

The Internet: A room of our own?

EVGENY MOROZOV

The debate about the impact of the Internet on democracy is barely a decade old, but it has already sowed great confusion in the minds of academics and practitioners alike. It doesn't help that both of these concepts represent complex, multilayered, and abstract ideas that do not lend themselves to easy or precise measurement. We have little choice but to reach for the best readily quantifiable proxy, which usually only obfuscates the relationship further.

The Internet part of the equation is relatively easy to grasp; the rate of Internet diffusion has been one reliable indicator. Other tangible proxies—the number of Internet or mobile phone users per capita or more complex indicators like the density of a national blogosphere—are also quite straightforward, if not conclusive. Measuring democracy, on the other hand, requires us to substitute something more tangible: human rights, freedom of expression, transparency and corruption, civic engagement, media concentration, and even more esoteric indicators such as the diversity of the public sphere (itself often requiring another host of proxies to be measured properly). Factor in the vast economic, technological, and political differences across countries in transition, dictatorships, and established democracies, and it's clear why the study of the Internet's impact on democracy won't earn anyone the Nobel Peace Prize in the foreseeable future.

For all these reasons, the grand debate of the last decade has by now split into numerous nano-discourses that have acquired a life of their own: the role of mobile phones in economic development, the role of blogs in increas-

ing media diversity, the role of social networking in political mobilization, and so forth. It's easy to overestimate the obscurity of such seemingly arcane discussions; after all, it's not the first time that academics or bloggers can't make up their minds about a subject with dubious relevance to the real world. And yet, many of the assumptions underpinning our thinking about the impact of the Internet on democracy shape policymaking inside the world's most powerful institutions preoccupied with promoting democracy, human rights, or an open society (my own host institution—the Open Society Institute—is on this list and is not innocent of relying on similar assumptions).

One could say that the Internet has acquired a cult following among such institutions. While the U.S. State Department wraps its own efforts to use the Internet to promote democracy around the globe in the dry rhetoric of "Public Diplomacy 2.0," other agencies closely associated with and funded by the U.S. government—Internews and the National Endowment for Democracy being the two most visible—are actively recalibrating their toolkits to fit the age of new media. European governments and foundations are also not far behind, with the Dutch and Danish governments at the forefront of supporting the use of new media and the Internet for digital activism.

One particular assumption made by many of us early in this game was that cyberspace would provide the breathing room that civil society (and especially civil society in authoritarian countries) needed to operate. Armed with cheap and easy-to-use tools for fundraising, accessible ways of self-publishing, and effective

platforms of mobilization (first MySpace, now Facebook and MeetUp), civil society organizations could transcend the resource gap and institutional inefficiencies that had plagued their work in the past; they would be leaner, faster, and stronger. It's only now that we discover that leaner doesn't always mean louder, particularly for civil society organizations with controversial (at least by local standards) agendas. Although the Internet may have made many of their peripheral activities easier, it has often made their core activities—such as advocacy and awareness-raising—more difficult and less effective.

This unexpected outcome is easier to explain than it seems. Cyberspace politics is a zero-sum game; although Internet technology has certainly decreased the power of the nation-state—much as gunpowder or the printing press did in earlier stages of history—it has also empowered those whom we wouldn't necessarily list as “friends of civil society” (once again, analogies with gunpowder and the printing press, and their heavy use by extremist and militaristic organizations, are worth reflecting on). So, if we are ultimately concerned with limiting the power of the state—and when it comes to countries like China and Russia, our concerns are well justified—the Internet's impact has been very positive. However, this is only one part of a much larger picture; the pernicious influence of the nation-state has often been replaced in cyberspace by a host of decentralized, uncontrollable, and ultimately more dangerous elements. They have not only survived into the cyber age; they seem to prosper in it.

For example, nationalists in Russia (as well as in many other countries) rely on the Internet for fundraising, propaganda, and mobilization and recruitment of new supporters. Most disturbingly, DPNI (which is the Russian abbreviation for the Movement Against Illegal Immigration), the most active of such organizations, is on the cutting edge of Web innovation, going so far as to create visually appealing “mash-ups”—combinations of different data streams—that “mash” census data about the location of various ethnic minorities living in Russian towns with actual online maps of the neighborhoods where they live (curiously, a

host of NGOs and activists rely on the same mash-up technology—usually in less effective ways—to showcase illegal logging, pollution, and even ethnic attacks). Russians are not alone here; nationalist groups in many other countries, from Turkey to India, are exploiting cyberspace to publish previously unavailable nationalistic materials and add to their ranks.

