THE WALL STREET JOURNAL.

THE SATURDAY ESSAY

The Dark Side of the Digital Revolution

Google's Eric Schmidt and Jared Cohen, fresh from a visit to North Korea in January, on why the Internet is far from an unalloyed good to the citizens of dictatorships around the world.

By Eric Schmidt and Jared Cohen
Updated April 19, 2013 2:59 p.m. ET

How do you explain to people that they are a YouTube sensation, when they have never heard of YouTube or the Internet? That's a question we faced during our January visit to North Korea, when we attempted to engage with the Pyongyang traffic police. You may have seen videos on the Web of the capital city's "traffic cops," whose ballerina-like street rituals, featured in government propaganda videos, have made them famous online. The men and women themselves, however—like most North Koreans—have never seen a Web page, used a desktop computer, or held a tablet or smartphone. They have never even heard of Google (or Bing, for that matter).

Eric Schmidt and Bill Richardson examine the content that a North Korean soldier is looking at on his computer screen. ASSOCIATED PRESS

RELATED

- The Trade in the Tools of Tech Tyranny
- Korea Real Time: Jasper Kim: North Korea Needs the Internet so Let's Help

Even the idea of the Internet has not yet permeated the public's consciousness in North Korea. When foreigners visit, the government stages Internet browsing sessions by having "students" look at pre-downloaded and preapproved content, spending hours (as they did when we were there) scrolling up and down their screens in totalitarian unison. We ended up trying to describe the Internet to North Koreans we met in terms of its values: free expression, freedom of assembly, critical thinking, meritocracy. These are uncomfortable ideas in a society where the "Respected Leader" is supposedly the source of all information and where the penalty for defying him is the persecution of you and your family for three generations.

North Korea is at the beginning of a cat-and-mouse game that's playing out all around the world between repressive regimes and their people. In most of the world, the spread of connectivity has transformed people's expectations of their governments. North Korea is one of the last holdouts. Until only a few years ago, the price for being caught there with an unauthorized cellphone was the death penalty. Cellphones are now more common in North Korea since the government decided to allow one million citizens to have them; and in parts of the country near the border, the Internet is sometimes within reach as citizens can sometimes catch a signal from China. None of this will transform the country overnight, but one thing is certain: Though it is possible to curb and monitor technology, once it is available, even the most repressive regimes are unable to put it back in the box.

FROM REVIEW

- Seven Lessons for Fixing an Economy
- By God's Nails! Careful How You Curse

What does this mean for governments and would-be revolutionaries? While technology has great potential to bring about change, there is a dark side to the digital revolution that is too often ignored. There is a turbulent transition ahead for autocratic regimes as more of their citizens come

online, but technology doesn't just help the good guys pushing for democratic reform—it can also provide powerful new tools for dictators to suppress dissent.

Fifty-seven percent of the world's population still lives under some sort of autocratic regime. In the span of a decade, the world's autocracies will go from having a minority of their citizens online to a majority. From Tehran to Beijing, autocrats are building the technology and training the personnel to suppress democratic dissent, often with the help of Western companies.

Of course, this is no easy task—and it isn't cheap. The world's autocrats will have to spend a great deal of money to build systems capable of monitoring and containing dissident energy. They will need cell towers and servers, large data centers, specialized software, legions of trained personnel and reliable supplies of basic resources like electricity and Internet connectivity. Once such an infrastructure is in place, repressive regimes then will need supercomputers to manage the glut of information.

Despite the expense, everything a regime would need to build an incredibly intimidating digital police state—including software that facilitates data mining and real-time monitoring of citizens—is commercially available right now. What's more, once one regime builds its surveillance state, it will share what it has learned with others. We know that autocratic governments share information, governance strategies and military hardware, and it's only logical that the configuration that one state designs (if it works) will proliferate among its allies and assorted others. Companies that sell data-mining software, surveillance cameras and other products will flaunt their work with one government to attract new business. It's the digital analog to arms sales, and like arms sales, it will not be cheap. Autocracies rich in national resources—oil, gas, minerals—will be able to afford it. Poorer dictatorships might be unable to sustain the state of the art and find themselves reliant on ideologically sympathetic patrons.

And don't think that the data being collected by autocracies is limited to Facebook posts or Twitter comments. The most important data they will collect in the future is biometric information, which can be used to identify individuals through their unique physical and biological attributes. Fingerprints, photographs and DNA testing are all familiar biometric data types today. Indeed, future visitors to repressive countries might be surprised to find that airport security requires not just a customs form and passport check, but also a voice scan. In the future, software for voice and facial recognition will surpass all the current biometric tests in terms of accuracy and ease of use.

Today's facial-recognition systems use a camera to zoom in on an individual's eyes, mouth and nose, and extract a "feature vector," a set of numbers that describes key aspects of the image, such as the precise distance between the eyes. (Remember, in the end, digital images are just numbers.) Those numbers can be fed back into a large database of faces in search of a match. The accuracy of this software is limited today (by, among other things, pictures shot in profile), but the progress in this field is remarkable. A team at Carnegie Mellon demonstrated in a 2011 study that the combination of "off-the-shelf" facial recognition software and publicly available online data (such as social-network profiles) can match a large number of faces very quickly. With cloud computing, it takes just seconds to compare millions of faces. The accuracy improves with people who have many pictures of themselves available online—which, in the age of Facebook, is practically everyone.

