A main difference from the past, however, is that citizens who are denied freedom of expression now have new ways to express their legitimate rights through the Internet. No longer do dissidents have to resort to mimeograph machines or handwritten copies of sensitive documents. These days, a modem and keypad will do the job, but one should not be complacent about the ability to keep the flow of technology free. Indeed, authoritarian regimes are adjusting quickly to the new types of communications that are out there. Just because many conversations are virtual these days doesn't mean they're free of government efforts to control.

In April, my organization, Freedom House, released its latest *Freedom on the Net 2011* report assessing the degree of Internet freedom in 37 countries in six geographical regions. At a global level, Freedom House has worked over the last four years to document the state of Internet freedom (our *Freedom on the Net* reports, among other ways); improve access to a wide range of censorship circumvention technologies in countries where the Internet is restricted; build indigenous capacity to promote and support the use of anti-censorship tools in highly repressive environments; provide technology developers with ongoing assessment of the performance of anti-censorship tools; and advocate to promote and support Internet freedom with national, regional and international bodies such as the United Nations.

In focusing on states of the OSCE region, we see both opportunities and challenges for states and citizens in the sphere of Internet freedom. Filtering and blocking of political and social content by governments are incompatible with freedom of expression and the free flow of information, both of which are basic OSCE commitments. Freedom House is encouraged by the role of the OSCE in pressing for accountability among participating States for upholding commitments on freedom of expression in the new media realm. I want to acknowledge the very positive and active role of my fellow panelist, Dunja Mijatovic, the OSCE Representative on Freedom of the Media. She has done an excellent job in raising the profile of media freedom issues broadly—including with a conference last month in Vilnius, Lithuania on protecting journalists that I was privileged to attend—and Internet free-

dom specifically, and it's a pleasure to be with her here this morning. I also want to recognize the solid work that Dr. Daniel Baer and his colleagues in the State Department's DRL Bureau are doing in this area.While much of the world's attention the past few months has been focused on the volatile Middle East, citizen activism against repressive governments, through the connective power of online media, is spreading to the OSCE region. And so let me turn to some specific countries and challenges that we face there.

Belarus

Arguably nowhere more than in Belarus do we see the competing efforts of citizens fighting to preserve the openness of the Internet to advance the cause of freedom and the government seeking to crack down on everything, including the Internet and the free flow of information. In recent weeks, Lukashenka's regime has been at a loss to stop a growing number of young activists from taking to the streets to protest against the country's economic crisis, for which Lukashenka deserves full blame, and the Internet is the source for their mobilization, with echoes of the Arab Spring reverberating. Over the course of the last month, 1,800 have been detained in street protests organized via online media (silent "clapping protests") namely, Facebook and VKontakte.

Lukashenka has retorted that peaceful demonstrations are meant to "sow uncertainty and alarm, to destroy social harmony, and.bring us to our knees and bring to naught our hard-won independence." What is clear is that the people of Belarus are signaling that they have had enough of Lukashenka. And he is striking back against these increasingly tech-savvy, peaceful, clapping citizens. My money is on the citizens in this showdown, and our support should be with them unstintingly as well.

The Belarusian government desires to suppress the free flow of information, and the Internet is simply the latest frontier. The authorities impose severe restrictions on all news outlets, and the security services have increasingly attempted to introduce various Internet surveillance technologies. A presidential decree signed in February 2010 and subsequent regulations provide a legal basis for extensive censorship and monitoring of the Internet. The rules concerning using the Internet are quite restrictive. The users who access the Internet from home, are subject to regular checks and can easily be tracked by IP address. Going online from an Internet cafe one must present identity documents. The administration of an Internet cafe is obliged to keep the details of the user, along with the information about the visited websites, social networks and other online activity for a certain period of time; this information can be provided for investigation upon request. Internet service providers must also ensure state registration of their personal and their client's information networks, systems, and resources in order to carry out activities inside Belarus. For using wireless Internet (either through buying Internet cards or going online from any public place that has free wireless network), identification is needed beforehand. These mechanisms are deliberately designed to eliminate anonymous use of the Internet. Such Internet monitoring and filtering runs counter to OSCE norms and commitments.

Nonetheless, in an effort to diffuse the impact of these latest online calls to protest, the government has resorted to a number of repressive steps via multiple tools such as spamming online threads about protests; misusing hashtags; and creating fake Twitter accounts to undermine actual activists. In this last method, pro-government bloggers referenced messages on these fake accounts to help spread disinformation. But old habits are hard to break, especially when your security services are still called the KGB, and so the Belarusian regime also relies on its tried and true methods of control by harassing the VKontakte administrator and asking for users' passwords (during the last month of protests).

The government's desire to suppress the free flow of information was also on display during and immediately following the December 2010 presidential election: international connections were blocked and users couldn't use Facebook, Twitter, or send secure Gmail messages. Fake mirror websites were created to divert users from accessing independent news sources. Opposition websites and news sites were hijacked.

While the Belarusian government has promoted the use of the Internet for economic purposes—even though Lukashenka has been quoted as calling the Internet "trash"—the impact of the new medium in the political sphere remains limited. In fact, the Belarusian Internet is monopolized by a governmental provider—Beltelecom, which is subsequently re-selling the traffic to other commercial providers. Moreover, heightening the challenge digital activists face, according to the OpenNet Initiative, 70 percent of all Belarusian Internet traffic goes through Russia

and is reviewed by the Russian mechanisms for "operational and investigative activities" (SORM) and "authorities for national security.'

Recent years have seen an increase in Internet use and mobile-telephone penetration in Belarus. Some 27 percent of the population uses the Internet and 93 percent of the population uses mobile phones. However, state-imposed and other infrastructural restrictions significantly constrain Belarusians' ability to fully access these technologies and related applications. Internet costs in Belarus are higher than in all neighboring countries

Online activists and web-based journalists face extralegal harassment, mostly in the form of phone calls or intimidating messages. Independent civil society is also subject to electronic attacks such as distributed denial of service attacks (DDOS). Charter97 suffered a very well documented DDOS attack after the 2006 elections. More recently they have been subject to a very intense and prolonged DDOS attack over the last 3 weeks. However, until 2010, physical attacks were not common. For that reason, the death of the founder of Charter97, Aleh Byabenin, prompted many questions among his colleagues and fellow journalists. Byabenin was found hanged from a stairway at his summer home in September 2010. Although the authorities declared his death a suicide, most independent sources questioned the official version and suspected foul play.

Belarus is ranked "Not Free" in *Freedom on the Net 2011*; it is also ranked "Not Free" in Freedom House's *Freedom of the Press 2011* report.

Azerbaijan

Although Azerbaijan's Internet usage has increased in recent years, authorities have attempted to exercise greater control, particularly in the wake of the Arab Spring. The government routinely blocks public access to various websites that are critical of the government and among the most targeted are the websites of the newspapers published by the main opposition parties, as well as the Radio Free Europe/Radio Liberty's Azerbaijani service (RFE/RL). It is widely believed that surveillance of Internet communication, as well as SMS and phone conversations is common practice, as demonstrated in the case of the Ministry of National Security's interrogation in 2009 of 43 Azerbaijanis who voted for the Armenian song in the Eurovision contest. Internet restrictions are particularly frequent in the autonomous exclave of Nakhchivan, where the most severe restrictions on the freedom of speech and freedom of assembly are reportedly imposed by the personal order of the chief of the executive authority Vasif Talibov. The recent jailing of online youth activists, such as Jabbar Savalan (sentenced to 30 months, supported Arab Spring inspired protests) and Bakhtiyar Hajiyev (a former parliamentary candidate, sentenced to 2 years), has a further chilling effect.

