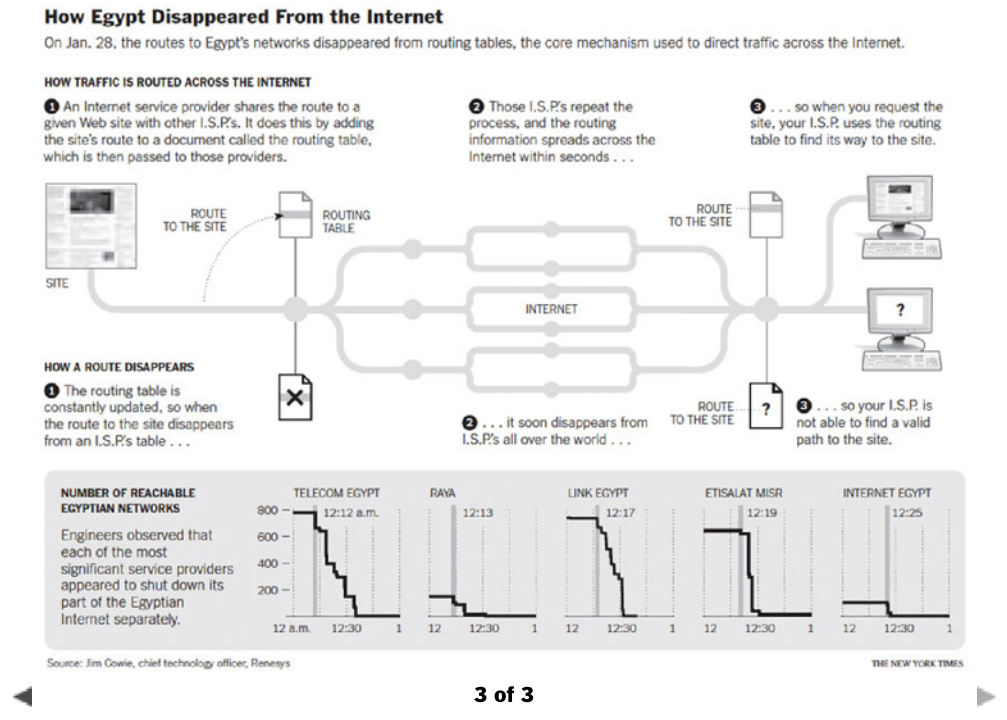
Egypt Leaders Found 'Off' Switch for Internet

BY JAMES GLANZ AND JOHN MARKOFF
FEBRUARY 16, 2011



3 of 3

Epitaphs for the Mubarak government all note that the mobilizing power of the Internet was one of the Egyptian opposition's most potent weapons. But quickly lost in the swirl of revolution was the government's ferocious counterattack, a dark achievement that many had thought impossible in the age of global connectedness. In a span of minutes just after midnight on Jan. 28, a technologically advanced, densely wired country with more than 20 million people online was essentially severed from the global Internet.

The blackout was lifted after just five days, and it did not save President Hosni Mubarak. But it has mesmerized the worldwide technical community and raised concerns that with unrest coursing through the Middle East, other autocratic governments — many of them already known to interfere with and filter specific Web sites and e-mails — may also possess what is essentially a kill switch for the Internet.

Because the Internet's legendary robustness and ability to route around blockages are part of its basic design, even the world's most renowned network and telecommunications engineers have been perplexed that the Mubarak government succeeded in pulling the maneuver off.

But now, as Egyptian engineers begin to assess fragmentary evidence and their own knowledge of the Egyptian Internet's construction, they are beginning to understand what, in effect, hit them. Interviews with many of those engineers, as well as an examination of data collected around the world during the blackout, indicate that the government exploited a devastating combination of vulnerabilities in the national infrastructure.

For all the Internet's vaunted connectivity, the Egyptian government commanded powerful instruments of control: it owns the pipelines that carry information across the country and out into the world.

Internet experts say similar arrangements are more common in authoritarian countries than is generally recognized. In Syria, for example, the Syrian Telecommunications Establishment dominates the infrastructure, and the bulk of the international traffic flows through a single pipeline to Cyprus. Jordan, Qatar, Oman, Saudi Arabia and other Middle Eastern countries have the same sort of dominant, state-controlled carrier.