THE SATURDAY ESSAY

- Fifteen Days in Rome: How the Pope Was Picked (4/13/13)
- How Machiavelli Saved My Family (4/6/13)
- When Simplicity Is the Solution (3/30/13)
- The Brains of the Animal Kingdom (3/23/13)
- Let Them Eat Fat (3/16/13)
- What to Look for in a New Pope (3/9/13)
- The Tyranny of the Queen Bee (3/2/13)

By indexing our biometric signatures, some governments will try to track our every move and word, both physically and digitally. That's why we need to fight hard not just for our own privacy and security, but also for those who are not equipped to do so themselves. We can regulate biometric data at home in democratic countries, which helps. But for newly connected citizens up against robust digital dictatorships, they will need information and tools to protect themselves—which democracies and nongovernmental groups will need to help provide.

Dictators, of course, are not the only beneficiaries from advances in technology. In recent years, we have seen how large numbers of young people in countries such as Egypt and Tunisia,

armed with little more than mobile phones, can fuel revolutions. Their connectivity has helped them to challenge decades of authority and control, hastening a process that, historically, has often taken decades. Still, given the range of possible outcomes in these situations—brutal crackdown, regime change, civil war, transition to democracy—it is also clear that technology is not the whole story.

Observers and participants alike have described the recent Arab Spring as "leaderless"—but this obviously has a downside to match its upside. In the day-to-day process of demonstrating, it was possible to retain a decentralized command structure (safer too, since the regimes could not kill the movement simply by capturing the leaders). But, over time, some sort of centralized authority must emerge if a democratic movement is to have any direction. Popular uprisings can overthrow dictators, but they're only successful afterward if opposition forces have a plan and can execute it. Building a Facebook page does not constitute a plan.

History suggests that opposition movements need time to develop. Consider the African National Congress in South Africa. During its decades of exile from the apartheid state, the organization went through multiple iterations, and the men who would go on to become South African presidents (Nelson Mandela, Thabo Mbeki and Jacob Zuma) all had time to build their reputations, credentials and networks while honing their operational skills. Likewise with Lech Walesa and his Solidarity trade union in Eastern Europe. A decade passed before Solidarity leaders could contest seats in the Polish parliament, and their victory paved the way for the fall of communism.

Most opposition groups spend years organizing, lobbying and cultivating leaders. We asked former secretary of state Henry Kissinger, who has known many of the major revolutionary leaders of the past 40 years, what is lost when that timetable is advanced. "It is hard to imagine de Gaulles and Churchills appealing in the world of Facebook," he says. In an age of hyperconnectivity, "I don't see people willing to stand by themselves and to have the confidence to stand up alone." Instead, a kind of "mad consensus" will drive the world, Mr. Kissinger argues, and few people will be willing to openly oppose it—even though that's precisely the kind of risk that a great leader must take.

"The empowered citizen," Mr. Kissinger says, "knows the technique of getting people to the square, but they don't know what to do with them when they are in the square. They know even less of what to do with them when they have won." These people can get easily marginalized, he explains, because their strategies lose effectiveness over time.

Mahmoud Salem, an Egyptian blogger-turned-activist who became a spokesman for his country's 2011 revolution, is a bit more optimistic about the promise of online activism, yet he shares some of the American statesman's concerns about the difficulties of moving from activism to governance. Mr. Salem is highly critical of his fellow Egyptians for what he sees as their inability to move past the short-term goals of unseating Hosni Mubarak and opening the political system to competition. As he wrote in June 2012, just after Egypt's first post-revolution presidential election, "If you are a revolutionary, show us your capabilities. Start something. Join a party. Build an institution. Solve a real problem. Do something except running around from demonstration to march to sit-in. This is not street work: real street work means moving the street, not moving in the street."

It's this transition that digital revolutionaries now have to make—from protest to politics. Historically, a prominent position grew out of a degree of public trust (with the exceptions of, say, warlords or machine bosses). The visibility of a high-profile leader corresponded with the size of his or her support base. But in the future, with the broad reach of digital media, this equation will be inverted. Prominence will come earlier and more easily; only then will a would-be leader start to build tangible support, credentials and experience.

Opposition groups will have to compete with each other to have the best plan for their country's future, the best set of internal and external alliances and the most useful operational tool kits and hubs for organizers. If you're running an opposition group, your influence will be measured not only by the number of supporters you can get to a rally but also by the number of times your field manual is downloaded, the comments on your proposed constitution and the guest posts on your blog.

Competition is as healthy for opposition groups as it is for companies. Mr. Kissinger is right that dissident organizations need time to gestate, but technology can accelerate that process, helping communities to assemble and to refine themselves. In the long run, technology will continue to do what it does best: connect people to each other and to ideas. And leaders will continue to do what they do best: discern what truly matters and build plans to get from the present to the future.

Dictators and autocrats in the years to come will attempt to build all-encompassing surveillance states, and they will have unprecedented technologies with which to do so. But they can never succeed completely. Dissidents will build tunnels out and bridges across. Citizens will have more ways to fight back than ever before—some of them anonymous, some courageously public.

The digital revolution will continue. For all the complications this revolution brings, no country is worse off because of the Internet. And with five billion people set to join us online in the coming decades—perhaps someday even the Pyongyang traffic police and the students in the Potemkin computer lab we visited in North Korea among them—the digital future can be bright indeed, despite its dark side.

—Mr. Schmidt is Google's executive chairman and former CEO. Mr. Cohen is the director of Google Ideas. They are the authors of "The New Digital Age: Reshaping the Future of People, Nations and Business," from which this essay is adapted, to be published on April 23 by Alfred A. Knopf.