Similarly, pseudoscience has found a second home on the Internet. Banned from the classroom, it's making a comeback on Facebook and YouTube. For example, aggressive antivaccination communities have eagerly embraced the Web to spread their antiscientific statements on a scale that was probably never available to them in the pre-Internet age. A 2007 study by a group of academics from Canada analyzed all unique English-language YouTube videos (at that time, all 153 of them) that contained any messages about human immunization; the researchers found that a third of them were outright negative about its value and another fifth were ambiguous, with negative videos usually receiving much higher ratings by YouTube users. Of the negative videos, almost half contradicted existing reference standards on immunization (the antivaccination movement is also extremely active in the developing world; UNICEF reports that its recent awareness-raising campaign ran into powerful online opposition from vaccination-denialists). In addition to illustrating the appeal of cyberspace to advocates of pseudoscience, this case raises an interesting question about whether a technology company such as YouTube (and ultimately its parent company, Google) should verify scientific claims made in the videos uploaded to the site; if yes, how should they go about it? (Google faced a similar set of problems when it erroneously classified a video documenting prison abuse in Egypt as too violent, overlooking its social role.) The editorial and fact-checking layers of traditional media organizations would make it unlikely that such videos would ever be aired, for there is usually someone on staff to distinguish facts from opinions; how user-generated sites will cope with this challenge is not yet clear.

Much has been made of bloggers' ability to take on corporations and hold them accountable. Consumerist.com, a popular consumer-oriented blog has emerged as, perhaps, the most

notable of such sites, attracting complaints from dissatisfied customers all over the world and advising them on how to fight back. A typical blog post from The Consumerist—entitled “How to Launch an Executive Email Carpet Bomb”—offers tips for “rattling the corporate monkey tree to make sure your complaint gets shoved under the nose of someone with decision-making powers.” However, corporations themselves have not been slow to exploit cyberspace for their own purposes, with many of them relying on “search engine optimization” (SEO)—a set of online techniques to boost their Google ranking—to make themselves easier to find. Now, they have stepped up their efforts, hiring the services of dedicated SEO firms that can ensure that any online complaints about corporate misbehavior posted by the likes of The Consumerist will be almost impossible to find on Google. ComplaintRemover.com, the most visible of such companies, advertises “Do you need negative information removed? We are masters at knocking bad links off the front pages of search engines!” boasts its front page. In some sense, cyberspace has made life relatively easy for companies: they don’t need to beat up journalists anymore; they just need to beat up Google. The latter can be done quietly, privately, and at little expense—to their finances or their reputations. The buck doesn’t stop with consumer-oriented blogs: Western governments are also quite eager to beat Google’s search algorithms: Britain’s Office for Security and Counter-Terrorism is planning to coach moderate Islamic groups in SEO, so that they can “flood the Internet” with positive interpretations of Islam. There are many other reasons why the Internet has failed to amplify the voices of civil society. The most obvious one is that governments have mastered the tricks of Internet censorship; this has been the most accessible and often the most reliable way to neutralize the dissemination of critical information on the Internet. To the great disappointment of free-speech advocates, global backlash against Internet censorship has been extremely limited, with several American companies feeling bold enough to supply governments such as China’s with technology that is being actively used for censorship. It’s too early to tell whether nascent international efforts to draw more attention to this issue—such as the Global Network Initiative, a consortium of corporations, human rights groups, and individual

activists aiming to thwart the censorship attempts of governments—will be successful, but the early signs are not encouraging.

Paradoxically, Western governments, which like to be seen as the biggest advocates of free speech in the world, deserve a fair share of blame here. Governments in the United Kingdom, Canada, Australia, and in much of Scandinavia (to mention just a few) are currently debating or enacting draconian Internet laws to target Internet pirates and child predators. The very act of lumping of these two groups together illustrates the governments’ profound misunderstanding of the Internet. A glimpse at any recent report—like the one that found that 95 percent of music downloads are illegal—would make any discussion of criminalization of Internet piracy impractical, if not outright silly.

A *much bigger* problem about these laws is that they add legitimacy to Internet censorship campaigns in China, Thailand, Vietnam, Turkey, and Russia, with the only difference being that in the latter case these laws are used primarily to crack down on political speech under the banner of a war on “online vulgarity.” But note that some of the pornographic sites blocked in the much-discussed Chinese crackdown at the beginning of this year are now back online, this time with even more pornographic content, while some of the political sites that were shut down during the same crackdown are still silent.

