SPENCER ACKERMAN SECURITY 02.07.2011 07:00 AM

U.S. Has Secret Tools to Force Internet on Dictators

When Hosni Mubarak shut down Egypt's internet and cellphone communications, it seemed that all U.S. officials could do was ask him politely to change his mind. But the American military does have a second set of options, if it ever wants to force connectivity on a country against its ruler's wishes. There's just one wrinkle. [...]

When Hosni Mubarak shut down Egypt's internet and cellphone communications, it seemed that all U.S. officials could do was ask him politely to change his mind. But the American military does have a second set of options, if it ever wants to force connectivity on a country against its ruler's wishes.

There's just one wrinkle. "It could be considered an act of war," says John Arquilla, a leading military futurist.

The U.S. military has no shortage of devices -- many of them classified -- that could restore connectivity to a restive populace cut off from the outside world by its rulers. It's an attractive option for policymakers who want an option for future Egypts, between doing nothing and sending in the Marines. And it might give teeth to the Obama administration's demand that foreign governments consider internet access an inviolable human right.

Arquilla, a professor at the Naval Postgraduate School, spent years urging the military to logic-bomb adversary websites, disrupt hostile online presences, and even cause communications blackouts to separate warring factions before they go nuclear. What the military can turn off, he says, it can also turn on -- or at least fill dead airspace.

Consider the Commando Solo, the Air Force's airborne broadcasting center. A revamped cargo plane, the Commando Solo beams out psychological operations in AM and FM for radio, and UHF and VHF for TV. Arquilla doesn't want to go into detail how the classified plane could get a denied internet up and running again, but if it flies over a bandwidth-denied area, suddenly your Wi-Fi bars will go back up to full strength.

"We have both satellite- and nonsatellite-based assets that can come in and provide access points to get people back online," Arquilla says. "Some of it is done from ships. You could have a cyber version of pirate radio."

Then there are cell towers in the sky. The military already uses its aircraft as communications relays in places like Afghanistan. Some companies are figuring out upgrades: FastCom, an effort led by the defense firm Textron, is a project that hooks up cellular pods to the belly of a drone, the better to keep cellular and data connections in the air without pilot fatigue. Underneath the drones, a radius of a few kilometers on the ground would have 3G coverage.

Sharon Corona, a spokeswoman for the project, says that there's an obstacle to using a technology like FastCom for an Egypt-like situation: The recipient devices need to be able to talk with the cell and data signal. But compliant phones or netbooks -- small and lightweight -- could conceivably be smuggled into a denied area.

Alternatively, operatives could smuggle small satellite dishes into a country. Small dishes were crucial to getting the internet back running in Haiti after last year's earthquake. It's how cameramen in war zones rapidly transmit high quality video from the middle of nowhere.

Of course, slow-flying drones or a broadcasting center in the sky have an inherent weakness: They're sitting ducks for any half-decent air defense system. (And did we mention that Hosni Mubarak became a national hero for his air defense prowess in the 1973 war against Israel?)

That leads to another possibility: "Just give people Thuraya satellite phones," says John Pike of Globalsecurity.org. The cheapish phones hunt down signals from space hardware.

Even expanding access to the military's own satellite communications networks is theoretically possible, Arquilla says. But he won't say more than that: "Let's just say that's an area decided at the level of the commander-in-chief."

In the absence of those options, there's always the old-school methods of jamming a government's communication frequencies and broadcasting favorable messages. That's the Commando Solo's specialty. "Jamming is something we think about in the context of shooting wars," says Arquilla, but "it may have its place in social revolutions as well."

The trouble is, if a government follows Egypt's lead and turns off the internet, it's not going to be keen to see a meddling foreign power turn it back on.

That act might not be as provocative as sending in ground troops or dropping bombs. But it's still an act of what you might call forced online entry -- by definition, a hostile one.

In situations like Egypt, siding with an uprising against a longtime ally is a difficult choice, whether analog or digital.

That might be why the military hasn't done it. Asked about whether the Pentagon would consider deploying mobile connectivity to restore internet access for a social uprising, all a senior official would say is that such a situation was "hypothetical."

And all that underscores how Egypt's internet shutoff pushed the poorly defined limits of cyber hostilities. Foreign actors don't really have a blueprint for responding. The U.S. military "has a great deal of expertise on rebuilding communications network, but that's ... very different when the government is interested in resisting," Arquilla says. "This is far less an engineering problem and far more a political one."

Image: Wikimedia

See Also:

- Egypt Arrests 4 Facebook Activists
- Egypt Hacked Vodafone to Send Pro-Regime Texts
- YouTube Rappers Clown Egypt's Dictator

- Inside the Air Force's Secret PsyOps Plane
- Radio Free Haiti, on the Ground and in the Skies

Danger Room senior reporter Spencer Ackerman recently won the 2012 National Magazine Award for Reporting in Digital Media.

SENIOR REPORTER

TOPICS DISSENT TECH INFO WAR MIDDLE EAST