Yet the expansion of the online media is for now mostly limited to the capital Baku and a few large cities, in part due to poor infrastructure and the cost of Internet access in the country. The vast majority of the population is not able to access the web, or has service that is so slow it cannot enjoy Web 2.0's potential.

On June 22, the Azerbaijani Popular Front Party issued a statement condemning the restrictions imposed by the government on Internet access of key members of the main opposition party over the last three months. The Party linked these attempts to the government's concern over the increase in political activity. The violations referred to include:

- Websites of the main opposition newspapers were experiencing several attacks and access restrictions in the recent months.
- The personal blog site of Mr. Ali Karimly, the Party's chairman, was taken down by a hacker attack; even after it was restored, he was unable to add new content, which was claimed to have been caused by unknown restrictions imposed on his IP address.
- Later, Internet access to Mr. Karimli's apartment cut off for a month under various excuses.
- Three of Mr. Karimli's deputies (Gozal Bayramli, Fuad Gahramanli and Razi Nurullayev) also faced Internet restrictions, including technical difficulties and reduced speed.

The government has also tried to suppress their activities in social-networking sites. Mr. Gahramanli's Facebook page was hacked and is being used to slander the opposition to this day. The Facebook page of Natig Adilov, head of Party's press service, has been blocked twice in the past few months due to a large number of false complaints/reports.

Azerbaijan is ranked "Partly Free" in *Freedom on the Net 2011*; it is also ranked "Not Free" in Freedom House's *Freedom of the Press 2011* report.

Russia

In Russia, the Internet landscape is complicated, like the country. Many view Russia as a "country at risk" given the likelihood that authorities will look to consolidate control over means of communication in the lead-up to the December parliamentary and March 2012 presidential elections. Citizens and bloggers are becoming increasingly active online, and so is the government. Since the Internet was first launched in Russia, the country has made significant gains in the expansion of its information infrastructure. Most Russians access the Internet from their homes (94 percent of users) and workplaces (48 percent), and use of cybercafes has consequently dropped off. Internet access via mobile telephones and similar devices has gained popularity since 2006, and 9.4 million people report using this method. Faster and more credible than conventional media, online outlets are becoming the main information source for a growing number of Russians, and certain websites have larger audiences than television channels.

Where traditional forms of media are more actively restricted, the Internet in Russia has become a space for relatively free speech and discussion. Applications like the social networking site Facebook, the Russian social networking site VKontakte, the microblogging platform Twitter, and various international blog-hosting services are freely available. Unlike, say, in China where Internet control is a repressive blanket, in Russia, government leaders are using subtle control methods not designed (usually) to prevent the transmission of information but instead to shape and control it, often by disseminating propaganda and by placing pressure on Internet access providers. Under the ideological umbrella of managed democracy, the government is trying to have the Internet suit its own purposes. President Medvedev is active as a blogger and a tweeter. But there has been on-and-off discussion in Russian political and security circles about the need to rein in Internet providers. The Internet in Russia is regulated by the Federal Service for Monitoring Communications, Information Technology, and Mass Communications, whose director is appointed by the Prime Minister. It is currently using a tactic that has been effective in spreading a climate of fear among print journalists—it publicly goes after a few known dissident voices and bloggers. Russian authorities have used current laws against "extremism" effectively to punish dissenting voices, including several bloggers who have been prosecuted under such charges, and have checked several opposition news portals for "extremist" content.

Bloggers have been actively covering the citizen's movement to defend the Khimki Forest from damaging construction of a highway that would run through the forest. While bloggers were freer in their ability to get the word out, they still faced the same repression after expression; journalists and bloggers have been assaulted and arrested for daring to contradict official interests in the forest. Several journalists/bloggers who actively opined on the Khimki Forest issue were savagely beaten—Oleg Kashin last November and Mikhail Beketov in September 2008—and many more harassed and threatened. Their attacks serve as brutal reminders of the dangers bloggers and digital activists face from various interest groups, whether it be those in power (locally or nationally) or business groups. And yet corruption issues have broken through and galvanized citizen action. Blogger Alexey Navalny is the most recent and public example: on his blog, he has bravely exposed possible corruption in Russian oil companies, banks, and government agencies, and he has also launched a site RosPil, dedicated to exposing state corruption, where he invites readers to review public documents for malfeasance and post their findings. Suspicious government contracts, totaling millions, have been annulled, as a result of Navalny's efforts. Yandex was forced by the FSB security agency to hand over details of contributors to Navalny's website. Notwithstanding government pressure, Navalny has persisted in his online efforts; in a recent controversial blog, Navalny asked legal authorities to investigate the legitimacy of the Russian People's Front initiated by Prime Minister Vladimir Putin.

The Internet has also given voice to those who in the past had not had a way to speak out. As is the case in Russia in the online and offline world, freedom of expression is still always a dangerous endeavor. The case of Aleksei Dymovsky, the Russian police officer who triggered a political storm in 2009 by blowing the whistle on rampant police corruption through widely viewed videos posted on the Internet, is a perfect example. His courage earned him instant dismissal from his job, a brief time in jail on fraud charges, as well as threats against him and his family. By speaking out, however, he emboldened others to do the same in a series of similar Internet postings in which fellow law-enforcement officers described how police routinely extort money from ordinary Russians. Most whistle-blowers eventually face harassment, prosecution, or both. Unfortunately, in the new police law which went into effect in March, there is a troubling provision in the law banning police officers from discussing their superiors' orders publicly or voicing their opinions in the

media. It is tough to feel hopeful in a country where speaking out rarely leads to an improved situation.

Russia is ranked "Partly Free" in *Freedom on the Net 2011*; it is also ranked "Not Free" in Freedom House's *Freedom of the Press 2011* report.

Kazakhstan

Kazakhstan's government has sought to make the Internet a new source of economic strength and views it as a vehicle to build the country into the information-technology hub of Central Asia. With that goal in mind, the government has made modest efforts to liberalize the telecommunications sector, promote Internet usage, and enhance the Internet portals of state entities. At the same time, the authorities also attempt to control citizens' access to information and seemingly fear the Internet's democratizing potential. In recent years, the government has blocked a popular blog-hosting platform and passed several pieces of legislation that restrict free expression online, particularly on topics that are deemed threatening to President Nursultan Nazarbayev's power and reputation. Opposition blogs and websites face particular pressure.

Even during its stint as OSCE chairman, Kazakhstan did little to ameliorate the status of Internet freedom. According to Freedom House's most recent *Freedom on the Net* survey, select Web 2.0 applications have been blocked in the country, and the authorities regularly exercise substantial political censorship. In an effort to restrict content from government critics, state-owned Internet providers blocked the popular blogging site LiveJournal in 2008 (it was open again only in November 2010, a few days before the OSCE summit), while the site Blogger.com was restricted throughout much of 2010; in 2011, Kazakh providers blocked Wordpress.com, another popular blogging platform. While the Kazakh Center of Network Information was originally established as a nongovernmental organization to manage the .kz domain, it reportedly has 80 percent government ownership and regularly makes politicized decisions on registering sites on the domain. In July 2009, President Nazarbayev signed amendments that identified all online resources (including blogs, forums, Internet shops etc.) as mass media with judicial responsibility and blocked all resources that carry content that could be used in an "information war against Kazakhstan." Taken together with the law that conferred Nazarbayev the status of "Leader of the Nation" and attached criminal responsibility to public insults to the President, these trends have only heightened the level of self-censorship in the nation. While the "For a Free Internet" campaign has organized flash mobs, monitored blocked websites, and filed 120 resultant lawsuits, the operating environment overall and government restrictions in Kazakhstan are such that large-scale civic activism on Internet freedom is not entirely feasible.

