

# Let's protest": Surprises in communicating against repression

Brian Martin

n Egypt in June 2010, a young man named Khaled Said was beaten to death by the secret police. In response, Google executive Wael Ghonim set up the Facebook page "We are all Khaled Said," and within a day, tens of thousands of people had joined. The Facebook page was used to publicize a series of protests against police brutality and government corruption, including a huge protest on 25 January 2011. As the resistance gathered momentum, Egyptian president Hosni Mubarak ordered Internet and mobile phone service be shut down.

In response, opponents used web proxies and other ways to communicate, including fax, dial-up modems, and ham radio. Due to mass-media censorship, many Egyptians had previously not heard about the protests; the Internet shutdown led them to take to the streets to find out what was happening. Before long, the pressure on Mubarak became so great that he stepped down. The protesters had overthrown a dictator.

We normally think of Facebook as a social-networking platform, not a tool for regime opponents. The IMAGE LICENSED BY INGRAM PUBLISHING

Egyptian revolution illustrates that network communication tools are especially valuable for challenging oppressive regimes when they are embedded in society, as standard methods for commercial and social purposes. On the other hand, they provide unparalleled opportunities for government surveillance. To understand the paradoxes of communicating against repressive regimes, it is useful to go back to the time before the Internet, when the primary media were newspapers, radio, and television. These are all mass, one-directional media and, as such, are ideal tools for repressive governments. All they have to do is run or control these media, and propaganda is the order of the day.

This was true in both fascist and communist regimes and, to a lesser extent, elsewhere. For example, in 1975, Indian Prime Minister Indira Gandhi declared a state of emergency, suspended parliament, arrested thousands of peopleand cut off electricity supplies to newspapers and put pressure on them to censor the news. In pre-Internet times, controlling the mass media was critically important to the survival of dictatorial governments. When insurgent troops attempted a coup d'état, their first port of call was television stations: broadcasting served as propaganda central.

#### Issuing a challenge

To challenge a repressive regime, there are three main approaches. One is to use legitimate procedures, such as courts and election campaigning.

Digital Object Identifier 10.1109/MPOT.2016.2569722 Date of publication: 8 September 2016

However, if the regime controls the courts and rigs the elections, this approach can achieve little. A second approach is armed struggle, for example, using a guerrilla army or terrorist attacks, though from their viewpoint they are freedom fighters. For example, the racist South African apartheid government called its armed opponents terrorists, though the government's own use of violence against opponents was much greater and deserved the label "state terrorism." Armed resistance to repressive governments has several disadvantages. Only some people, mostly young, fit men, can participate, and violence can alienate witnesses and solidify the commitment of government troops.

A third approach is unarmed resistance, using rallies, marches, strikes, boycotts, sit-ins, workplace occupations, and a host of other assertive methods that avoid physical violence against opponents. This third approach is called *nonviolent* struggle, people power, or civil resistance. In a statistical study of 323 anti-regime, secession, and anti-occupation struggles over a century, Erica Chenoweth and Maria Stephan found that nonviolent campaigns were far more likely to be successful than armed ones and also more likely to lead to free societies years later. Hence, the focus here is on nonviolent struggles, in particular on the role of communication.

#### Mass media and network media

Because regimes can easily control mass media, opponents often rely on network media that allow people to contact each other directly. The classic method is word of mouth, by face-toface conversations. Then came the telephone, allowing person-to-person conversations at a distance. With the rise of the Internet and mobile communications, the possibilities for network-type interactions have exploded, with options now including e-mail, texting, and numerous social media platforms. Not only is the technology available, its cost has declined dramatically while ease of use has improved. Social media are, by design, media for the people as both senders and receivers.

In 1989, the communist bloc dissolved with the collapse of Eastern European regimes including East Germany, Poland, and Czechoslovakia. This dramatic transformation of governments was achieved without violence (except in Romania), and is one of the best examples of how civil resistance can operate. The Soviet Union remained, and in 1991 there was a coup; President Gorbachev was arrested. Immediately, there was a popular nonviolent resistance, which succeeded without help from the West. The Internet, in its rudimentary form at the time, served as a valuable tool for the resistance in informing outsiders of what was happening and connecting different parts of the country.

With today's widespread network communication, a further transformation of nonviolent struggle has occurred. It is now possible to organize demonstrations in a very short time through Facebook, texting, and other means. The historical precedent would be crowds in which members talk with each other to decide what to do next, but now "smart crowds" can coordinate their activities via social media.

