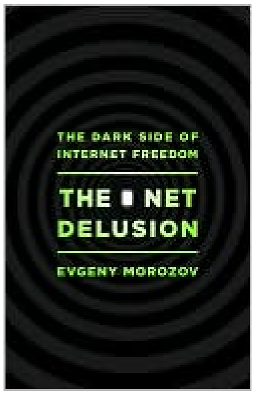
CARNEGIE COUNCIL
The Voice for Ethics
in International Affairs

The Net Delusion: The Dark Side of Internet Freedom

Evgeny Morozov , Joanne J. Myers

Tuesday, January 25, 2011



The Net Delusion: The Dark Side of Internet Freedom

Introduction

JOANNE MYERS: I'm Joanne Myers, director of Public Affairs Programs, and on behalf of the Carnegie Council, I'd like to thank you all for joining us.

If you have been following the news out of Tunisia and are interested in the idea of democracy promotion via the Internet, you will find today's discussion to be extremely interesting. The question our speaker will be addressing is about whether the increased use of the Internet and technological innovations such as Twitter, YouTube, and Facebook have, in reality, brought increased democracy to those under authoritarian rule—or have these new cyber tools actually made things worse?

Evgeny Morozov is often described as a gifted young cyber policy scholar who made his way to America from Belarus. He is recognized as the expert on the interaction of digital technology and democracy. In fact, his writings on this topic have reshaped many foreign policy debates and initiated new thinking on the power of the Internet to promote democracy around the world.

In writing this book, Mr. Morozov's aim is to bring a dose of *realpolitik* to discussions about how much of a difference the Net and digital technologies actually make in advancing democracy and freedom. His findings may surprise you. They did me.

He writes that although the Internet was supposed to help free oppressed people, it has often become a tool for control rather than liberation. For example, during the Iranian presidential elections in June 2009, when our government endorsed the theory that the Internet was playing a vital role in democracy promotion and the State Department requested that Twitter delay some of its planned maintenance at the height of the protest, it isn't all that difficult to see how this would encourage the Iranian authorities to crack down on social networks of all kinds.

In this case, technology was cleverly used to the advantage of the regime by helping to identify dissidents who were later arrested for their protests. This, of course, was the opposite of what American policymakers wanted or expected.

In *The Net Delusion*, Mr. Morozov points out how mistaken it is for policymakers to draw parallels between the Internet and earlier propaganda services, such as Voice of America or Radio Free Europe, and the roles that they played in undermining the Soviet Union. He argues that this has had erroneous conclusions of what the Internet can do today in bringing down authoritarian governments. Making it clear that he believes that the Internet can be used to promote democracy, if done the right way, our speaker proposes three things that need to be accomplished:

- First, that we discard a belief in cyber utopianism, or what he defines as our refusal to acknowledge the downside of online communications.

- Secondly, we have to dispense with Internet centrists who propose a philosophy of action that informs how decisions are made and how long-term strategies are crafted, including those that deal with democracy promotion.

- Finally, once we abandon these Net delusions, we can implement a policy of cyber realism to achieve our goals.

What does this suggest, and what questions should future cyber realists be asking? For the answers, please join me in giving a warm welcome to our guest, Evgeny Morozov.

Thank you for joining us.

Remarks

EVGENY MOROZOV: Thank you so much for this excellent introduction and very good summary of the main ideas in my book.

Before I get to the substance of the book, I would like to say a few words about why I actually chose to write it.

I come from Belarus, as you have already heard. This is not a country famous for its respect for democracy or human rights. As Condoleezza Rice once described it, it is the last outpost of tyranny in Europe. I always felt a strong interest in thinking about ways in which a country like Belarus can actually be opened up with the help of the West and outsiders**.** Clearly something was missing in how things were working internally.

Back in, I would say, 2004, there was a lot of enthusiasm about the power of the Internet in the United States. You may remember that it was then that Howard Dean used the Internet very successfully to campaign. There was a lot of enthusiasm about the power of blogs and how they were helping the underdogs to establish themselves in the public discourse. I became fascinated with this idea of using new media, blogs, and social networks to try to push against some of the excesses of authoritarian rule back in Belarus.

I joined an NGO, Transitions Online, which was based in Prague and was funded mostly by various Western foundations, government agencies, some European governments, and so forth. I spent about three years traveling throughout the former Soviet Union, going to places like the Caucasus, Central Asia, Belarus, and Moldova, and meeting with their bloggers, activists, and journalists. I trained them on how to do blogs in the new media, and showed them how they could actually use new media to push for change in their countries.

After several years of this job, I realized that there were several consequences that probably few of us who began this job actually predicted. One of them was that the authoritarian governments themselves were becoming extremely sophisticated in their approach to the Web.