Kazakhstan is ranked "Partly Free" in Freedom on the Net 2011; it is also ranked "Not Free" in Freedom House's Freedom of the Press 2011 report.

Turkey

Internet and mobile-telephone use in Turkey has grown significantly in recent years, though access remains a challenge in some parts of the country, particularly the southeast. The government had a hands-off approach to regulation of the Internet until 2001, but it has since taken considerable legal steps to limit access to certain information, including some political content. According to various estimates, there were over 5,000 blocked websites as of July 2010, spurring street demonstrations against Internet censorship. (Note: some estimates are much higher but those include pornography sites, not politically oriented ones.)

In the latest public reaction to Internet censorship, tens of thousands of people joined nationwide protests in May and June against the current regime's decision to introduce a countywide mandatory Internet filtering system that will go into effect on August 22, 2011. According to a recent study commissioned by the OSCE Office of the Representative on Freedom of the Media, if realized this decision will lead to the first government controlled and maintained mandatory filtering system within the OSCE region.

In *Freedom on the Net 2011*, Freedom House notes that government censorship of the Internet, including some political content, is relatively common in Turkey and is on the rise. The new mandatory filtering system follows on the heels of Law No. 5651, widely known as the Internet Law of Turkey, which the government enacted in May 2007. One troubling provision allows the blocking of websites that contain certain types of content, including websites deemed to insult Mustafa Kemal Ataturk, modern Turkey's founding father. Domestically hosted websites with proscribed content can be taken down, and those based abroad can be blocked and filtered through ISPs. The procedures surrounding decisions to block websites are nontransparent, creating significant challenges for those seeking to appeal.

Turkey is ranked "Partly Free" in *Freedom on the Net 2011*; it is also ranked "Partly Free" in Freedom House's Freedom of the Press 2011 report.

Hungary

While Freedom House did not include Hungary in its recent Freedom on the Net report, it is worth noting that the Hungarian parliament passed a controversial media law last year, portions of which (related to broadcast media) went into effect on January 1. Other parts (more relevant to print and the Internet) went into effect on July 1. The new law gives authority to a newly created media agency to impose large fines on any media outlet that violates "public interest, public morals, or order," all terms that are extremely vague. After an outcry from the international community, the law was modified (e.g. online media are no longer required by law to provide "balanced coverage" and very demanding registration requirements were relaxed, among other things), but several worrisome and vague provisions remain—all media providers need to "respect human dignity," and "self-gratifying and detrimental coverage of persons in humiliating or defenseless situations" is prohibited.

As a result, just last week, at least one online news outlet reported that it was under investigation for offensive comments its users posted in the comments portion of its website. This has had a chilling effect, and there are several online outlets that have subsequently disabled the commenting feature on their website to minimize their liability. One challenge is the difficulty among various government agencies in interpreting the new law consistently. For example, some claim that the law is not applicable to the comments section of any website, only to the editorial content. On the other hand, others see it differently as evidenced by ongoing investigations.

Recommendations

- This Commission, government officials, activists, and others cannot stress enough the message affirmed in the report by OSCE Representative on Freedom of the Media Dunja Mijatovic that open access to the Internet is a fundamental human right of freedom of expression. The Internet, after all, is a space for mobilizing citizen engagement, holding governments accountable, and providing and accessing independent information.
- The OSCE, led by the Representative on Freedom of the Media but with strong support from member states, should continue to press all participating States to abide by their commitments on fundamental freedoms in the digital age and call out those states that fail to comply or go astray.
- We must recognize that technology can also have a negative impact on human rights and seek to remedy such negative potential.
  - Companies should conduct transparent human rights impact assessments to determine how American-made technology can adversely affect the privacy of citizens in countries that severely restrict freedom.
  - Congress should follow the lead of the European Parliament in instituting an export control regime of products that have a negative impact on Internet freedom.
- We should also recognize that support for "firewall busting" anti-censorship technologies needs to be complemented by other measures such as:
  - Training: recognition of threats, reduce vulnerabilities.
  - Urgent Response Mechanisms: To support activists in urgent need humanitarian support needs to be coupled with technology assistance.

Mr. Chairman, authoritarian regimes around the world are coordinating their efforts at cracking down on the Internet, or infiltrating it to go after digital activists. They share firewall technologies, pose as activists, and threaten to shut down flows of information when all else fails. Those of us in the democratic community of nations need to do a better job in confronting these threats, protecting the fundamental freedom of expression represented through open Internet access, and standing in solidarity with those who are looking to open space virtually in repressive societies. The Internet affords huge opportunities for expanding freedom around the world, not least in the OSCE region, but it also needs support and protection against such threats. The communications revolution means we live in a different world, and supporters of freedom and democracy must keep up with these changes better than they have to date and certainly better than authoritarian regimes. Thank you.

BIOGRAPHY OF DAVID J. KRAMER

David J. Kramer is President of Freedom House, which he joined in October 2010. Prior to joining Freedom House, Kramer was a Senior Transatlantic Fellow at the German Marshall Fund of the United States. He was an Adjunct Professor at the Elliott School for International Affairs at The George Washington University. Before joining GMF, Kramer served as Assistant Secretary of State for Democracy, Human Rights, and Labor from March 2008 to January 2009. He also was a Deputy Assistant Secretary of State for European and Eurasian Affairs, responsible for Russia, Ukraine, Moldova and Belarus affairs as well as regional non-proliferation issues. Previously, he served as a Professional Staff Member in the Secretary of State's Office of Policy Planning. Before that he served as Senior Advisor to the Under Secretary of State for Global Affairs. He also was Executive Director of the U.S. Advisory Commission on Public Diplomacy in Washington. Kramer received his M.A. in Soviet studies from Harvard University and his B.A. in Soviet Studies and Political Science from Tufts University.

PREPARED STATEMENT OF RAFAL ROHOZINSKI, SENIOR SCHOLAR, CANADA CENTER FOR GLOBAL SECURITY STUDIES AND THE CITIZEN LAB, UNIVERSITY OF TORONTO

Chairman, distinguished members of the Commission,

I'd like to thank the Commission for the opportunity to appear and testify at today's hearing, which comes at a particularly important moment. The Internet has precipitated perhaps the fastest and largest expansion of rights in human history. And yet we are also at a constitutive moment—where our actions, and leadership can lead to two opposing outcomes. One promises a future of greater freedoms and transparency; the other threatens a return to a darker, more authoritarian past.

My name is Rafal Rohozinski, I am a senior scholar at the Canada Center for Global Security Studies, and the CEO of the SecDev Group and Psiphon Inc. For the past 10 years I've been a Principal Investigator of the OpenNet Initiative, a collaborative international research project between the University of Toronto, Harvard University, Cambridge University, and the SecDev Group, which has studied and documented the practice and policy of Internet censorship and surveillance worldwide. We have published more than two dozen case studies and thematic reports and are in the process of publishing our third volume documenting censorship practices in over 70 countries worldwide. The OpenNet Initiative has amassed the largest, most complete profile of how countries seek to shape access to cyberspace using a combination of regulation, repression, and technical means.

Just over 65 years ago, Winston Churchill warned an American audience of the danger of an Iron Curtain falling across Europe—casting a shadow of authoritarianism and depriving citizens of their democratic rights. Churchill spoke in 1946, at a time when the United States stood uncontested as a global power. He urged the creation of norms and institutions that would safeguard freedom, and actively oppose the forces of authoritarianism. For Churchill, the end of World War II was a constitutive moment: the choices made by the victorious Allies would have enduring consequences for the cause of freedom in Europe, and elsewhere.