Then there is the ease of taking and distributing photos and videos, which is unprecedented historically. Police brutality can be recorded as it occurs and promptly uploaded or directly streamed online using applications such as Periscope. Atrocities that might once have been subject to media management by perpetrators now can be presented directly to audiences. On the other hand, there can be an overload of horrific stories, leading to "compassion fatigue." Injustices for which there is no visual record may fail to generate concern.

After the invasion of Iraq in 2003, reports began surfacing about abuses in U.S.-run prisons. But the brief mass media stories did not generate much concern. What broke open the issue was the publication in April 2004 of photos of torture in Abu Ghraib prison in Iraq. The prison guards had digital cameras and took numerous photos of their treatment of prisoners, including piles of naked bodies and the now iconic image of a hooded man standing on a box with electrodes attached to his body. Without digital photography, it is unlikely the perpetrators would have recorded their own abuses so liberally.

The photos might have remained unknown except that Joseph Darby, who was not involved, saw some of them and took them to the Army's Criminal Investigation Command, which undertook an investigation. Despite the sensational nature of the material, U.S. mass media were reluctant to break the story, with CBS's 60 Minutes II only going ahead to avoid being scooped by investigative journalist Seymour Hersh.

The Abu Ghraib scandal undermined the credibility of the U.S. government throughout the Middle East and continues to reverberate today. Yet it only surfaced through the confluence of several factors: ease of cheap photography, the courage of a whistleblower and investigators, and sufficient initiative by independent journalists to push the mass media to break the story. Much the same scenario had occurred 25 years earlier in breaking the story of the My Lai massacre committed by U.S. soldiers during the Vietnam War.

#### The value of embeddedness

On the surface, it might seem that dissidents would benefit from setting up their own special-purpose communication systems, designed with their requirements in mind. While such systems might be more suitable, they would suffer a major disadvantage: they could be targeted by the regime for disruption or infiltration.

Therefore, it is more helpful for resistance communication to piggyback on widely used systems. This is exactly what has occurred in significant struggles over many years. Protesters have used the telephone, e-mail, and social media as they have emerged. Regimes, if they shut a system down, risk alienating many others in the population, as in Egypt in January 2011. Paradoxically, the opponents' communication system is protected because so many people are using it for other purposes.

# The dark side of network communication

The rise of digital network communication has come with a downside: ubiquitous surveillance. Government agencies now collect data from all sorts of transactions: phone calls, texts, bank deposits, sales transactions, car travel, and many others. WikiLeaks founder Julian Assange even commented that whistleblowers might be better to use the postal service when communicating with journalists, because telecommunications are under such extensive surveillance.

In many cases, a person's actual messages are not saved, but rather metadata showing who they contacted, when, and for how long. This information is remarkably revealing, enabling patterns of interaction to be traced. Furthermore, social media data can be analyzed to find out about individuals' habits. This means that spy agencies can start by identifying a few dissidents and then, using their surveillance data, find out with whom these dissidents interact. Then these contacts can be subject to more intensive surveillance, for example, phone tapping and insertion of keystroke loggers on computers.

Digital communications thus have a dual role so far as resistance to repressive governments is concerned: they are powerful and convenient organizing tools, yet also avenues for intensive surveillance. The result is that the new battleground is over the security of communications.

One way for resisters to protect their messages with each other is through encryption. Spy agencies do not like encryption they cannot break and, for a couple of decades, have been pushing for requirements that they have access via backdoors. If the only targets were activists, this might have been feasible, but encryption is also vital to the security and credibility of financial and commercial transactions. Again, protection of activist communication benefits from wider uses of the technology.

The government strategy of tracking down opponents has a serious weakness: it assumes that opposition is organized hierarchically, with

a leadership cadre directing action. In essence, managers of surveillance operations assume opponents are organized the same way they are themselves. However, the most effective opposition movements are horizontally rather than vertically organized: they have no leaders or, rather, many participants who take leadership roles. This means the opposition cannot be stymied by arresting, discrediting, or buying off a few individuals at the top. The movement is driven by the coordination of numerous semi-autonomous groups and associated individuals. The movement is organized in the same way its communication is structured.

#### Unintended consequences

Vast resources are poured into military systems around the world to support training, salaries, equipment, and weapons. Many of the world's top scientists and engineers devote their efforts to developing more effective weapons systems and defenses against them. Part of this effort goes into military communications, widely considered a crucial part of any military system.

In comparison, nonviolent struggle has received hardly any support from governments and corporations, and has usually operated on a comparatively shoestring budget. The amount of research and development on communication for nonviolent struggle is minuscule. Because of this, nonviolent activists have relied on technologies that have become available for other purposes. In this sense, the usefulness of a communication technology, such as the telephone, e-mail, or Facebook, for nonviolent struggle is an unintended consequence of its development for other purposes, most commonly commercial and social uses.