They were no longer just censoring websites or banning access to particular URLs. They were actually getting much more involved with the online world. They were paying their own bloggers to go and spread pro-government messages. They were turning to technology provided by, often, Western companies to go and track dissidents online or to analyze huge amounts of data that was posted, in order to understand political and social trends, and what was actually happening in the country.

They were also engaging in all sorts of intimidation using the Internet, not just this very blunt Internet filtering and Internet censorship, but also turning to activities like cyber attacks. They would go and attack the website of an independent publisher, a newspaper, an NGO, or even a blog.

This would be resolved shortly afterwards, but it would also exert a huge amount of psychological pressure on the publisher. If you are a target of a cyber attack over the course of a year, chances are you may soon just give up, because the pressure is just so intense. It was a very interesting manifestation of psychological warfare.

The reason why authoritarian governments were so active online was, in part, because they saw that the Internet had become the new political battleground with their opponents in the West, especially America and Europe, who were trying to use new media for regime change.

They saw platforms like Twitter and Facebook as a way for the West to train activists and power dissidents. They became extremely suspicious of everything that America was doing in this space, but they also became very suspicious of the role that American companies were playing in this space.

Much of the, if you wish, civic infrastructure for this digital activism was put together by companies like Facebook, Twitter and Google, which have a commercial stake in this and which were representing America, in some sense.

The clearest manifestation of how authoritarian governments actually think about the Internet and how they would be exploiting it for their own purposes came during the protests in Iran in 2009. There was a lot of speculation in the West that there was a Twitter revolution happening in the country, that Twitter and blogs were used to basically overthrow the government. That intervention was already mentioned in the introduction.

This famous outreach and contact between the State Department and someone in Twitter basically helped to create the myth that, since the protests were facilitated by Twitter and since Twitter got some communication note from the U.S. government, it must be the U.S. government who is using Twitter for encouraging the protests in Iran.

I tracked the reaction to this event in the international media, in places like Russia and China. That event was seen as basically the American government trying to pull strings on the Internet in order to force democratic change in Iran.

What happened afterwards in Iran got lost in the media coverage, with all the media still focused on how the Green Movement was using the Internet, but not focused enough on how the government itself was using the Internet.

What happened was that the thousands of photos that protesters in Iran uploaded to sites like Flickr and videos that were uploaded to sites like YouTube were actually aggregated. They were all posted on the websites of the Iranian state-owned news agencies, with the faces of some of the protesters that were still unidentified circled in red, asking people—ordinary Iranians, who happened to be visiting those websites—to report anyone whom they recognize.

So in some sense, the government actually profited from so much material being posted to the Internet. Then they turned to the Internet to help them identify the real opponents.

They also went and analyzed a lot of information posted to Facebook and Twitter. They looked at the networks that existed on Facebook and Twitter, to know how activists were connected to each other, but also to figure out how some of those activists were connected to their supporters in the West.

There was clearly an effort on behalf of the government to turn to new media for intelligence gathering, but also for evidence of any improper connections that might exist between Iranian activists in Iran and their supporters abroad who were using Twitter to encourage them. Some of this evidence was also later presented in court.

The biggest consequence of what happened one and a half years ago in Iran was that most governments did wake up to the possibility that the State Department would be using new media to promote democracy. Of course, all of them immediately began pushing for replacing Twitter, Facebook, and Google with their own domestic alternatives.

If you look at what now is happening in Russia, China, and Iran, we see little domestic companies being championed by the government to replace the likes of Google, Facebook and Twitter, in part because they are much easier for the government to influence.

It's much easier for the Iranian or the Russian government to basically go and force the domestic companies to go offline on the day of the protests or force them to delete content that is being posted to the website without having to actually censor open access to the website.

This poses a few very interesting questions about the way in which America and the American government should actually be engaging with this space. There is nothing wrong with using new media and the Internet for pushing democratic values and freedom of expression, but there is always the factor that since it's done by the U.S. government and the West, and American companies are at the frontlines promoting all of this, they will actually suffer a bit more.

Their users might suffer, in part because if all of your communications take place on Facebook, in Iran or in China, chances are not all of them will be censored and not all of them will be monitored, because this is an American company. It's very hard for the Iranian, Chinese, or the Russian government to ask for this data or force Facebook to delete something off its website.

In most cases it will not happen, in part because it will lead to a lot of buzz in the international media. It's very easy to do that when you replace Google, Facebook, and Twitter with domestic alternatives. This is happening, and is one of the problems of politicizing this space.

The space was politicized even further during the famous speech that Hillary Clinton delivered a year ago, on January 21, 2010. It was a speech about Internet freedom, where she basically proclaimed that Internet freedom will be one of the new cornerstones of American foreign policy.

The subtitle of my book is actually not "The Dark Side of the Internet;" it's "The Dark Side of Internet Freedom," in part because there is something about this concept that basically sets up a trap for America. Clinton's speech was all about Internet freedom.