Today, we stand at the threshold of a similar constitutive moment brought about by a revolution whose long-term consequences we are only now starting to grasp. For the past two decades, the emergence of the Internet and cyberspace has led to the largest sustained global expansion of knowledge, rights, and freedoms. Over a third of all humanity is connected to the Internet, and there are almost as many cell phones in circulation globally there are people. Significantly, we are now seeing the coming-of-age of the "digital natives" who have grown up knowing only a connected world. Two-thirds of those currently accessing cyberspace are under the age of 25, and over 80% use at least one form of social media.

But the numbers do not do justice to the social significance of this expansion. This revolution is so pervasive and so all encompassing that it's difficult to see just how fundamentally it has changed the exercise of individual human rights, how much it has added to the cause of basic freedoms, and the ability of all peoples—no matter how small—to make their voices heard. We need not look further than the Color Revolutions of the Commonwealth of Independent States, or the recent Arab Spring, to witness the extraordinary power of the networked social movements.

But the tectonic plates of cyberspace are also shifting. The US—once the heartland of the Internet—now makes up approximately 13% of the global Internet connected population. Europe and the US together constitute approximately 40%. The center of gravity is fast shifting to the South and East. The consequences of the shift are of direct relevance to today's proceedings.

A **Digital Curtain** is descending across the globe that threatens to reverse the gains made possible through the emergence of the global commons of cyberspace. Just over half of the world's Internet-connected population live under one form online restriction or another, and that number is fast rising. Since 2003, when we first documented the emergence of the "Great Firewall" of China, more than 45 states worldwide have adopted similar means for turning the Internet from a global commons into a gated community.

Eurasia, and in particular the states of the former Soviet Union, are a petri dish of experimentation in new forms of online repression that deprive citizens of the means to demand transparency from their leaders, accountability from their governments, and the right to seek social and political change.

These new forms of restrictions, which we have documented as second and third generation controls, leverage the ability of governments to create restrictive legal environments that attempt to enforce self-censorship through fear of punishment. They also include the application of sophisticated technical means, just-in-time blocking, disrupting access to critical information resources at times when they are most needed, sowing disinformation, and otherwise manipulating information flows—as well as the use of targeted online attacks, denial of service, injecting false

content, and sophisticated information operations turned inwards at the domestic populations. These controls are pervasive, but also applied selectively, such as during elections, in order to discredit legitimate opposition groups and deprive them of the right to free and unfettered speech.

In Kazakhstan, Uzbekistan, Turkmenistan, Russia, and notably in Belarus, these techniques have been used with great success to silence opposition groups, driving them and their followers offline. In fact, the Internet is subject to some form of control in all post-Soviet states. Indeed, the mechanisms for control are getting deeper and more coordinated through regional bodies such as the Shanghai Cooperation Organization, and the Collective Security Treaty Organization, as well as via bilateral cooperation between governments and their security services.

Tragically, perhaps, we are complicit in this growing trend towards authoritarianism. Our own fears of cyber insecurity and terrorism make it easier for others to appropriate these terms to justify political repression.

The label "terrorists" can be applied to anyone inconveniently opposed to the political status quo; and calls for changing the Internet, introducing greater security, and the ability to identify users—helpful in tracking down hackers and cyber criminals—find their place in the arsenal of repressive regimes as a means of selectively prosecuting human rights activists, journalists, or anyone seeking to struggle for social and political reform.

Our emphasis on harmonizing laws on cybercrime and seeking global solutions to cyber security paradoxically makes it difficult to assert and demand respect for freedom of expression and access to information online.And security is not the only means by which rights can be suppressed. Net neutrality, copyright enforcement, and the empowerment of telecommunications carriers to "clean pipes" are convenient means for regimes with less than Democratic tendencies to offload and outsource policing and ultimately repression.

There are no simple solutions to these challenges, only difficult trade-offs. To paraphrase the words of the immortal Pogo, "we have met the enemy and he is at least partially us."

So what is to be done?

Future historians will look back at this time and see it as a constitutive moment. Before us are some hard choices—but also clear norms and ideals that have been core to the Euro Atlantic alliance over the past 50 years, and part of our shared cultural and historical heritage.

Leadership comes from the courage to make the hard decisions in pursuit of a greater common good. In this respect, a commitment to an open global commons of cyberspace is by far the most important far-reaching objective for the US and its like-minded partners worldwide to support.

Security is an important obligation of the state, but must be balanced against preserving the right to dissent, communicate, and act online—even if it comes at some costs. This is especially true as the new generation of digital natives find their own voice in the online world. New forms of protest, whether they come in the form of making public confidential information, as in the case of Wikileaks, or "hacktavism" as has been exercised by LulzSec and Anonymous, may be the necessary friction for preserving a global norm that enshrines the right to seek and access information. We carefully adjust our own laws to accommodate some of the new forms of dissent that will emerge. Is there a difference between picketing an employer during a labor dispute, and making his website and Internet systems inaccessible through a denial of service attack? These are important questions and we must pause before we consider how to address them, as the rules we apply will have repercussions well beyond their own borders. In a global world, there is no such thing as a purely domestic policy.

In specific terms, at the highest level this Commission should encourage our European partners to remain committed to a global commons of cyberspace.

- Calls such as those put forward by some members of the UN to end the multistakeholder engagement on the governance cyberspace should be strongly resisted.
- Pressure should be applied through bilateral agreements, as well as by organizations such as the WTO to ensure that restricted access to content is also framed as a trade issue, with consequences and sanctions against countries pursuing these practices.
- Access to an uncensored Internet should become a basic measure of freedom and democratic progress, and should be made a condition for recipients of preferential US trade relationships or development assistance;
- Access to political content via the Internet should become a central component of monitoring the freedom and fairness of national elections—as important as the right to assembly, and balloting.

Preserving the global Internet commons will not be easy, but the costs of not doing so are greater. The rise of new superpowers in the East is occurring just as the tectonic plates of cyberspace are shifting to the same region.

The historical moment in which we live and which have expanded the means for human expression made possible a quest for knowledge, and an ability to network and act on a planetary scale—which risks becoming a fading chapter in the future where the same technologies enable surveillance societies that far exceed those which George Orwell's 1984 could imagine.

The future is ours to lose, and as in those March days of 1946 when Churchill warned of the Iron Curtain, now is the time for us to courageously make choices so that our constitutive moment—the future of Cyberspace—furthers, rather than constrains, the universal values of dignity, freedom, and the right to choose.

BIOGRAPHY OF RAFAL ROHOZINSKI

Rafal Rohozinski is one of Canada's thought leaders in the field of cybersecurity and Internet freedom. He is the founder and CEO of the Secdev Group and Psiphon inc. His work spans two decades and 37 countries including conflict zones in the CIS, the Middle East, and Africa. In 2010 Rafal was named by SC magazine as one of the top five IT security luminaries of the year; and "a person to watch" by the Canadian media. He is known for his work on cyber espionage, including coauthorship of the Tracking GhostNet, and Shadows in the Cloud and Kookface studies examining Chinese cyber espionage networks and global cybercrime. Rafal is a senior scholar at the Canada Center for Global Security Studies, Munk School of Global Affairs, University of Toronto, and previously served as director of the Advanced Network Research Group, Cambridge Security Program, University of Cambridge. He is a senior research advisor to the Citizen Lab, and together with Ronald Deibert, a founder and principal investigator of the Information Warfare Monitor and the Open Net Initiative.