Over the past several days, activists in Bahrain and Iran say they have seen strong evidence of severe Internet slowdowns amid protests there. Concerns over the potential for a government shutdown are particularly high in North African countries, most of which rely on a just a small number of fiber-optic lines for most of their international Internet traffic.

A Double Knockout

The attack in Egypt relied on a double knockout, the engineers say. As in many authoritarian countries, Egypt's Internet must connect to the outside world through a tiny number of international portals that are tightly in the grip of the government. In a lightning strike, technicians first cut off nearly all international traffic through those portals.

In theory, the domestic Internet should have survived that strike. But the cutoff also revealed how dependent Egypt's internal networks are on moment-to-moment information from systems that exist only outside the country — including e-mail servers at companies like Google, Microsoft and Yahoo; data centers in the United States; and the Internet directories called domain name servers, which can

be physically located anywhere from Australia to Germany.

The government's attack left Egypt not only cut off from the outside world, but also with its internal systems in a sort of comatose state: servers, cables and fiber-optic lines were largely up and running, but too confused or crippled to carry information save a dribble of local e-mail traffic and domestic Web sites whose Internet circuitry somehow remained accessible.

"They drilled unexpectedly all the way down to the bottom layer of the Internet and stopped all traffic flowing," said Jim Cowie, chief technology officer of Renesys, a network management company based in New Hampshire that has closely monitored Internet traffic from Egypt. "With the scope of their shutdown and the size of their online population, it is an unprecedented event."

The engineers say that a focal point of the attack was an imposing building at 26 Ramses Street in Cairo, just two and a half miles from the epicenter of the protests, Tahrir Square. At one time purely a telephone network switching center, the building now houses the crucial Internet exchange that serves as the connection point for fiber-optic links provided by five major network companies that provide the bulk of the Internet connectivity going into and out of the country.

"In Egypt the actual physical and logical connections to the rest of the world are few, and they are licensed by the government and they are tightly controlled," said Wael Amin, president of ITWorx, a large software development company based in Cairo.

One of the government's strongest levers is Telecom Egypt, a state-owned company that engineers say owns virtually all the country's fiber-optic cables; other Internet service providers are forced to lease bandwidth on those cables in order to do business.

Mr. Cowie noted that the shutdown in Egypt did not appear to have diminished the protests — if anything, it inflamed them — and that it would cost untold millions of dollars in lost business and investor confidence in the country. But he added that, inevitably, some autocrats would conclude that Mr. Mubarak had simply waited too long to bring down the curtain.

"Probably there are people who will look at this and say, it really worked pretty well, he just blew the timing," Mr. Cowie said.

Speaking of the Egyptian shutdown and the earlier experience in Tunisia, whose censorship methods were less comprehensive, a senior State Department official said that "governments will draw different conclusions."

"Some may take measures to tighten communications networks," said the official, speaking on the condition of anonymity. "Others may conclude that these things are woven so deeply into the culture and commerce of their country that they interfere at their peril. Regardless, it is certainly being widely discussed in the Middle East and North Africa."

Vulnerable Choke Points

In Egypt, where the government still has not explained how the Internet was taken down, engineers across the country are putting together clues from their own observations to understand what happened this time, and to find out whether a future cutoff could be circumvented on a much wider scale than it was when Mr. Mubarak set his attack in motion.

The strength of the Internet is that it has no single point of failure, in contrast to more centralized networks like the traditional telephone network. The routing of each data packet is handled by a web of computers known as routers, so that in principle each packet might take a different route. The complete message or document is then reassembled at the receiving end.

Yet despite this decentralized design, the reality is that most traffic passes through vast centralized exchanges — potential choke points that allow many nations to monitor, filter or in dire cases completely stop the flow of Internet data.

China, for example, has built an elaborate national filtering system known as the Golden Shield Project, and in 2009 it shut down cellphone and Internet service amid unrest in the Muslim region of Xinjiang. Nepal's government briefly disconnected from the Internet in the face of civil unrest in 2005, and so did Myanmar's government in 2007.

But until Jan. 28 in Egypt, no country had revealed that control of those choke points could allow the government to shut down the Internet almost entirely.

There has been intense debate both inside and outside Egypt on whether the cutoff at 26 Ramses Street was accomplished by surgically tampering with the software mechanism that defines how networks at the core of the Internet communicate with one another, or by a blunt approach: simply cutting off the power to the router computers that connect Egypt to the outside world.