This trap was revealed just a few months ago with Wikileaks. On the one hand, you have parts of the U.S. government which actually want to limit Internet freedom. They want to establish control over cyberspace. They want to eliminate anonymity. The intelligence agencies and the law enforcement agencies actually want an agenda of Internet control.

For them, it's all about building secret backdoors into American software so that the NSA [National Security Agency] and FBI can monitor what's being said there to prevent terrorists and prevent anyone else, including, probably, Wikileaks, from benefiting from the power of the Internet.

On the other hand, you have people in the State Department actively campaigning on the issue of Internet freedom in the foreign context.

This makes the American government itself look extremely hypocritical. Foreigners look at this and they realize that—why do you want to take away the opportunity to monitor the citizens from the Iranians or the Chinese, while you want to keep the same opportunity for yourself?

My problem with Internet freedom as a concept is not so much the intents behind it. It's not that they want to promote democracy and freedom in Iran, China, and Russia. I'm all for that.

The way in which they are trying to do that is what bothers me, because it sets up just too many traps for American policymakers themselves, and eventually it subtracts from the effectiveness of what it is they are trying to accomplish. This is something that has not really been recognized, up until Wikileaks, and still we have not really seen much adjustment in terms of how American policymakers want to phrase and frame the subject matter.

Another thing that we need to keep in mind is that if you look at Clinton's speech delivered in January 2010, it is just amazing how much of that speech is referencing the Cold War.

It talks about "the information curtain" that is now descending upon much of the world. It talks about bloggers being the new dissidents. It talks about new media being the new *samizdat*. It talks about the new virtual walls which are replacing the Berlin Wall. All of the conceptual frameworks for thinking about Internet freedom still derive from the experiences of the Cold War.

Some of it is useful. Voice of America and Radio Free Europe certainly played some role in smuggling photocopiers and fax machines into the Soviet Union and into the Soviet satellite territories, which probably did play some of a role in what happened afterwards.

But if you go and analyze what American pundits say about this, many people do assume that the moment all of the Chinese, Iranians, and Russians get online, they will immediately rush to download reports from Human Rights Watch or coordinate protests and then pour into the streets and more or less topple the government.

It's a huge misconception. As someone who comes from Belarus and who knows what people use the Internet for, much of that actually centers on getting away from politics and political life altogether. A lot of that is seeking some kind of solace in the entertainment offered on YouTube and elsewhere, in part because the daily existence in most authoritarian states is just so stale and dreary that most people choose to forget themselves and use new media.

That aspect is completely misunderstood, in part because there is this very optimistic narrative in America that it was the broadcast of Radio Free Europe and it was the photocopiers that brought down the Soviet Union. Of course, it played a role, but it was not the broadcast.

If you look at the case of East Germany, which is studied in detail in the book, something like 80 percent of the East German territory could watch Western television because the Germans couldn't block it and at some point they just gave up.

If you look at them and compare the rates of political activity and dissent with those Germans who did not have access to German television, it's the Germans who didn't have access to Western television who were most political, participated in protests, and applied for the most exit visas from the country.

The most popular programs watched by East Germans who had access to Western television were all American soap operas, not broadcasts about what was happening in the NATO/Warsaw Pact and Moscow.

There is this tendency to forget that making information available, even if this information is about human rights abuses, will not necessarily turn people to it if they have more pressing needs, which, in most of these countries, is the need to communicate with their peers.

We have to look at the role of social networking or entertainment online. None of the concepts that so far have been offered by American diplomats when they think about Internet freedom actually take account of this sort of seamier entertainment side of Internet freedom.

But there are many other problems. We cannot assume that all blogging is *samizdat*, in part because there are plenty of bloggers in countries like Iran, China, or Russia who are actually more conservative than their leaders. They are more antidemocratic than their leaders. There are plenty of bloggers in Russia who basically support nationalism and extremism, and the Kremlin actually fears them because these guys just look much crazier than most of the people running the country. There must also be a little recognition of that. The fact that we have all of those antidemocratic forces online does not necessarily mean that the country is heading towards democracy.

There was no pro-government *samizdat* in the Soviet Union like there is pro-government blogging in Russia, China, or Iran. We have to keep that in mind.

If you look at photocopiers and fax machines, none of them were capable of launching cyber attacks on the websites of the Pentagon. It's the case with our modern computers, which creates a completely different policy environment, where you cannot just assume that by getting everyone in those countries online, you are going to have certain outcomes. You don't even know what will follow once all of them are online.

The biggest fallacy that was made by many policymakers in the West was this assumption that somehow dictators wouldn't be able to grow economically if they censored the Internet. There was this very deep-rooted assumption in Western media, but also in public discourse, that you either censor the Internet and then your economy suffers or you let the Internet in and then political liberalization occurs. That's what is known as the dictator's dilemma.