Rafal is the author of numerous academic and policy papers. His recent publications include, "Stuxnet and the Future of Cyberwar" (Survival, IISS, 2011), "Liberation vs. Control: The Future of Cyberspace" (Journal of Democracy, 2010),"New Media and the Warfighter" and, "Strategic utility of cyberspace operations" (US Army War College), and "Risking Security: Policies and Paradoxes of Cyberspace Security" (International Political Sociology, 2010). His is also a lead editor and contributor to *Access Denied: the practice and policy of global Internet filtering* (MIT, 2009), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (MIT 2010), and *Access Contested: Security, Identity, and Resistance in Asian Cyberspace* (MIT, 2011). His forthcoming book (co-authored with Ron Deibert), *Ghost in the Machine: The Battle for the Future of Cyberspace*, will be published by McClelland and Stewart in 2012.

Rafal's commercial ventures are active across the spectrum of cyberspace. The SecDev Group provides clients in the governments and commercial space with intelligence, toolsets, and investigations that inform policy and address risk in the information age. Psiphon inc is a leading content delivery network—delivering content and connectivity for Voice of America, Radio Farda, Radio Free Asia and the BBC into areas and regions where Internet broadcasts are censored or blocked. The Secdev Foundation—a Canadian non-for-profit—provides support and advanced research capabilities to university, public research and advocacy efforts aimed at preserving the global commons of cyberspace.

Rafal's work and research frequently appears in such publications as the New York Times, Washington Post, and the Guardian, and he has appeared as a commentator on the BBC World Service, Canadian Broadcasting Corporation, CNN, and other international media.

PREPARED STATEMENT OF IVAN SIGAL, EXECUTIVE DIRECTOR, GLOBAL VOICES

Chairman Smith, Co-Chairman Cardin, and Commission members, thank you for the opportunity to address the Commission, and the topic of online freedom of expression in OSCE countries. I am Ivan Sigal, Executive Director of Global Voices, a nonprofit organization and community of bloggers, writers, and translators from around the world who analyze and amplify the most interesting conversations appearing in citizen media for global audiences.[1] Global Voices has a team of writers who cover issues of citizen media in Eastern Europe and the former Soviet Union.[2] They are also contributors to and authors of several recent research documents that focus on online rights and freedom of expression in countries of the former Soviet Union, and examine the tactics that governments use to suppress online speech.[3] Additionally, I lived and worked in the former Soviet Union from 1996 to 2004, primarily working with local media outlets on journalism and program production and training, media law and regulation, and media sector association building, with the media development organization Internews. My testimony is informed both by the work of the Global Voices community, and my own experiences.

While I am drawing upon work of the Global Voices community, the conclusions, analysis, and recommendations are mine alone: Global Voices community members hold a diverse range of viewpoints about the U.S. government's foreign policy, international organizations, and policies of other governments including their own.

The Global Voices mission reads in part, as follows:

> *We believe in free speech: in protecting the right to speak—and the right to listen. We believe in universal access to the tools of speech. To that end, we seek to enable everyone who wants to speak to have the means to speak—and everyone who wants to hear that speech, the means to listen to it. Thanks to new tools, speech need no longer be controlled by those who own the means of publishing and distribution, or by governments that would restrict thought and communication. Now, anyone can wield the power of the press. Everyone can tell their stories to the world.*[4]

Global Voices seeks to listen to and amplify the voices of many people online, without specific advocacy positions on given issues. Instead, we support basic principles for speech and access that encourage civic participation. These concepts are in line with OSCE Charter commitments, as well as with Article XIX of the Universal Declaration of Human Rights.

To that end, ongoing restrictions and suppression of the tools of online speech in the OSCE region, the harassment, arrest, and imprisonment of individuals for exercising speech rights that are protected under OSCE and United Nations obligations, are a matter of concern, and a subject of our website's coverage.

While attacks on mass media in the OSCE region have occurred for years, and continue, with this document I am focusing mostly on attacks on individuals, citizen media communities, and social media networks. These targets have fewer resources, less experience, and face a different kind of risk than traditional mass media, which have institutional capacity, capital, and organizational standing, which, while making them targets, also offers them relatively robust protection.

Recent events have once again highlighted the disregard demonstrated by several OSCE member states seem to have for the protection of freedom of speech obligations expressed in numerous OSCE documents.[5] Specifically, we have seen restric-

---

[1] http://globalvoicesonline.org/.

[2] http://globalvoicesonline.org/-/special/runet-echo/, http://globalvoicesonline.org/-/world/ eastern-centraleurope/, http://globalvoicesonline.org/-/world/central-asia-caucasus/.

[3] "Freedom on the Net 2011: Russia," Freedom House,http://www.freedomhouse.org/images/File/FotN/Russia2011.pdf; Rebekah Heacock, "Second- and Third-Generation Controls Rise in Russian Cyberspace," OpenNet Initiative, April 7, 2011, http://opennet.net/blog/2011/04/second-and-third-generation-controls-rise-russian-cyberspace.

[4] http://globalvoicesonline.org/about/gv-manifesto/.

[5] The OSCE has commissioned an extensive report regarding the legal and regulatory environments of OSCE member states by Yaman Akdeniz titled "Freedom of Expression on the Internet" (http://www.osce.org/fom/80723) that covers legal and regulatory practices of OSCE member states in relation to the following documents: Final Act of the Conference on Security and Cooperation in Europe, Helsinki, 1 August 1975. http://www.osce.org/documents/mcs/1975/08/4044_en.pdf. Budapest Summit Declaration, December 21, 1994. http://www.osce.org/mc/39554. Lisbon Summit Document, December 3, 1996. Official text at http://www.osce.org/mc/5869. Charter for European Security, adopted at the OSCE Istanbul Summit, November 1999. http://www.osce.org/documents/mcs/1999/11/4050_en.pdf. OSCE PC.DEC/633 on Promoting Tolerance and Media Freedom on the Internet, endorsed by MC.DEC/12/04 at the OSCE Ministerial Council in Sofia, 7 December 2004. http://www.osce.org/mc/23133.

tions and attacks on access to online platforms and social media networks, in response to protesters' use of those tools to organize. Prominent recent examples include Russia, Kazakhstan, Belarus, and Turkmenistan.

Protesters in Belarus, for instance, in June and July 2011 organized, documented, and amplified protests using social media platforms such as vKontakte. The membership in these vKontake groups numbered in the thousands with at least one group with nearly 214,000 members.[6] The size of these groups intimated the possibility of mass protests in Belarus, in rallies initially set for June 22, 2011.

The response of the Belarus government has been a creative mix of hacking and distributed denial of service (DDoS) attacks on vKontake groups, disinformation campaigns via videos on YouTube and Twitter, and intermittent blocking or slowing of access speeds to popular the social network LiveJournal.[7] Belarus authorities also went online, seeking to dissuade group members from participating. The Belarus Ministry of the Interior and the Minsk Police Department both launched Twitter accounts (@mvd__by, @GUVD__Minsk), which they used to discourage people from attending rallies and warning them of potential punishments should they appear at protests.[8]

This kind of multi-layered response by governments seeking to suppress or discredit online speech is increasingly becoming the norm in several OSCE member states, particularly in the former Soviet Union. While Turkmenistan and Uzbekistan practice extensive filtering, other countries such as Kazakhstan, Russia, Belarus, and Azerbaijan implement a range of responses that together serve to restrict online access to information, participation, and content creation, and monitor and surveil online communities.[9]

This mix of tactics of suppression and repression goes back at least 10 years. A combination of filtering and hacking of websites, physical threats and intimidation, propaganda and defamation, burdensome legal and regulatory environments, market manipulation, and the use of tertiary legal controls such as tax inspections worked to threaten an earlier generation of online content providers.

It is no secret that many governments in the FSU have gained their legitimacy through questionable means. Rigged elections, heavily biased and government-controlled media, dependent and corrupt judiciaries, opaque and vague laws and regulations, arbitrary implementation of law, and extralegal responses to political opponents including violence and killing are all too common. This has been true for some countries in the region since the fall of the Soviet Union, and has given governments a sense of impunity in regard to their behaviors.