Some governments are combining aggressive Internet laws with truly innovative measures aimed at identifying and barring undesired content early on in the publishing cycle. The Thai government, for example, uses the country’s severe *lèse majesté* laws, prohibiting any offensive material aimed at the reigning sovereign, to go after administrators of critical Web sites. The most recent case is that of Cheeranuch Premchaiphorn, the Web administrator of Prachatai, the most influential Thai political Web site, who was recently detained because a comment critical of the king was discovered on the site. The Thai authorities also “crowdsource” the process of gathering URLs of sites to be blocked by encouraging their loyalists to submit such sites for review (a site named ProtectTheKing.net is a primary collection point of the offensive URLs).

Predictably, it's a one-way street: there is no similar invitation to submit sites to unblock.

However, censorship is not the only way to silence critical opinions and unwanted information online. Cyber attacks are increasingly becoming a weapon of choice, not only for governments but for anyone else with a grudge against particular ethnic, political, or sexual minorities. 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. 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. The only way to reduce the damage was temporarily to delete CYXYMU's account from LiveJournal, which its administrators did. Cyber attacks followed the blogger even after he set up a new blog on WordPress.com, another popular blogging platform (his account was quickly deleted from there as well). DDOS attacks against his new and old URLs continued unabated for more than six months. 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 Web sites were unavailable for more than a week, as a result of a massive wave of denial-of-service attacks. This trend is not limited to countries like Russia or Burma; many of the Web sites raising money to oppose Proposition 8 in California last November were attacked as well, most likely to make them unavailable for those who wanted to donate money to gay-friendly causes. That is one of the cases where neither the “leaner” nor the “louder” benefits that the Internet was supposed to bestow on civil society are obvious.

To understand how cyberspace may fail to empower civil society, there is no better case to study than that of Russia. Both the title and subtitle of “The Web that Failed: How opposition politics and independent initiatives are failing on the Internet in Russia,” a recent study of the Russian Internet published by the Reuters Institute at the University of Oxford, are right on target (disclosure: it was funded by the Open Society Institute, where I am a fellow). One of its conclusions is worth quoting here:

In the Russian context, new communications developments are not yet breaking down well-established patterns of power. The state remains the main mobilising agent in Russia. It [the Internet] does operate as a platform which the state uses increasingly successfully to consolidate its power and spread messages of stability and utility among the growing number of Russians regularly accessing websites and blogs.

This points to a broader trend where Kremlin-affiliated public relations technologists increasingly turn to cyberspace to generate fresh ideas on how to keep the current regime in power. Virtually all the political technologists of yesteryear—those who were instrumental in getting Boris Yeltsin reelected in 1996 and Vladimir Putin elected in 2000—are now actively experimenting with cyberspace. Gleb Pavlovsky, perhaps the most famous of that cohort, has paved the way; his think tank—the Fund for Effective Politics (FEP)—has arguably been the most effective player in shaping Russian ideology during the Putin era. Sensing a tremendous opportunity on the Internet, FEP has ventured into what can only be called “social networking with a Kremlin twist.” By launching *liberty.ru*—half social network and half group blog (think Huffington Post meets the DailyKos meets Facebook), Pavlovsky managed to tap into the creativity of Russian Internet users for his own ideological projects—while also giving his online community the impression that they have influence over the Kremlin’s agenda.

When asked recently about his motives for launching a Web2.0-friendly project like *liberty.ru* (not to mention giving it such an un-Kremlin-like name), Pavlovsky answered with atypical frankness.

Based on the FEP polls in 2006-2008, we identified three major clusters in Russian society. The biggest one is that of Kremlin loyalists; the smallest one is the politicized opposition; the cluster in the middle—14-20% of the population—is the creative class. They...are part of a new economic system. They are the trendsetters: journalists, advertisers, PR experts, IT specialists, Internet users....These people are able to shape and promote new ideologies...[*Liberty.ru*] will help political parties tap into their collective wisdom, see what these people are really concerned about; [the parties] would even be able to borrow some major policy points from these online discussions.

Pavlovsky’s activities, which, in essence, allow the Kremlin to tap into the collective unconscious and use it both to identify new ideas and promote old ones, are in line with what political scientists call “authoritarian deliberation”—the practice of authoritarian regimes that

provide space for seemingly meaningful deliberation without any intention of engaging in regime-level democratization. Of course, pursuing such a policy requires giving up a modicum of political power, when it comes to selecting participants and prioritizing projects, for example, but it ultimately pays off as an “investment” in the future.

