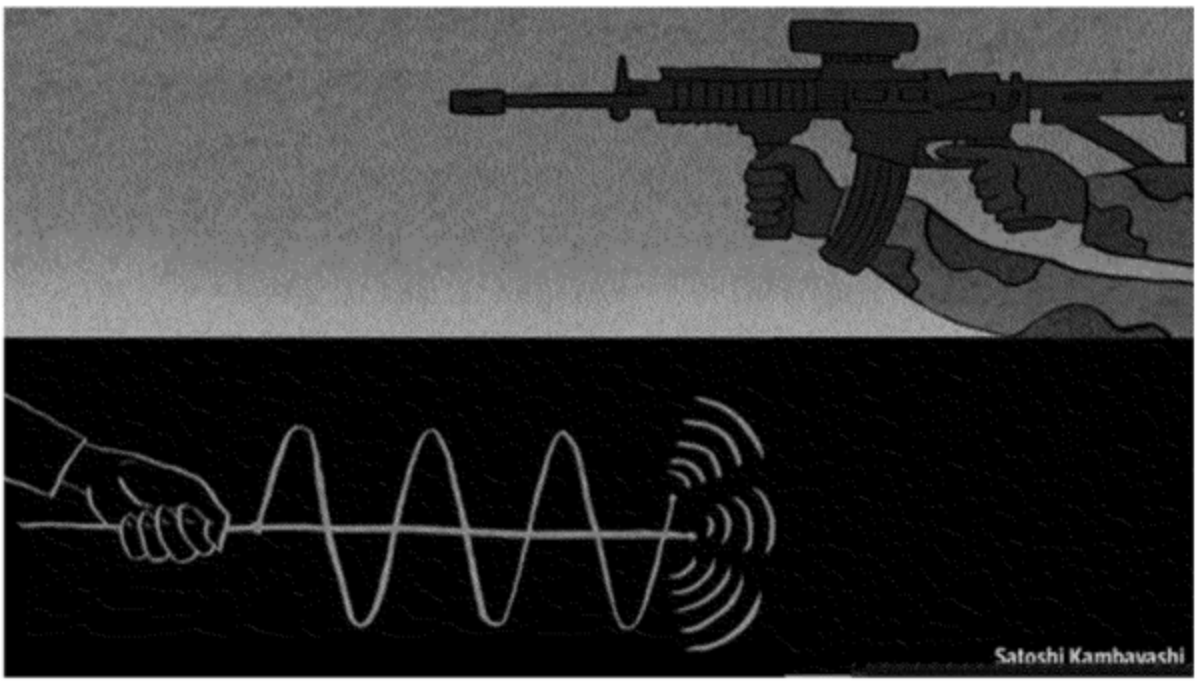
To: [redacted]; Patty Hartwell[redacted]; Michael Dubno[redacted]
From: Dan Dubno
Sent: Sun 3/20/2011 7:31:18 PM
Subject: Regarding Hourglass Initiative, etc., here's an interesting story about anonymizing technologies: in THE ECONOMIST
Daniel Dubno.vcf

Unorthodox links to the internet

Signalling dissent

Savvy techies are finding ways to circumvent politically motivated shutdowns of the internet

Mar 17th 2011 | from the print edition



WITH a tin can, some copper wire and a few dollars' worth of nuts, bolts and other hardware, a do-it-yourselfer can build a makeshift directional antenna. A mobile phone, souped-up with such an antenna, can talk to a network tower that is dozens of kilometres beyond its normal range (about 5km, or 3 miles). As Gregory Rehm, the author of an online assembly guide for such things, puts it, homemade antennae are "as cool as the other side of the pillow on a hot night". Of late, however, such antennae have proved much more than simply cool.

According to Jeff Moss, a communications adviser to America's Department of Homeland Security, their existence has recently been valuable to the operation of several groups of revolutionaries in Egypt, Libya and elsewhere. To get round government shutdowns of internet and mobile-phone networks, resourceful dissidents have used such makeshift antennae to link their computers and handsets to more orthodox transmission equipment in neighbouring countries.

Technologies that transmit data under the noses of repressive authorities in this way are spreading like wildfire among pro-democracy groups, says Mr Moss. For example, after Egypt switched off its internet in January some activists brought laptops to places like Tahrir Square in Cairo to collect, via short-range wireless links, demonstrators' video recordings and other electronic messages. These activists then broadcast the material to the outside world using range-extending antennae.

According to Bobby Soriano, an instructor at the Philippine branch of Tactical Tech, a British organization that teaches communication techniques to dissidents in five countries, such antennae can even foil government eavesdropping and jamming efforts. Directional antennae, unlike the omnidirectional sort, transmit on a narrow beam. This makes it hard for eavesdroppers to notice a signal is there.

Citizens banned?

Another way of confounding the authorities is to build portable FM radio stations. One broadcasting expert, who prefers not to be named but is currently based in Europe, is helping to develop a dozen such "backpack" radio stations for anti-government protesters in his native land in the Arabian peninsula. Though these stations have a range of only a few kilometres, that is enough for the leaders of a protest to use them to co-ordinate their followers. The stations' operators act as clearing houses for text messages, reading important ones over the air for everyone to hear.

Conventional radio of this sort cannot, unfortunately, transmit video or web pages. But a group called Access, based in New York, is trying to overcome that. To help democracy movements in the Middle East and North Africa get online, it is equipping a network of ham-radio operators with special modems that convert digital computer data into analogue radio signals that their equipment can cope with. These signals are then broadcast from operator to operator until they reach a network member in an area where the internet functions. This operator reconverts the signal into computer-readable data and then e-mails or posts the information online.

Satellites provide yet another way of getting online, though they are expensive to connect to. It is, however, beyond the authorities in most places to shut down a satellite operated by a foreign company or country. The best they can do is try to locate live satellite links using radiation-detection kit similar to that supposedly employed in Britain to seek out unlicensed televisions. The result is a game of cat and mouse between the authorities and satellite-using dissidents. Tactical Tech, for example, has trained dissidents in five countries to rig satellite dishes to computers in order to get online. It advises some users to log on only for short sessions, and to do so from a moving vehicle.

Such dishes can also be repurposed for long-range internet connections that do not involve satellites. Yahel Ben-David, an electrical engineer at the University of California, Berkeley, who has designed secret cross-border links to the internet for people in several countries, does so by adding standard USB dongles designed for home Wi-Fi networks. Thus equipped, two properly aligned dishes as much as 100km apart can transmit enough data to carry high quality video. Moreover, the beam is so tightly focused that equipment a mere dozen metres away from its line would struggle to detect it.

Creative ideas for circumventing cyber-attacks even extend to the redesign of apparently innocent domestic equipment. Kenneth Geers, an American naval-intelligence analyst at a NATO cyberwar unit in Tallinn, Estonia, describes a curious microwave oven. Though still able to cook food, its microwaves (essentially, short radiowaves) are modulated to encode information as though it were a normal radio transmitter. Thus, things turn full circle, for the original microwave oven was based on the magnetron from a military radar. From conflict to domesticity to conflict, then, in a mere six decades.

from the print edition | Science and Technology


Daniel Dubno
Hourglass Initiative
Founder and Executive Director
http://www.hourglassinitiative.org
[redacted]
Mobile
Work
41 West 83rd Street, Suite 9A
New York, NY 10024