Filtering and hacking of Internet content in the region now has a long history. Targeting of individual websites, online publications, or individual writers through a range of online and offline tactics is also not a new story. The concern is that as internet access grows across the FSU, governments will step up their restrictions, targeting not just relatively elite communities of writers and opposition politicians, but citizens writing and sharing multimedia content on a range of user-generated platforms.

While tactics may change, the overall strategy of mixing the tools of repression to achieve various ends remains in place. The ultimate goal of this kind of harassing activity seems to be to systematically suppress speech and media content that questions the legitimacy of those in power, and particularly those who question how power and wealth are gained and distributed. It is notable, as well, that some of these practices are not restricted to non-democratic regimes. Recent mass media

---

[6] Alexey Sidorenko, "Belarus: Police Crack Down on Minsk Protest," June 24, 2011, Global Voices Online, http://globalvoicesonline.org/2011/06/24/belarus-police-crack-down-on-minsk-protest/.

[7] Alexey Sidorenko, "Belarus: Independence Day Clapping Protest (Video). Global Voices Online, July 6, 2011, http://globalvoicesonline.org/2011/07/06/belarus-independence-day-clapping-protest/.

[8] Sidorenko, "Belarus: Police Crack Down on Minsk Protest." It has been reported that people trying to connect to Vkontakte have been redirected by Belarusian Internet service provider BelTelecom to websites containing malware. From early May to early June, at least seven websites were closed at the behest of the police, which was given new prerogatives under a law adopted on 1 March. The journalists who continue to be held in prison after covering protests are mostly freelancers or reporters working for news websites that the government does not register as news media (source: Reporters Without Borders, personal communication, July 14, 2011).

[9] OpenNet Initiative, "Access Denied: Commonwealth of Independent States profile," accessed July 14, 2011, http://opennet.net/research/regions/cis.

laws in Hungary also treat websites as mass media, for instance, and Italy's intermediary liability laws also function to suppress speech.[10]

The tactics employed to suppress speech are varied, and explained elsewhere in considerable detail. [11] A short list of common tactics:

Legal and regulatory controls

- Media licensing and registration regulations which treat websites as mass media, in Russia, Belarus, Kazakhstan, and most recently, Hungary and online forums in Russia, which targets social media networking sites
- Legal access to data tracking online behavior of users and data retention requirements based in security laws such as Russia's SORM-II regulations and equivalents in Kazakhstan, Uzbekistan, Ukraine, and Belarus
- Legal filtering and blocking of websites and webpages
- Intermediary liability requirements for content on social networking, search, and user-generated content websites
- Improper use of laws that restrict "bad" speech—hate, pornography, support for "terror", sometimes used to justify Internet filtering [12]
- Use of intellectual property regulations to restrict access to an entire website or type of website
- Lack of due process for protesting blocked or filtered content, lack of transparency about reasons for filtering, and lack of clarity regarding who is blocked/filtered, and at what level
- Imprecise language within law that leads to overly broad application of restrictions, for instance against "inappropriate" content (Uzbekistan) or threats to "public order" (Kazakhstan) and lead to self-censorship; lack of recourse or appeals processes
- Secret laws and decrees that govern security agencies, and provide permission to filter, block, or slow access to specific services and websites.

Pressure on service providers

- Monopolization or state control of Internet Service Providers and telecoms
- High tariffs for Internet access
- Pressuring ISPs for data access, mandating expensive filtering at the ISP level.

Extralegal responses

- Filtering, blocking, hacking, and pressure on intermediaries such as social networking sites
- DoS, data-gathering for surveillance through traffic monitoring, spyware, and other unacknowledged tactics for disrupting access to or altering content. [13]

Propaganda, misinformation, disinformation campaigns, harassment

- Competing for influence in online forums, disinformation and misinformation on web 2.0 platforms, sometimes through paid networks of writers/bloggers or PR agencies
- Defamation, libel, false accusations to damage reputation [14]

---

[10] "An Open Letter from the Hungarian Civil Liberties Union (HCLU) to the European Commissioner, Neelie Kroes, regarding the Proposed Amendments to the Media Law," One Million for Freedom of Press in Hungary, March 8, 2011, http://freepress.blog.hu/2011/03/08/.

[11] Access Controlled, The Shaping of Power, Rights, and Rule in Cyberspace, Edited by Ronald J. Deibert, John G. Palfrey, Rafal Rohozinski and Jonathan Zittrain, April 2010, MIT Press, Cambridge, MA.

[12] In June 2011, the Kyrgyz parliament adopted a resolution issuing a legally binding instruction to the prosecutor general's office, culture ministry and justice ministry to block access to the independent online news agency Ferghana (www.ferghananews.com) because of its coverage of last year's violence in the south of the country.

[13] On March 30, 2011, the social networking site LiveJournal experienced a sustained DDoS attack. The target of the attack, in the opinion of many experts, appears to have been user Alexei Navalny, who is also the founder of the anti-corruption web platform Rospil. The attack rendered LiveJournal inaccessible on that day, and a second attacked achieved the same effect on April 4, 2011. Ashley Cleek: "Russia: DDoS Attack on LiveJournal Has Russians Debating Internet Politics," Global Voices Online, April 6, 2011, http://globalvoicesonline.org/2011/04/06/russia-ddos-attack-on-livejournal-has-russians-debating-internetpolitics/.

[14] Authorities in Russia are harassing bloggers in the country, urging them to remove content and threatening them with judicial action. The Federal Security Service (FSB) asked the well-known blogger Leonid Kaganov, through his hosting company, to remove an anti-Semitic poem that he had mocked. Kaganov complied, but replaced the original poem with a parody. The FSB reiterated its request. Finally, for fear of further conflict with the security services, Kaganov decided to move his blog onto a foreign server. (source: Reporters Without Borders, personal communication, July 14, 2011). See also Alexey Sidorenko, Russia: Famous Sci-Fi Writer's Blog

Continued

- Harassment by security agencies to suppress speech.

Indirect methods

- Use of alternative governmental agencies to apply pressure, such as burdensome tax inspections, access to utilities, building code violations, and military conscription [15]
- Physical and psychological pressure, threats to self and family
- Violence, destruction of property, arson.

It is worth noting that the growth of mobile internet access has created another set of security, privacy, and information access and creation concerns. Mobile phones allow tracking, monitoring, and surveillance with relative ease. The fragmentary nature of privacy and anonymity controls with phones that allow tracking by location, by phone id number, by phone number, and SMS capture, make meaningful privacy a challenge in all states. Phone companies in the many countries have weak controls or ability to resist requests for data, either legally or extralegally

Responses—what OSCE member states and the U.S. government can do

The documentation of these abuse tactics is reasonably well established, as reports referenced earlier in this document show, thanks to activist and freedom of expression watchdog activities. The OSCE should continue to support and promote monitoring and documentation of member states activities in this sector, both in their own work and in the work of civil society watchdog groups. A deeper question is the willingness of governments to apply political will to create positive incentives for citizens to participate in public spheres, pursuing both the letter and the spirit of commitments to OSCE rights obligations and Article 19 of the Universal Declaration of Human Rights. Those commitments are not just about the economic or scientific benefits of increasing Internet penetration, a concept that many FSU governments support, but about the political and civic rights of citizens. Without politically legitimate and accountable governance, the political will to foster those rights is unlikely to appear. To be clear—not every government in the former Soviet Union applies restrictions on online speech of the same measure or kind—the picture is varied across the region, with some countries working to meet their OSCE and UN obligations.

