

**EVGENY MOROZOV**

**Yahoo Fellow/Georgetown University and Contributing Editor/Foreign Policy**

**TESTIMONY**

**Commission on Security and Cooperation in Europe**

**Washington, D.C.**

**October 22, 2009**

I want to express my appreciation to the Members of the Helsinki Commission for holding a hearing on such an important subject today and for giving me the opportunity to share with you some thoughts drawn from my research into how authoritarian states are dealing with the challenges and opportunities presented by the digital age in general and new media in particular.

While I share much of the recent enthusiasm about the positive role that new media could play in opening up and democratizing authoritarian societies, I am increasingly concerned with both how well authoritarian governments have managed to adapt to the Internet threat and how poorly some digital activists, journalists, and even policy-makers understand the risks of trying to promote democracy via the Internet. Let me outline several of my most pressing concerns.

**I. New media will power *all* political forces, not just the forces we like.** Many of the recent Western funding and media development efforts have been aimed at creating "new digital public spaces", on the assumption that these new digital spaces would enable the nascent actors of civil society in places like Egypt or China to flourish on blogs and social networks. While this does sound reasonable in theory, in practice we have to be prepared that groups that are often anti-democratic, both in their nature and rhetoric, would probably benefit most from the existence of such new spaces. In a sense, promoting these new digital spaces entails the same risks as promoting free elections: it's quite possible we may not like who wins them. For example, research into the blogospheres in Egypt, Palestine, Russia suggests

that Muslim Brotherhood, Hamas, and various groups of Russian nationalists and fascists have been one of the heaviest users of blogs and social networks (in part because they are often blocked from any access to traditional media, so for them these spaces are the only platforms). Blind support for promoting blogging and social networking may have a lot of very unpleasant unexpected consequences.

## **II. Authoritarian governments have developed extremely sophisticated strategies to control**

**cyberspace.** It is a mistake to believe that authoritarian governments wouldn't be able to manipulate these new public spaces with their own propaganda or use them to their own advantage. Many authoritarian governments are already paying bloggers and Internet commentators to spin the political online discussions that they do not like. Strategies to build what I have dubbed "the spinternet" vary from country to country. The Russians outsource it to new media start-ups who then create ideological social networking/blogging sites that promote a pro-Kremlin ideology. The Chinese have created a decentralized and 280,000-people strong contingent of what is known as "50 cent party" - 50 cent refers to how much they get paid for each comment they leave online - whereby its "blog" soldiers are tasked with identifying sensitive online discussions and trying to hijack the conversation in directions favorable to the government. The Nigerian government has been reported to be working on an "Anti-Blogging Project" that would fund hundreds of pro-government voices to counter the growing influence of the oppositional bloggers – and pay them in cyber-café vouchers. Even the Iranian clerics have been running Qom-based blogging workshops - particularly targeting women - to control much of the online discourse about religious issues (they obviously do not want any competing interpretation of Shia to take hold online).

**III. Authoritarian governments are increasingly eager to build short-term alliances with digital groups that share their goals.** One of the reasons why Russia has emerged as the most feared player in the field of cyberwarfare is because it always acts indirectly, usually by relying on numerous nimble underground gangs of cyber-criminals. Most of the time these gangs perfect the art of stealing credit card details of foreigners. However, when the geopolitical pressure so requires, they could be easily mobilized to assist the state (just think of the cyber-component to the recent conflicts Russia had with Estonia and Georgia, when the communication networks of both those states were crippled). Arguably, the fact that it's networks of cyber-criminals who plan and executive the attacks - perhaps, with barely concealed toleration and even tacit encouragement by the Kremlin –gives Moscow a different kind of power. Now, it can deny its direct involvement in the cyber-attacks (as it has done), while sending a clear message that anyone who wants to argue with it would have to be ready to deal with its cyber-gangs. Equally disturbing are recent movements by the governments to legitimize Internet censorship by involving fake institutions of civil society in the deliberation process. For example, on the suggestion of the speaker of the upper chamber of the Russian parliament, Kremlin may soon create a “Bloggers’ Chamber” – another one of those state-controlled fake representatives of the “civil society” – that would invite prominent Russian bloggers (but almost certainly bypassing those that disapprove of the Kremlin’s policies) to set their own standards of what can and cannot be discussed on Russian blogs. That’s just another example where the supposed ceding of state power would probably only reinforce the Kremlin’s control over the Russian Internet.

**IV. Cyber attacks have become an important form of exerting indirect psychological pressure on civil society.** Distributed denial-of-service (DDOS) attacks--whereby servers of a given Web site are overloaded with bogus requests to “serve” a page--don’t only make important content temporarily

inaccessible, they also put a huge drain on staff and physical resources of an NGO or a newspaper. While the media tend to focus almost exclusively on cyber attacks against military and government targets--the overblown coverage of "cyberwars" in Estonia and Georgia have brought such dramatic terms as "cyber-Katrina" and "electronic Pearl Harbor" into public use--civil society organizations are hit the hardest. If left unchecked, DDOS attacks, which are increasingly cheap to organize and can be rented on the black market, may erase all the social capital that NGOs and even bloggers have cultivated online. The oft-quoted story of CYXYMU, a popular blogger from Georgia, is a case in point. A refugee from the earlier war in Abkhazia, CYXYMU emerged as one of the most visible and consistent critics of how both the Russian and Georgian governments handled last year's war in South Ossetia. Blogging in Russian, he has cultivated a relatively large following in both countries, particularly among the users of LiveJournal, one of the most popular blogging platforms in post-Soviet cyberspace. However, in October 2008, somebody got angry at his writings, and his blog--also hosted by LiveJournal--fell victim to a massive wave of cyber attacks, so severe that millions of other LiveJournal blogs became inaccessible for more than an hour. We should recognize CYXYMU for what he is--a "digital refugee" and a victim of geopolitics playing out in cyberspace, where free speech is possible in theory, but increasingly unavailable in practice.