The notion of the dictator's dilemma has been around since before the Internet, when in 1985 George Shultz wrote an article about it for *Foreign Affairs*. It still dominates how people in the West think about the political effects of the Internet.

The problem here is that it severely understates and underestimates the ability of modern censorship to be customized to the needs of authoritarian states. You cannot grow economically if you have to ban the same websites for everybody. If you can manage to separate investment bankers from human rights activists, then you can grow economically. You do this by letting investment bankers access anything they want online while keeping human rights activists limited to a few government-approved websites.

The way to do that is to rely on the kind of social media and social information that is in plenty on the Internet. If you have 25 investment bankers as your online friends on a site like Facebook, and if everything that you have been reading online for the past two years has been articles from *The Wall Street Journal* and *Financial Times*, chances are there is no point to the Chinese government to censor you.

If, on the other hand, you have 25 human rights activists as your friends on Facebook, and if all you have been reading for the last two years are critical reports accusing China of human-rights violations, chances are you shouldn't be online to begin with, from the perspective of the government.

The future battle over this will consist of governments trying to customize censorship and tap into the vast resources of data that users disclose voluntarily.

It's not that the government needs to hack into anyone's Facebook or email account to learn who your friends are. You post this information voluntarily. And there are plenty of marketing firms in the West that will be happy to provide authoritarian governments with the technology to harvest that data. Why?

First of all, they don't care whether it's an authoritarian state or Wall Street which buys this news-processing and data-processing technology from them. Secondly, customization is basically where modern business is heading towards these days.

Look at Google. The more you use it, the better your search results become. Customization is built into its very DNA. The more search results you place and the more you click, the more Google knows what kinds of searches and ads to show you.

If you really want to push hard and think about applying this idea to censorship, it's very simple. Instead of showing you the most relevant app, it will just prevent it from visiting the most relevant Web page. The last stage is the only thing that differs. What happened before is it was looking at all of this data that you yourself disclosed to predict what it is that you need to be looking at, or not looking at, next.

What happened in China two years ago—you may have heard the story of this Green Dam software that the Chinese government wanted to have installed in all computers—this is where some of this is going. It was a system that not just had a vocabulary of words that it didn't want users to use or look at; it actually analyzed the kind of content users were looking at. If you had too much pink in the photos you were looking at, the system judged that you were accessing pornography. So it will block access to any websites that have too much pink background on them.

This suggests that we are beginning to see the emergence of these new systems which tap into things like artificial intelligence, which tap into social data that users themselves disclose, before they make the decision whether to censor or not.

In this sense, authoritarian governments have found a way in which to solve the dictator's dilemma. Instead of suffering the consequences of an economic downside by censoring the Web, they will just be able to separate those who contribute to economic growth the most from those that don't.

The big question that many of us in the West have to answer is, what can we do to prevent them from gaining this technology? Much of it is supplied by Western corporations, both for censorship and for analyzing data. Much of this comes from research in Western universities.

Just think about the technology of face recognition. Within the next six to 12 months, every modern social networking website will have the capacity to recognize people in the photos that you upload and match them to some of the other users on the network. On some websites, this is already happening. Then think about how easy it would be for the Iranian government—building on the example I gave you earlier, instead of uploading 50 photos and circling people's names and faces in red, and asking others to identify them if they recognize anyone, they will just compare the photos from protests with photos that activists themselves uploaded from parties, social gatherings, and identify all of them.

The technology for that is being researched and created in Western companies and universities. You see the Chinese government funding some of this technology at UCLA. American universities are very happy to receive money to do research on something as innocent as face recognition, without realizing that this technology will be very easily turned towards dissidents.

The other thing that we have to keep in mind is the proliferation of mobile phones, which again creates a lot of vulnerabilities for activists. What happened in Belarus last month gives you a very good example.

There were presidential elections last December 19, and there were protests following the elections on the main public square in Minsk, the capital. A lot of people showed up with their mobile phones. Six hundred people got arrested during the protests. Now there are reports that the government is actually asking the companies that run mobile networks in Belarus for details about anyone who showed up in that particular square at that particular moment with a mobile phone. This information can easily be traced by mobile operators, because all of those phones have to connect to towers. So it's actually possible for the government to go and learn about people who chose to oppose it by showing up in the square with their mobiles.

The easy solution here is, don't take your mobiles with you when you go to protest, leave them at home, which is probably a good idea, but then that cancels out some of the early promises of social media and technology. People thought that by having a mobile phone at the protests, you would actually be able to coordinate with others, and your protest would thus become much stronger.

That idea is also something that we need to explore. Of course, who supplies technology for those companies to be able to do that? It's Western companies—Ericsson, Nokia, and others.