Unfortunately, the tendency of several OSCE member states from the former Soviet Union is in the direction of increasing control. A recent Commonwealth of Independent States framework law on Internet regulation, for instance, "contradict[s] the principles of online free expression and Net Neutrality by encouraging member states to exercise excessive control over what is a privileged space for exchanging information." [16] This document, intended as a guide for national parliaments in creating Internet regulation, seems to breech internationally accepted standards promoted by the OSCE in Net Neutrality and ISP data retention and access.

Responses to the failure of OSCE member states to abide by online freedom of speech principles begin with ideas behind the original Helsinki accords. Governments should be accountable to their own laws and their commitments under international agreements and treaties, and use legal, transparent, accountable regulations to manage internet access and content restrictions. Some basic principles for removing suppression of speech and discouraging self-censorship include:

- If filtering is necessary, place filter systems at the level of the user for maximum control; any filtering that goes on should be done in a transparent and accountable manner, so that citizens know who is responsible for it, how decisions about what is or isn't filtered are made, there is a clear process for having such systems reversed, and that there are clear political consequences for officials who abuse the system, and regulatory consequences for companies that abuse it [17]

Removed for 'Anti-Semitism'," Global Voices Online, May 29, 2011, http://globalvoicesonline.org/2011/05/29/russia-famous-sci-fi-writers-blog-removed-foranti-semitism/.

[15] In May 2011, an Azerbaijani district court sentenced the blogger Bakhtiyar Hajiyev, a Harvard graduate and former opposition candidate, to two years in prison on a charge of evading military service. He believes the trial is politically motivated and linked to his online activities. http://supportbakhtiyar.com/.

[16] Framework Law No. 36-9 "On the Bases of Internet Regulation," "Internet Regulation Should Not Curtail Freedom of Expression," Reporters Without Borders, June 15, 2011, http://en.rsf.org/europe-et-ex-urss-internet-regulation-should-not-15-06-2011,40463.html.

[17] Some governments seek to justify filtering in response to hate speech, child pornography, and terrorism. Several studies suggest that filtering has a limited value in restricting this kind of speech, in particular child pornography. See: Cormac Callanan, Marco Gercke, Estelle De Marco, and Hein Dries-Ziekenheiner, Internet blocking: balancing cybercrime responses in democratic societies Aconite Internet Solutions, October 2009, online at: http://www.aconite.com/

- Presume that the response to "bad" speech is more speech, and that restrictions on "bad" speech are proportionate and focused on specific incidents rather than classes of speech
- Ensure that restrictions and punishments are proportionate to the concern (for instance, domain-based filtering that also blocks legitimate content rather than the specific target is disproportionate)
- Apply laws consistently, without political or economic favor
- Avoid prior restraint measures such as indefinite enforcement of filtering
- Create clear legal terms for speech that is banned; there needs to be clear legal processes to appeal bans or for the overturning of bans. Banning must have a clear basis in the consent of the governed and must avoid the pitfall of reinforcing tyranny of the majority, and should be extremely rare
- Rely on independent courts rather than administrative bodies for enforcement
- Preferably, there will be no intermediary liability; if needed, clear rules of engagement, and response opportunities to requirements
- Encourage or even require corporate transparency with users and customers about what sorts of government surveillance and censorship demands are being made of them. The Google Transparency Report, which lists the number of government requests for hand-over of user information or deletion of content, is an excellent model [18]
- Do not filter the ISP level for IP issues; intermediary filtering of IP-related issues has negative speech freedom consequences. [19]

Beyond that, however, there are positive reinforcements that OSCE member states can follow, supporting both the letter and the spirit of their commitments to speech freedoms. From the perspective of citizen interests in online environments, this includes a focus not just on access to information, but on the opportunity for online participation, creation, and engagement. Online, in networked media environments, speech rights precipitate assembly, movement, and all other rights. Without the medium of speech, other rights are difficult to assert.

There has been in the past year an appearance of newly assertive civic voices in several OSCE countries that have poor records on government legitimacy issues such as free and fair elections, corruption, and repressive security regimes. The use of information technology tools and platforms that combine data analysis, visualization tools, mapping, community participation in reporting and mapping, and subject-specific expertise point to the creation of projects that are specifically designed to highlight corruption, create transparency, or demand governmental accountability. Examples include Help Map, which allowed Russian citizens to volunteer information and resources to fight fires in the summer of 2010, Roskomvzyatka, a crowdsourced map on which citizens can document instances of bribery, and Rospil, which crowdsources independent analyses of Russian government procurements. These projects show the potential that citizens in the former Soviet Union have to find creative solutions to their own problems. Such projects demonstrate that drivers of change often come from inside repressive environments, and that with greater connectivity, opportunities to participate can create meaningful change.

Supporting the continued openness and unfettered nature of the internet provides projects such as these with a firm foundations for the emergence of creative opportunities for people to express their citizenship. The OSCE role is best articulated as asserting that its members follow both the letter and the spirit of OSCE obligations.

The U.S. government role is best articulated as supporting the continued openness and unfettered nature of the internet. As a first step, the U.S. should consider how its policies on Internet freedom will effect local communities that they purport to help. It should follow a "do no harm" approach that is sensitive to local contexts and concerns, and takes into consideration the personal security and goals of online activists working in repressive contexts. [20]

---

sites/default/files/Internet_blocking_and_Democracy.pdf "Child pornography: MEPs doubt effectiveness of blocking web access" European Parliament official website, November 15, 2010, at: http://www.europarl.europa.eu/en/pressroom/content/20101115IPR94729/html/Child-pornography-MEPsdoubt-effectiveness-of-blocking-web-access.

[18] http://www.google.com/transparencyreport/.

[19] "Intermediary Liability: Protecting Internet Platforms for Expression and Innovation," Center for Democracy and Technology, April 2010, http://www.cdt.org/files/pdfs/CDTIntermediary%20Liability_(2010).pdf. Rashmi Rangnath, "Civil Society Walks Away from OECD InternetPolicy Principles," Public Knowledge Blog, June 29, 2011, http://www.publicknowledge.org/blog/civilsociety-groups-refuse-endorse-oecd-inte; "CSISAC Issues Statement on OECD Communique on Principles for Internet Policy-making," June 29, 2011, http://csisac.org/CSISAC_PR_06292011.pdf.

[20] Ivan Sigal, "Going Local," Index on Censorship, Vol 40, No. 1, 2011, p. 96.

In addition to voicing support for access, advocates should consider how to provide multi-faceted, diverse tools and resources that help people both to get access to information in restrictive environments, and perhaps more importantly, help people to create, share, preserve, and build the tools and resources that they need to be engaged citizens in their countries. Recent U.S. State Department initiatives to support a wide range of tools and education on information access creative content in countries that use extensive filtering and blocking is an example of the right kind of approach. Narrowly focusing resources only on information access to external information, on the other hand, downplays the importance of locally generated content, information technology tools, the opportunities for communities in repressive environments to strengthen their own content creation.

While building tools to help people participate freely online, protect identity and privacy, and participate freely in the exchange of information and knowledge is useful, it is ultimately not a substitute for the application of political will on the part of all OSCE member states to foster both legal environments and civic cultures of online participation, to ensure that we protect and grow the Internet for citizens first, rather than security agencies or corporate interests. In this context, the U.S. has the opportunity to lead by example, whether in supporting open government data, as with the recent launch of the Open Government Partnership; [21] supporting Internet policy principles that represent the interests of citizens as well as corporations and governments, in forums such as the OECD; or ensuring that its cybersecurity policies do not impinge on the privacy and rights of its citizens, as with the ongoing debates over the extension of the Communications Assistance to Law Enforcement Act (CALEA) to facilitate surveillance. [22] [23]

Finally, governments interested in supporting these commitments should support information access, but also focus on creative capacity and removing barriers to civic participation. As a set of tools to respond to restrictive governments, removing both economic and political barriers to access is just the beginning. Governments interested in meeting the spirit of OSCE intent can offer many positive incentives to use and participation. These include:

- Internet infrastructure development
- Tariff pricing schemes that ease access costs in underdeveloped regions
- State programs to ensure internet access exists in schools, libraries, and other public contexts, and digital media literacy opportunities in those same facilities.
- Open government programs to systematically open government data to public scrutiny, allowing citizens to understand and track the workings of government.