Nonviolent struggle, despite receiving such limited financial support, has proved remarkably effective in bringing down repressive regimes. It is also the method of choice for a wide range of social movements, including the labor, environmental, and feminist movements. It is strange that such a widespread and effective mode of social struggle should have to make do with communication technologies designed for other purposes. This suggests that in some future stage in the evolution of communication technology, it will be designed for the express purposes of nonviolent resistance and then popularized for other uses.

Meanwhile, social movements and their opponents are increasingly engaged in online struggles over access, censorship, messages, and meanings. Cyberspace is a new domain for applying the principles of nonviolent action, with suitable modifications given that bodies are not directly at risk of physical violence. The implications for organizing, strategy, and tactics are still to be determined and, as so often in the past, it is likely that practical innovations, in both activism and opposition to it, will be the drivers of new thinking.

#### Read more about it

• E. Chenoweth and M. J. Stephan, Why Civil Resistance Works: The Strategic Logic of Nonviolent Conflict. New York: Columbia University Press, 2011.

• W. Ghonim, *Revolution 2.0.* London, UK: Fourth Estate, 2012.

• R. MacKinnon, Consent of the Networked: The Worldwide Struggle for Internet Freedom. New York: Basic Books, 2012.

• B. Martin, *Technology for Nonviolent Struggle*. London, UK: War Resisters' Int., 2001.

• B. Martin and W. Varney, *Nonviolence Speaks: Communicating Against Repression*. Cresskill, NJ: Hampton Press, 2003.

• S. E. Nepstad, *Nonviolent Struggle: Theories, Strategies, and Dynamics.* New York: Oxford University Press, 2015.

• S. Popovic, with M. Miller, *Blueprint for Revolution*. New York: Spiegel & Grau, 2015.

• K. Schock, *Civil Resistance Today*. Cambridge, UK: Polity Press, 2015.

• S. Vinthagen, A Theory of Nonviolent Action: How Civil Resistance Works. London: Zed Books, 2015.

#### About the author

**Brian Martin** (bmartin@uow.edu. au) is professor of social sciences at the University of Wollongong. He is the author of 15 books and numerous articles on nonviolent action, dissent, scientific controversies, and other topics.



# Unintended consequences: A study guide

ow that you've immersed yourself in some of the challenges and paradoxes we face as a society (as our cities, businesses, governments, and personal lives become more digitized), it is time to reflect on everything you've read.

As much as we hope you've enjoyed this collection of articles, we really want you to find value in the discussions and debates that come from it. We have included some questions to get you started. Remember, there often isn't one right answer. These issues are complex. Sometimes the best answer to a challenging question is simply to ask more questions; to interrogate the issues at hand, using a multidisciplinary lens. So consider these questions a launch pad that will inspire you to ask your own questions, too. Share your questions with your peers in small groups and seek to brainstorm together on what possible future directions you can take to ensure these matters are integrated into development frameworks.

We thank the authors in this issue for assistance in drawing out these major themes.

### "Valuations and human values (a.k.a. the irony of granola bar economics)"

1) Why did people throw rocks at the Google bus? Were

Digital Object Identifier 10.1109/MPOT.2016.2569758 Date of publication: 8 September 2016 the people on the buses really the targets of their animosity?

- 2) According to Rushkoff, growth is the prevalent feature of the digital economy. What impact does that have on companies? What impact does that have on workers? What impact does that have on neighborhoods and communities?
- 3) Is there a way to keep the possibilities that digital tools afford, without the commensurate detrimental effects? What solutions are there?

### "Let's protest: Surprises in communicating against repression"

1) Select a social networking application (e.g., Snapchat). What are its strengths and weaknesses for serving ordinary users and nonviolent campaigners?

- Suppose you are put in charge of a country's technology policy today. What communication technology would you promote to ensure that a dictator could never come to power? Explain your reasoning.
- 3) Imagine that you want to assist some foreign friends who live under an authoritarian government. You can mainly help by using the Internet. What skills do you think are most important for you to learn? You might reflect on the possibilities of learning foreign languages, encryption, Web design, data collection, data verification, organizing denial-of-service attacks, and hacking. How will these skills help your friends specifically?

## "Predictive policing and civilian oversight"

- Would you trust software more than you would a law enforcement officer?
- 2) Who should be held responsible when the software described in the article by Hirsh

IMAGE LICENSED BY INGRAM PUBLISHING