There is a way in which civil society in the West can try to pressure some of those companies not to provide the technology. The usual excuse is, "It's the same technology we sell to the Western countries. It doesn't really differ from what we sell to Iran or China. It's just that since those countries don't have a strong rule of law, they end up abusing the system. In the West, we have due process and we have courts judging whether they should be doing that or not."

This is not a valid excuse for many of these companies anymore and they themselves have to come under some pressure from the Western governments and civil society.

The lesson here is that social media and technology can definitely make protests more effective. You look at what happened in Tunisia just a few weeks ago. Twitter and Facebook were used to get people into the streets. This is something that deserves recognition. The problem is that if the government doesn't end up falling in the end, the government also gets much more data and much better technology to engage in a crackdown.

What we saw happening in Iran two years ago was that the government simply went and collected all the tweets and Facebook messages and then went and arrested whoever it wanted because it had all the data. It's the same thing we saw in Belarus. Yes, it helped to bring people into the streets, but if the government doesn't fall in the end, it has a much better capacity, I would argue, than before technology, to actually go and track down anyone it doesn't like. So we have to be very careful.

The other thing to keep in mind here is that it's not just a question of whether technology and social media make protest more effective; we also have to answer the question of whether technology, the Internet, and new media also make protest more likely. This is the key question.

If you believe that there is some sense of this engagement by young people who turn to YouTube and Facebook in places like Iran and China to satisfy the demands they cannot satisfy in the real world, then, yes, you have to consider that probably they will be less likely to participate in the political process in those countries. They may not join the opposition movement or they may just want to join virtual campaigns. There is plenty of opposition in many of these countries that exists nowhere but the Internet. Often it does not translate into any real-world action.

This is what bothers me so much: The next generation of activists in places like Belarus will believe that they are actually changing something by signing petitions on Facebook and by organizing all kinds of virtual protests, without actually changing anything in the real world. The government is happy to have them isolated in this digital sandbox without ever going out into the streets and protesting in the real world.

This is the fear that I have, because many of these new media movements, while they do look promising, have no way to connect to the older, established political movements in some of these countries, whether it's Belarus, Egypt, Russia, or China. Finding a way to bridge the gap between these young digital natives turning to Facebook and Twitter and wanting to protest there, and the older generation of activists who are prepared to face the consequences and go to jail, will be a very important task that we don't know how to solve yet.

We do need to keep in mind the question of whether the Internet, technology, and social media make protests more likely, and not just focus on whether protests become more effective. My fear is, yes, it will be possible to mobilize the entire country in Iran or China through Facebook in a year or two years or five years at most. But being able to mobilize them is very different from having them actually show up in the streets and protest.

There are certain features in social media and technology that make it easier for the government to monitor what people are doing online, to harass them online with cyber attacks, or just to fund all sorts of funny websites that distract people from politics altogether. In the book I describe one website which is affiliated with the Kremlin, which basically is an entertainment website. They have very funny TV shows which revolve around sex and are not about ideology. The Kremlin is happy with that site because it helps to keep people off the streets.

We will be seeing more and more of that, rather than just blunt Internet censorship, in part because all of these political regimes have to evolve and adapt to the more capitalist economies that all of them are running. That will require some degree of flexibility in how their public discourse functions.

So we will be probably seeing less censorship overall, but much of the censorship will become targeted, and people who may be dissenting otherwise will just be distracted from politics. We will be seeing the emergence of online propaganda, with some of those governments not just paying bloggers, but deliberately creating all sorts of websites and campaigns which, instead of trying to suppress what a dissident in China or Russia has to say, would actually be trying to discredit his or her reputation.

Instead of censoring something on the Chinese Internet, for example, and thus risking that this information will be reposted to 200 other blogs, the government tries to accuse the person who posted the information of being a Russian spy or receiving money from America. This makes other people and other bloggers much less likely to repost what they have just read.

There are all sorts of ways in which governments are smartening up, and they are turning to many of the techniques that are well known to Western politicians. There is the technique of astroturfing, which are bloggers who present themselves as genuine voices on some issues, while actually being paid by the government. It does not come from China. It does not come from Russia. It comes from political and corporate campaigns here in the United States. So a lot of these techniques are being borrowed from America and Europe.

We do need to be much more careful in expecting major political and social turmoil in these countries simply because the citizens are online.

Thank you.

Questions and Answers

QUESTION: James Starkman. Thank you for a very interesting discussion.

To what degree do you think American Internet carriers should self-censor? How much self-censorship has occurred, for example, with regard to pornography? What are the laws that govern the regular media as opposed to the Internet media that exist today? To what degree is there voluntary self-censorship, particularly like the Google-China example?

EVGENY MOROZOV: There are existing laws on libel, privacy, and many other issues in America. I don't know why so many people assume that these laws wouldn't apply online. It's just that some of them are very difficult to enforce in the virtual world, because information spreads quickly, and maybe the expectations of privacy online are now much lower.