The term “authoritarian deliberation” gained currency when it was used to describe the Chinese public sphere, which does provide the illusion of new models of governance without having any significant impact on the regime itself. “The Deliberative Turn in Chinese Political Development” by He Baogang and Mark Warren, the seminal paper on “authoritarian deliberation” in the Chinese context, explains why:

What they [the Communist Party of China—CCP] gain is the ability to legitimate policies by reference to a relatively inclusive deliberation process rather than to an official ideology or the variable benefits of economic development. These effects in turn can increase the political capacities of the CCP while furthering the careers of party officials. Under this scenario, then, the functional effectiveness of authoritarian deliberation stalls regime-level democratization. The CCP continues to encourage local officials to develop participatory and deliberative institutions to curb rampant corruption, reduce coercion, and promote reason-based persuasion....But ultimate control over agendas as well as outcomes remains with the Party and beyond the reach of democratic processes.

Baogang and Warren point out that in the Chinese case “authoritarian deliberation” predates the Internet: consultative meetings, public hearings, deliberative polls, citizen rights to sue the state, and even some kinds of autonomous civil society organizations started appearing two decades ago. However, what the Internet provides is many more opportunities to make the provision of deliberative elements more effective (and also very cheap). Despite recurring censorship campaigns, civil society is, indeed, provided with more and more space on the Internet, especially after Wikipedia introduced many people to various Wikipedia-like governance processes. And blogs provide a mechanism for self-expression and even harsh criticism of authorities.

What makes the Russian case so peculiar in comparison to the Chinese is that the blogosphere—and cyberspace at large—have not only given the public an opportunity to blow off steam, it has also allowed spin doctors like Pavlovsky to harvest and eventually promote new ideologies that could fill the vacuum in an otherwise spiritually bankrupt regime. The recent economic crisis has only highlighted the fact that with all the attention that Putin and Medvedev—and less visible Kremlin insiders like Vladislav Surkov—have paid to ideology, they have come up with nothing.

And yet we cannot say that the Internet offers no ways of transforming regimes like Russia or China. It's just that change is likely to come from unexpected quarters—from the need for legitimacy and modest respect in the eyes of the international community, for example, along with membership in elite clubs like G-8 or G-20. These are, perhaps, the only sticks that Western democracies can use against the authoritarian rulers in these countries. Given the brutal methods that their rulers employ to stay in power, their legitimacy has traditionally required manipulating international public opinion by preventing the locals from speaking out loud or simply limiting access to sensitive government data on human rights, pollution, or even disease outbreaks. Thanks to the Internet—and many of the phenomena it has begotten (such as crowdsourcing or citizen journalism)—this is one area where we can expect real change, particularly through the use of hybrid models, where nongovernmental organizations partner with ordinary citizens to produce authoritative reports based on crowdsourced methods of data gathering.

To a large extent, this is already happening, as a few dozen NGOs begin tapping into all sorts of previously unavailable data—reports on levels of urban crime and pollution, for example—which are being contributed by regular users, many of them previously unaffiliated with these NGOs. In fact, some of the most exciting projects currently strive to incorporate user-submitted data into traditional old-school data-gathering processes. WikiCrime, a project started in Brazil to allow citizens to map instances of violent crime that often go underreported and thus push governments to do something about it, is a

very good example of how techniques like crowdsourcing could be helpful. The same software is now being rolled out in Zimbabwe to allow reporting of cholera outbreaks. The true media darling of user-contributed Web sites is an African initiative called Ushahidi, which has been used (with various degrees of success) to allow user-generated reports (primarily via text-messaging) in a number of recent conflicts—most successfully in the postelectoral turmoil in Kenya, but also in the Democratic Republic of Congo, Gaza (where it was deployed by Al Jazeera), and Madagascar. The technology behind Ushahidi is simple: anyone can send a text message reporting a particular incident and then see this report visualized on an online map. This not only provides almost real-time data about dangerous conflict zones, it also helps to create a crowdsourced bank of reports that could then be used for human rights purposes.

However, this revolution in data availability has brought its own problems, chiefly in the realm of data verification. The fundamental and still unanswered question is, How much trust can we place in data that have been sent by unknown third-party sources? If someone wanted to discredit authorities in Kenya or DRC, the easiest way would be to bombard the service with thousands of bogus reports, hoping that they would be picked up by the mainstream media. There is no easy way to validate the authenticity of such reports; nor is there a way to meet the strict criteria for data validity that are often imposed by traditional human rights organizations. Are some data on human rights abuses, some of which may have been fabricated, better than no data at all? This controversial question divides the data community, but I am optimistic that we will be able to improve the algorithms and come up with “electronic lie detector” tests allowing us to make better distinctions between valid and fabricated data. Ultimately the supply side of the data equation will be solved; the demand side, however, will still remain problematic. What should we do with documented evidence of human rights abuses in Zimbabwe or Belarus or anywhere else? Unfortunately, the Internet offers no answers here.

Evgeny Morozov is a fellow at the Open Society Institute. He is at work on a book that examines the Internet's impact on global politics.