The Heritage Foundation
LEADERSHIP FOR AMERICA

ISSUE BRIEF

No. 3585 | APRIL 27, 2012

Target Cyber-Oppressors, Not U.S. Businesses

Helle C. Dale and Paul Rosenzweig

The Obama Administration has been heavily criticized for not acting forcefully to stem human rights abuses in the Middle East. Criticism of the Administration has largely focused on Iran and Syria, where Bashar al-Assad's government is guilty of atrocious bloodshed against its own people. In response, President Obama announced several new initiatives on April 23, including an interagency Atrocities Prevention Board and a new presidential executive order to protect Internet freedom, taking effect the same day.[1]

In a speech at the U.S. Holocaust Memorial Museum, Obama explained that the order was aimed at curbing the abuse of information technology, targeting Syrian and Iranian cyber-activists. There is good news and bad news in this. The good news is that the Obama Administration, under pressure, is finally putting teeth into its two-year-old Internet freedom policy, showing seriousness by sanctioning regimes that perpetrate human rights abuses via the Internet. The bad news is that the order also targets the companies that produce the advanced technologies used by the Iranians and Syrians for cybercensorship or tracking, many of which are American companies. There are better ways to approach the problem of human rights in cyberspace.

Getting Serious About the Internet and Human Rights. The executive order, titled "Blocking the Property and Suspending Entry into the United States of Certain Persons with Respect to Grave Human Rights Abuses by the Governments of Iran and Syria via Information Technology," states that the governments of Iran and Syria are attempting to upgrade their technological abilities to impede communication internally, as well as between their people and the outside world. It correctly establishes that it is in the interest of the United States to keep this flow of communication open. The order then authorizes the Treasury Secretary in consultation with the Secretary of State to freeze the assets of anyone determined to have engaged in abusive Internet activities, such as network disruption, monitoring, or tracking that could enable serious human rights abuses. This step should attract the attention of the perpetrators if the U.S. government follows through on the threat.

There can be no doubt that the State Department needed to strengthen enforcement of its Internet freedom policy as enunciated by Hillary Clinton in January of 2010. In this sense, the new policy is a welcome step. Clinton committed to "a comprehensive and innovative approach—one that matches our diplomacy with our technology, secure distribution networks for tools and direct support for those on the front lines."[2] The actions of the State Department, however, have not fully matched this commitment.

While Congress was providing funding for anti-censorship technologies to the tune of $50 million over three years, State was slow to disburse the funds. Eventually, Congress gave $10 million of this funding to the Broadcasting Board of Governors anti-censorship office, which in January opened the "Freedom to Connect Project" at Radio Free Asia. Further, while persecution of cyber-activists

This paper, in its entirety, can be found at **http://report.heritage.org/ib3585**

Produced by the Douglas and Sarah Allison Center for Foreign Policy Studies

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

has become part of the State Department's Human Rights Report, it has not been a high-profile issue in U.S. relations with countries in the Middle East or Cuba, China, and other rampant violators of freedom of expression.

Punish Human Rights Violators, Not Their Tools. Problematically, the executive order also targets anyone determined to "have sold, leased, or otherwise provided, directly or indirectly, goods, services, or technology to Iran or Syria likely to be used to facilitate computer or network disruption, monitoring, or tracking that could assist in or enable serious human rights abuses by or on behalf of the Government of Iran or the Government of Syria."[3]

It is indeed disconcerting that the mass Web-filtering tools used by Middle Eastern and North African governments in the course of the Arab uprisings and their aftermath have often been created by Western companies. According to a report by the OpenNet Initiative, a collaborative effort between several universities dedicated to exposing and analyzing Internet filtering operations, a number of American companies have sold their Web-filtering systems to repressive regimes that use these products to censor Web content.

Nevertheless, penalizing technology providers does not make sense in the long run, any more than it would making it a crime to use a computer because some bank robbers use computers to rob banks. Human rights violations are condemnable, irrespective of the technology involved.

Furthermore, this is also an export control problem. Controls only work if all the possible sources of supply agree to enforce the rules. Otherwise, government action may be morally satisfying but will have no effect other than to disadvantage American industry. It is clear that in this case, there will not be uniform worldwide agreement on the technology in question. This order will, in effect, be handing markets to Chinese companies that are glad to sell intercept capabilities. And what will the U.S. do when these companies, with protected markets in places like China, Iran, and Syria, use their economic advantage to compete with American companies?[4]

Instead of penalizing the companies, the Administration should:

- **Spend Internet freedom funds wisely.** Funds to support Internet freedom should be efficiently directed toward providing an incentive for private companies to design more effective firewall circumvention technologies. The Broadcasting Board of Governors has enjoyed a degree of success in funding the Global Internet Freedom Consortium.

- **Speak out against Internet freedom's worst offenders, and where possible, freeze their assets.** The U.S. should continue to unequivocally condemn nations who jail citizens for communicating on the Web, following the assessment of State's Annual Human Rights Report. The U.S. should let every nation know that status as a free nation depends not only on its human rights record but also on the degree to which it restricts freedom of expression over the Web.

- **Encourage other nations to join a coalition, which could provide the venue for "naming and shaming" offenders.** The Financial Action Task Force (FATF) provides a model for voluntary intergovernmental cooperation. Its purpose is combating money laundering and terrorist financing, and it encourages the development of national and international policies in member nations. An International Internet Freedom Task Force could similarly encourage the protection of freedom of expression on the Internet.

*—**Helle C. Dale** is Senior Fellow for Public Diplomacy in the Douglas and Sarah Allison Center for Foreign Policy Studies, a division of the Kathryn and Shelby Cullom Davis Institute for International Studies, and **Paul Rosenzweig** is a Visiting Fellow in the Center for Legal and Judicial Studies and the Allison Center at The Heritage Foundation.*

1. Barack Obama, "Blocking the Property and Suspending Entry into the United States of Certain Persons with Respect to Grave Human Rights Abuses by the Governments of Iran and Syria via Information Technology," Executive Order, April 23, 2012, http://www.whitehouse.gov/the-press-office/2012/04/23/executive-order-blocking-property-and-suspending-entry-united-states-cer (accessed April 26, 2012).
2. Hillary Clinton, "Internet Rights and Wrongs: Choices and Challenges in a Networked World," remarks at George Washington University, Washington, DC, February 15, 2011, http://www.state.gov/secretary/rm/2011/02/156619.htm (accessed April 26, 2012).
3. Obama, Executive Order.
4. The authors are grateful to Stewart Baker for sharing this insight.