I think all of the existing laws have to be applied somehow to the Internet. It may be that we'll need to change business models for many of them. For example, the entertainment industry may need to change the business model, because it's very tough to enforce copyright laws on the Internet.

The degree to which they have to self-censor should not be driven by their ideological assumptions about the Internet. It has to be driven by the presence of the existing laws, which have not been canceled just because everything has moved online.

What happened in China with Google is a slightly different story. They kind of entered into a pact with the devil, because the Chinese kept changing the terms of whatever contract they signed, almost every three months. Google was asked to add new features to the censorship system. They were asked to remove links to the main homepage from google.cn. YouTube was blocked.

They entered into this deal with the Chinese, and the Chinese kept adding new requirements. At some point, when Google was struck with cyber attacks, they just thought it was enough, and they chose to completely restructure the relationship. It probably was a smart move, given that they could not simply expect and predict how the Chinese would react next and what kinds of conditions they would demand of Google.

But we have to distinguish between the demands that authoritarian governments and Western governments place on these companies, in part because the rule of law still exists in this country, and it does not exist to the same extent in China. So their governments have no problem disregarding their own previous commitments.

We have to be careful not to lump all of this together. Some of this is political, some of this is legal, and many of these companies are not angels themselves.

But once a precedent is being established, when a company like Research In Motion, the maker of BlackBerry, concedes to the demands of the Indian state or the Saudis, everyone else wants to impose their own demands. So now we see that the government of Indonesia wants to block access to any sort of pornographic websites on the BlackBerry simply because they already know that this company gave in to the Indians and the Saudis.

There is this domino effect, where it's possible that now everyone would want to jump on Research In Motion and basically demand that they configure their own systems to their own needs.

There are a lot of questions here which have to be thought of strategically. If the case would be that other companies and other governments will jump in, maybe it would be smart for the United States or Canada to be a little bit more aggressive in their defense of Research In Motion, because if other countries start imposing new restrictions, it may fundamentally reshape what the Internet looks like.

QUESTION: Susan Gitelson.

Your talk was a real eye-opener, especially early in the morning. But there is a whole area that you didn't have a chance to touch upon, and that is terrorism. We've read that a lot of disaffected young people, often Muslims, turn to the Internet to learn how to become a terrorist and a suicide bomber and organize actions with just small groups. They don't have to have a whole movement behind them.

EVGENY MOROZOV: There are two things which are basic truths about the Internet. One is that it facilitates collective action. The second is that it makes access to information easier and cheaper. Once you have those two in mind, you can figure out who stands to benefit the most and in what context. Sure, in the Middle East some of the people who will benefit will be the extremists and the terrorists. In some cases it will be nationalists and whoever else.

I don't think it's possible to resolve all these questions, from terrorism to extremists, to nationalists, to dissidents, in one comprehensive policy. That's why the whole idea of Internet freedom as a new pillar of foreign policy is misguided. The United States will be forced to engage in crackdowns on the Internet and to engage in cyber attacks, as we already know—and some of them go unreported even to Congress—to pursue its own strategic objectives.

The argument I'm making in the book is that, instead of trying to come up with this centralized approach which you can carry under the banner of Internet freedom, we need to empower regional experts and people in the State Department. These people may not know much about the Internet, but they will be able to understand how those two basic features—its impact on collective action and its impact on access to information—are likely to reshape their own areas of expertise and policy areas.

What has happened right now is that, instead of empowering these regional experts to think about the impact of the Internet on their own turf, the State Department empowered very smart technologists, who have a lot of experience in Silicon Valley. They know everything that there is to know about blogs and Twitter, but they may not know much about the history of Chinese foreign policy or how the Iranian government is likely to react to whatever America does. This is a very dangerous process and we need to move away from that.

But once you empower the right people, they will be able to recognize all of those pitfalls, whether it's terrorists using the Internet, copyright pirates, nationalists, or someone else.

The quest here is about sort of the first epistemological principle: Who gets to look at the problem and who gets to solve it? We have been empowering the wrong people to look at the problem and we have been empowering the wrong people to solve it.

I don't know to what extent that answers your question. Before we start asking questions about political issues —whether it's terrorism or something else—we need to make sure that our own policymaking apparatus is resilient enough to foresee challenges like terrorism and cyber attacks that will eventually create some traps for policymakers. Carrying the banner of Internet freedom may not be particularly helpful.

QUESTION: John Richardson.

Since you have a unique background, my question is really a variation on the theme of sparing the rod and spoiling the child. We have examples recently of this professor at Yale talking about how the Chinese raise their children vis-à-vis how the Americans do. You talked about Germany, that part of Germany where they didn't get Western television and they were politically more active.

