Testimony of David J. Kramer
President of Freedom House

before the

The Commission on Security and Cooperation in Europe
(U.S. Helsinki Commission)

"The Promises We Keep Online:
Internet Freedom in the OSCE Region"

July 15, 2011

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 2011* 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 Mijatović, 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 freedom 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 café one must present identity documents. The administration of an Internet café 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 Bayramlı, Fuad Gahramanlı 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. Gahramanlı'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 Mijatović 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.
    - Security: Internet activists need support to fight against the complex and sustained cyber-security issues they face.
    - 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.