But either way, the international portals were shut, and the domestic system reeled from the blow.

The Lines Go Dead

The first hints of the blackout had actually emerged the day before, Jan. 27, as opposition leaders prepared for a "Friday of anger," with huge demonstrations expected. Ahmed ElShabrawy, who runs a company called EgyptNetwork, noticed that the government had begun blocking individual sites like Facebook and Twitter.

Just after midnight on Jan. 28, Mahmoud Amin's iPhone beeped with an alert that international connections to his consulting company's Internet system had vanished — and then the iPhone itself stopped receiving e-mail. A few minutes later, Mr. ElShabrawy received an urgent call telling him that all Internet lines running to his company

were dead.

It was not long before Ayman Bahaa, director of Egyptian Universities Network, which developed the country's Internet nearly two decades ago, was scrambling to figure out how the system had all but collapsed between the strokes of 12 and 1.

The system had been crushed so completely that when a network engineer who does repairs in Cairo woke in the morning, he said to his family, "I feel we are in the 1800s."

Over the next five days, the government furiously went about extinguishing nearly all of the Internet links to the outside world that had survived the first assault, data collected by Western network monitors show. Although a few Egyptians managed to post to Facebook or send sporadic e-mails, the vast majority of the country's Internet subscribers were cut off.

The most telling bit of evidence was that some Internet services inside the country were still working, at least sporadically. American University in Cairo, frantically trying to relocate students and faculty members away from troubled areas, was unable to use e-mail, cellphones — which were also shut down — or even a radio frequency reserved for security teams. But the university was able to update its Web site, hosted on a server inside Egypt, and at least some people were able to pull up the site and follow the emergency instructions.

"The servers were up," said Nagwa Nicola, the chief technology officer at American University in Cairo. "You could reach up to the Internet provider itself, but you wouldn't get out of the country." Ms. Nicola said that no notice had been given, and she depicted an operation that appeared to have been carried out with great secrecy.

"When we called the providers, they said, 'Um, hang on, we just have a few problems and we'll be on again,' " she said. "They wouldn't tell us it was out."

She added, "It wasn't expected at all that something like that would happen."

Told to Shut Down or Else

Individual Internet service providers were also called on the carpet and ordered to shut down, as they are required to do by their licensing agreements if the government so decrees.

According to an Egyptian engineer and an international telecom expert who both spoke on the condition of anonymity, at least one provider, Vodafone, expressed extreme reluctance to shut down but was told that if it did not comply, the government would use its own "off" switch via the Telecom Egypt infrastructure — a method that would be much more time-consuming to reverse. Other exchanges, like an important one in Alexandria, may also have been involved.

Still, even major providers received little notice that the moves were afoot, said an Egyptian with close knowledge of the telecom industry who would speak only anonymously.

"You don't get a couple of days with something like this," he said. "It was less than an hour."

After the Internet collapsed, Mr. ElShabrawy, 35, whose company provides Internet service to 2,000 subscribers and develops software for foreign and domestic customers, made urgent inquiries with the Ministry of Communications, to no avail. So he scrambled to re-establish his own communications.

When he, too, noticed that domestic fiber-optic cables were open, he had a moment of exhilaration, remembering that he could link up servers directly and establish messaging using an older system called Internet Relay Chat. But then it dawned on him that he had always assumed he could download the necessary software via the Internet and had saved no copy.

"You don't have your tools — you don't have anything," Mr. ElShabrawy said he realized as he stared at the dead lines at his main office in Mansoura, about 60 miles outside Cairo.

With the streets unsafe because of marauding bands of looters, he decided to risk having a driver bring $7,000 in satellite equipment, including a four-foot dish, from Cairo, and somehow he was connected internationally again by Monday evening.

Steeling himself for the blast of complaints from angry customers — his company also provides texting services in Europe and the Middle East — Mr. ElShabrawy found time to post videos of the protests in Mansoura on his Facebook page. But with security officials asking questions about what he was up to, he did not dare hook up his domestic subscribers.

Then, gingerly, he reached out to his international customers, his profuse apologies already framed in his mind.

The response that poured in astonished Mr. ElShabrawy, who is nothing if not a conscientious businessman, even in turbulent times. "People said: 'Don't worry about that. We are fine and we need to know that you are fine. We are all supporting you.' "■