My point is, from your point of view, isn't some level of strict government, authoritarian government, sometimes quite useful? I'll give you the example—a silly example, maybe—of the very famous Soviet marshal in the Second World War who played a crucial role at Stalingrad and Kursk, who had no fingernails.

EVGENY MOROZOV: It's an easy answer: Of course, it's often very useful. The question is, is it worth the cost? Yes, the Chinese were much better at handling the financial crisis. Does it make you feel eager to move to China and become a citizen there?

There are certain issues and challenges which authoritarian governments would be able to handle much more efficiently and professionally, because they just do not have any kind of distraction coming from civil society. They do not have Human Rights Watch throwing around that they are abusing prisoners or whatever, the way it happens in America.

The simplest answer I can give is that, sure, it can be useful, and sure, it can be effective. But most of us are aware of what the costs are.

I'm not sure I would want the Chinese, Russians or Iranians playing a disproportionate role in shaping the future of Internet governance, because I know which way they would push for. They would want to have governments to have more oversight over what's happening online. They would want to have a say in what kinds of websites can appear online and what websites cannot. They would want to have a say in how basic infrastructure would work and whether the governments will have the capacity to wiretap or eavesdrop on the communications.

Most of us are aware of the costs. So the question is, what it is that we're trying to accomplish?

I would not want China to be promoting democracy in Russia, because I don't think they will be doing a good job of it.

QUESTION: Harry Langer.

Could you please discuss the impact of cyber warfare on the military, as well as industrial espionage—for example, the attack on the Iranian nuclear facilities and the theft of sensitive technology from industry, as well as government?

EVGENY MOROZOV: There is no good news, unfortunately, for me to report. We are bound to see more governments, both in the West and authoritarian ones, seeking to establish more control over cyberspace, simply to prevent leaks, espionage, or the kinds of effects that may happen if someone penetrates a nuclear power grid.

The interesting thing about Stuxnet is that there was actually no role that the Internet played in that particular development. It all happened offline. Those centrifuges were not connected to the Internet. It all happened by bringing the virus on a USB stick and inserting it into the system.

That little detail got lost in the public conversation, and now all sorts of governments will be trying to use Stuxnet as an excuse to crack down on the Internet, even though the Internet played no role whatsoever. We'll be seeing that in Iran and elsewhere.

With regard to cyber warfare, the problem in assessing the nature of the threat is that people who are shaping the conversation in most cases have a direct stake in the particular outcome of that conversation. So you have a lot of contractors from the cyber security industry planting all sorts of fears into the public debate, without providing any evidence, because they say the evidence is classified, or they point to examples and then twist them in a certain manner.

Yes, something happened in an Australian water-management plant 12 years ago, and someone managed to disable the system, but it didn't happen because hackers managed to penetrate into it. It happened because a disgruntled employee already had all the credentials and he managed to get in and press the wrong button.

But you will not hear that detail about the disgruntled employee. You will just be told that the Internet is so insecure that someone can penetrate the Australian water-management plant system.

We have to be very careful in terms of assessing many of the threats, because they are twisted one way or another by people who have a stake in who gets part of the pie. The kind of money that is invested in cyber security is growing by the year. We have to be very careful to assess that some of those threats are actually real and some of those threats actually come from the Internet and not from people inserting USB sticks or pressing the buttons when they already have the credentials.

It does pose a problem, which is not in any way recognized in the Internet freedom agenda. You have Hillary Clinton complaining about countries that engage in cyber attacks.

In her speech last year, she said any country that engages in cyber attacks should bear responsibility for what they are doing. Then a month ago, we learned that Cyber Command in America has been engaged in cyber attacks forever, without ever actually telling Congress about it, because they thought there was some kind of exception.

Will they be held responsible for what they did? That's sort of a secondary question, but my point is that it does tap a lot of problems and traps for American policymakers. They have to be a little bit less naïve about selling this concept of Internet freedom to foreigners and abroad, because eventually they will be asked to explain themselves. And they can't, in some cases.

QUESTION: Richard Valcourt, *International Journal of Intelligence*.

Can you distinguish a little bit between the social dynamics involved in the circulation of, say, *samizdat* literature in the former Soviet Union and the current use of social media in creating a certain kind of resistance in countries that have autocratic rule?

EVGENY MOROZOV: First of all, it's much easier to trace what's being exchanged online than what's being exchanged offline.

You may have heard about this group, Anonymous, that has been launching cyber attacks on the websites of Amazon, PayPal, and Visa to protest against their treatment of Wikileaks. The interesting thing is that they released a press release and they actually forgot to delete the name of the user of the computer from the metadata that was in that PDF file. You could actually go and check who wrote the press release, and that guy was arrested.

It's a bunch of teenagers engaged in those attacks, and we should not expect them to be very cautious. But I doubt he would ever put his name on whatever press release in print form. This is one part.