CYXYMU is not an isolated case. On the first anniversary of the monks' uprising in Burma, a similar fate befell the three major Web sites of the Burmese exiled media--Irrawady, Mizzima, and the Democratic Voice of Burma. Administrators of the Web sites speculated that the attacks were launched by the junta to limit expected demonstrations. Oppositional Web sites in Kazakhstan and Mauritania have recently experienced similar problems, quite possibly at the hands of their own governments or agents affiliated with them. Nonpolitical Web sites are becoming regular targets of cyber attacks as well: in February 2009, virtually all major gay and lesbian Web sites in Russia were unavailable for more than a week, as a

result of a massive wave of denial-of-service attacks. In other words, that many anti-government discussions have moved online doesn't mean that these discussions would become any louder.

**V. We do not fully understand how new media affects civic engagement.** We shouldn't assume that establishing unfettered access to information is going to push people to learn the truth about human rights abuses/other crimes of the regime (and thus, make them more likely to become dissidents). Most likely, lifting the censorship lid would result in people using this opportunity to fill in other gaps in their info vacuum - those may have to do with religion, culture, socializing, and so forth. Political activism/active citizenship would probably only come last in this "pyramid of cyber-needs". The creators of tools like Psiphon and Tor, which allow for anonymous access to banned resources, report that many users like these tools because it gives them access to downloading pornography, which is not as easy to do in tightly -controlled societies. In China, two-thirds of the respondents to one opinion poll agreed with the proposition that "It's possible to have real relationships purely online," compared with one-fifth of Americans who felt the same. Just because a handful of young activists are turning to Twitter and Facebook to push for political change, we shouldn't automatically assume that thousands of others would follow. In fact, there is a growing risk that they would be sucked in into an endless cycle of infotainment, and their commitment to political life would be significantly eroded.

**VI. The losses in online privacy may not be worth the gains in online mobilization.** The emergence of new "digital spaces" where dissenting conversations can occur inevitably leads to the emergence of new ways to track those conversations. The proliferation of social networking has inadvertently made it easier to gather intelligence about whole networks of activists at very low costs. Even a tiny security flaw in the settings of one's Facebook profile may compromise the security of many others. While many

established activists take the necessary precautions to remain undetected, it's the amateur, "spontaneous" activists who are at greatest risk. Selective intimidation of bloggers - coupled with a real (or perceived) ability to track online conversations - erodes the trust that aspiring activists place into "social media" and eventually makes them less likely to partake in protest movements. The old, "analogue" model of activism was arguably much safer: if one node of the network got identified/de-activated, there was little or no damage done to others, because they were much harder to trace in physical space. The new, "digital" model puts entire networks at risk, because getting access to an activist's inbox can put all of his interlocutors at risk. Moreover, by overlapping different "social graphs" - an Internet jargon for "one's connections on a social network" - it may be possible to reveal identities of people who have taken all precautions to remain anonymous. It's also important to remember that obtaining that password may not require any sophisticated knowledge of technology; as the prominent Egyptian blogger and activist Alaa Abd El Fattah once remarked to me "when torture is cheap, you are not as concerned with what they can do to you technologically".

**VII. New media development is an extremely complicated business that often has adverse unexpected consequences.** Many of the latest attempts to create new "digital public spheres" from abroad/with foreign funding might have adverse effects on their future health/sustainability. The very business of "new media development" - so eagerly embraced by Western governments and foundations - at this point looks very dubious (I am speaking as someone who has directed new media activities at a media development NGO funded by most big donors and as someone who now sits on a foundation board investing into new media). The injection of cash into foreign-based NGOs who are then expected to promote "social media" in a given authoritarian country usually means that they make smart, entrepreneurial new media whizzes of this country addicted to grant money; soon they become

unwilling to work for free or don't bother creating their own unprofitable projects. New media is usually a low-investment/high-reward business and the reason why we have so many interesting new media sites in the US or Western Europe is because it's cheap to start, experiment, fail and move on to the next project. When you look at a grant-driven new media environment in a country like Belarus, what usually happens is that projects last for longer than they need to - they are not driven by business realities but rather by the bureaucracy of grant-reporting - and they usually commit the brightest minds who may otherwise be working on something else. In other words, the business of "new media development" suffers from all the classical pitfalls of economic development – and many more pitfalls of its own.

**VIII. Current US government restrictions on the export of technology to sanctioned countries thwart the adoption of new technologies.** I would also like to point out that the current sanctions against many authoritarian regimes - such as Cuba, Iran, North Korea and several others - make it significantly difficult for their ordinary citizens (as well as well-established activists and NGOs) to take advantage of all the opportunities that the Internet and social media offers. American technology companies face a fairly complicated process of obtaining and renewing licenses and waivers to be able to export their technology to the sanctioned countries. These rules are not 100% clear and some tech companies decide not to take any risks and withdraw from these markets altogether. For example, some American hosting companies refuse to deal with customers from Zimbabwe or Belarus or Iran; this inevitable leads to implicit censorship, where activist groups - that are actually supported and recognized by the US government - have to justify their activities to Web administrators of these companies. What has not been widely discussed during the recent events in Tehran is that these protests succeeded, to a large extent, despite all the hurdles that the US government has imposed in terms of accessing these new media technologies.

Mr. Chairman, Mr. Co-Chairman, members of the Commission, thank you for giving me the opportunity to address you today.