BIOGRAPHY OF IVAN SIGAL

Ivan Sigal is the Executive Director of Global Voices (http://globalvoicesonline.org), a non-profit online global citizens' media initiative. Previously, as a Senior Fellow at the U.S. Institute of Peace, Sigal focused on how increased media and information access and participation using new technologies affect conflict-prone areas. He spent over ten years working in media development in the former Soviet Union and Asia, supporting journalism, media regulatory reform, and working on media co-productions. During that time he worked for Internews Network, as Regional Director for Asia, Central Asia, and Afghanistan. In that capacity he designed and implemented dozens of media assistance projects, including helping to create more than thirty Afghan-run radio stations and building an independent Afghan radio network; a project to provide humanitarian information to victims of the 2005 South Asian earthquake in Pakistan-administered Kashmir; a post-2004 tsunami humanitarian information radio program in Sri Lanka, legal and civil society reporting programs for Chinese journalists, and numerous current affairs TV programs for Central Asian audiences. He has a masters' degree from the Fletcher School of Law and Diplomacy, and an undergraduate degree from Williams College.

---

[21] http://www.transparency-initiative.org/news/ogp-launch-july2011

[22] "CSISAC Issues Statement on OECD Communique on Principles for Internet Policy-making." See also Milton Mueller, "Civil Society Defects from OECD Policy Principles," Internet Governance Project, June 28, 2011, http://blog.internetgovernance.org/blog/—archives/2011/6/28/4847563.html. Full "Communique on Principles for Internet Policy-Making" available at http://www.oecd.org/dataoecd/40/21/48289796.pdf.

[23] Greg Nojeim, "Privacy and Security Are Not a Zero Sum Game," Center for Democracy & Technology, February 11, 2011, http://www.cdt.org/blogs/greg-nojeim/privacy-and-security-are-not-zero-sum-game.

BIOGRAPHY OF DR. CHARLES LEE

Charles Lee is a Harvard educated medical doctor and citizen of the United States who suffered mental and physical torture, brainwashing, force-feedings and was forced to make products for export to the United States while he was illegally held in a labor camp in China from 2003 to 2006. He currently resides in New Jersey and is married, and has one daughter. He is now the spokesperson for the Global Service for Quitting the Chinese Communist Party and the spokesperson for the Global Mission to Rescue Persecuted Falun Gong Practitioners. He works actively to spread the truth about the Falun Gong and to promote the movement of quitting the Communist Party and its affiliated organizations.

Charles Lee was born in 1965 in Communist China. When Charles was only nine years old, "anti-revolutionary" posters showed up at his parents' work place. No "culprit" was found, and somehow Charles became the scapegoat and was labeled a "young anti-revolutionary criminal."

In the year of 1982, feeling depressed and frustrated by the manner in which his professors taught, Charles started to teach himself and promoted self-study research at the university in 1983. Charles then began independent research work on campus when he was only 18 and published his first research paper in 1986 when he was 21.

Charles left China in 1991 because he was extremely disappointed by the CCP's crackdown on democracy movement in 1989. He came to the United States to continue his study in neuroscience. In 1995, Charles went to Harvard Medical School and passed the United States medical board exams.

In 1997, Charles came to know the mind/body discipline of Falun Gong. He quickly became enamored by its guiding principles of "Truthfulness, Compassion, and Forbearance" and practiced these principles wholeheartedly.

Since 1999, the Chinese communists started a crackdown on Falun Gong. Tens of thousands of Falun Gong practitioners were arrested and thrown into jails with fabricated crimes. Millions of Falun Gong practitioners were stripped of their natural born right to freedom of religious practice and freedom of assembly. Many have been tortured to death.

Because there was no way for the Chinese people to know the truth, and because the persecution had been going on for such a long time, Charles decided to go back to China to reveal the truth of the persecution by tapping into the state cable TV system in the year of 2002. Charles was arrested in October 2002, though he managed to escape from the detention center and get back to the United States.

Since Charles did not finish what he intended to do to clarify the truth, he went back again in January 2003, though he was arrested upon his plane's arrival.

In order to justify their unlawful persecution, they used all possible means to force Charles to renounce Falun Gong. They designed an unrelenting persecution program to keep him under continuous physical and mental pressure.

The inhumanity and cruelty of the persecution conducted by the CCP not only manifested in physical and mental torture, but also in its total disregard for basic human values. During Charles's imprisonment, they used his mother's health condition to apply more mental pressure.

He understood fully that yielding to the prison's pressures and accepting their conditions would be a crime against his own conscious and a loss of his very soul. In addition, it would cause tremendous humiliation and suffering to both Charles and his mother, so Charles refused to cooperate with them. Charles' mother fully understood and supported him, but she was never able to visit him or see his release.

Charles is an American citizen and there were efforts being made all around the world by Falun Gong and other human rights organizations to protest his unlawful imprisonment and persecution. His finance' kept constant contact with the U.S. Embassy and sprung into action contacting policy makers and the press. Yet Charles was forced into slave labor and suffered vicious persecution in the prison camp. He was forced to make "Homer Simpson" slippers, Christmas lights, calendars and other consumer products exported to the United States. The working conditions were so harsh that he became sick frequently.

The forced brainwashing by the CCP lasted the entire three years. Their goal was to replace all Charles's thoughts with their propaganda by cutting off all outside information. He was forced to watch brainwashing TV programs and listen to readings that slandered Falun Gong. They also conducted frequent so-called "condemnation sessions," in which he was surrounded by 15 inmates and prison officers who would threaten, antagonize, and humiliate him.

The descriptions above are only a small fraction of what Charles experienced in the Chinese Communist forced labor camp. The calculated combination of mental

and physical abuse he suffered was not carried out arbitrarily. The goal was to transform Charles's spiritual belief. The reason the Communist Regime is so threatened by those with true spiritual and religious beliefs is because it directly challenges their forced religion of Communist Party worship onto the people.

The true nature of the Communist Regime in China has been thoroughly exposed in the Epoch Times groundbreaking editorial series *The Nine Commentaries*. As a result, more people are realizing that as long as the Chinese Communist Party is in power, it will be impossible to truly improve the human rights situation.

The quitting the CCP "TuiDang" movement started then and people who have quit the party and its affiliated organizations have reached about 98,500,000 recently.

Charles has been dedicating much of his time raising awareness of the persecution on Falun Gong, helping practitioners who are in need, and advocating the Tuidang movement since it's the only way for Chinese people to break away from the mind control by the CCP and get prepared for the future and de-communization.

This is an official publication of the
Commission on Security and Cooperation in Europe.

★ ★ ★

This publication is intended to document developments and trends in participating States of the Organization for Security and Cooperation in Europe (OSCE).

★ ★ ★

★ ★ ★

http://www.csce.gov @HelsinkiComm

The Commission's Web site provides access to the latest press releases and reports, as well as hearings and briefings. Using the Commission's electronic subscription service, readers are able to receive press releases, articles, and other materials by topic or countries of particular interest.

Please subscribe today.