The other part is that, while it does make it easy for governments to trace it, it's also more resilient, in the sense that it's very hard to get something off the Internet, as, again, the U.S. government itself discovered with Wikileaks.

It is very hard to make information disappear. There are people who basically want to host it on their own servers. It's easier to make it disappear by just brutal censorship. You can just ban access to websites, and then, as new websites pop up, you can ban access to new websites. It will limit the exposure that most people have to this information. It will not eliminate it altogether. Dissidents will still have their own networks through which to pass it on.

The key distinction that we need to draw is between professional dissidents—people who know what the risks are and know that if something goes wrong, they will go to prison—and the wider audience of people who may just go and sign a petition or join a Facebook group, thinking that they are participating in some democratic process, without being aware of any costs.
Anyone who has joined a group that campaigns against Ahmadinejad in Iran should probably be aware that they can be easily traced simply by looking up the membership list of that group, which is public. I hope that everyone knows that.

But I'm not sure that that is really the case. Even if you look at the protests in Iran in 2009, there were a lot of people who changed their Twitter avatar to green. They would add some green features to their portrait. The way they would do that would be by going to a website and uploading their photo and having a green-color photo in return.

No one ever asked, who is the guy behind this website? Who has set up this website, where people can go and upload photos? It was kind of an innocent guy in San Francisco, but it may as well be someone working on behalf of the Iranian government who just wants to know the IP addresses of everyone who feels sympathetic to the Iranian cause, which you can do once you upload a photo.

These kind of non-professional, amateur dissidents, who present the greatest promise of social media, are the ones who are not fully aware of the risks.

I'm not sure that was the case with *samizdat*, in part because it was much less complex. You have a piece of paper. You either distribute it or you don't, and you know what the risks are. Now you don't know what the risks are, because there are so many ways to participate on different websites and platforms, all of them having different privacy policies.

QUESTION: William Verdone. Thank you.

In keeping with the thread of East Berlin, I was friendly with a number of people back in the late 1970s, early 1980s, and they didn't want to know about America; they wanted to know about *Dynasty*, *Falcon Crest*, and *Dallas*.

But going forward, there are revolutions now that are color-coded. There was orange, and I don't remember the color for Tunisia, but there was a Saffron Revolution in Burma. Some of the monks, with whom I have become friends—there is a Buddhist monastery in Brooklyn—were tortured over a period of ten years or more. It's not so much the Internet, they said to me, but it was the camera that is on our cell phones that sent these images around the world. They said that maybe peripherally this had something to do with Aung San Suu Kyi's release recently.

Can you address the power of the picture, as you were alluding to, as opposed to blocking literature on the websites?

EVGENY MOROZOV: Much of it depends on the particular political situation in the country. You look at the power of the picture and you look at what happened in Somalia in 1993, when photos of American soldiers dragged through the streets of Mogadishu made the rounds on cable television. It was not exactly favorable to democracy or peace in Somalia.

We have to be attentive to the power of the image. In the case of Iran, we saw the famous video of the 27-year-old woman who was shot, Neda. It did create a lot of sympathy and empathy. But they also have the power to mislead.

The fact that that video was taken made many people think that bloggers and people online have much more power than they actually do. Much of the conversation then focused on that video as opposed to the broader political and social context in which the Green Movement emerged. It looked like a popular movement driven from the bottom up, while it actually had very well-established leaders. It does have the power to also change the conversation, not necessarily for the better, in the West.

There is one last comment I would like to make about the power of journalism and media here. The reason why we hear so many optimistic and rosy stories about the power of bloggers and the power of new media is because Western journalists who cover places like Egypt, China, or Iran, end up talking only with one particular subset of bloggers. They end up with those who want to talk to Western journalists; they disproportionately happen to be those who speak English, who already support secular values, who want democracy and who want a Western kind of political regime to prevail.

People from the Muslim Brotherhood do not necessarily want to talk to BBC or CNN, even though they have plenty of bloggers who are very active online. A lot of Iranian conservative bloggers would never speak to a foreign reporter, because it will get them into trouble.

We end up with these very one-sided news stories about bloggers being dissidents, simply because Western journalists do not bother looking and reporting on the other side of the story, which often is much more interesting and fascinating than the struggle of the secular bloggers.

That's why I'm emphasizing the role for us to get the first principles right. We do need to make sure that we have the right processes and procedures in place, and not to make wrong assumptions about the power of the Internet. If the only thing you look at is the Internet itself, and not how it's being used by the Chinese, Iranians, or Russians, you end up with a very optimistic scenario. I want to push away from just thinking about the Internet through the lens of the Internet and begin to think of it through the lens of local politics on the ground.

Thank you so much.

JOANNE MYERS: Thank you for a wonderful morning on politics and technology. It was really terrific.