

**THE UNINTENDED CONSEQUENCES OF U.S. EXPORT
RESTRICTIONS ON SOFTWARE AND ONLINE SERVICES
FOR AMERICAN FOREIGN POLICY AND HUMAN RIGHTS**

*Lee Baker**

TABLE OF CONTENTS

I. INTRODUCTION.....	537
II. THE LANDSCAPE OF U.S. TRADE SANCTIONS	541
A. <i>Policy Rationales</i>	541
B. <i>Regulatory Framework</i>	543
III. A CRITICAL ANALYSIS OF SANCTIONS	546
A. <i>Sanctions Are Ineffective and May Have Unintended Consequences</i>	549
B. <i>Sanctions Impose Suffering on Innocent Citizens of the Target Country</i>	551
IV. REGULATORY CONFUSION PREVENTS THE LEGAL EXPORT OF ICT.....	552
V. ICT ARE USEFUL TOOLS FOR THE PROMOTION OF HUMAN RIGHTS	555
A. <i>Online Organization and SMS — Ukraine’s Orange Revolution</i>	556
B. <i>Circumvention Tools — Breaching the Great Firewall of China</i>	558
C. <i>Social Networks, Twitter, and Modern ICT — Election Protests in Moldova and Iran</i>	560
VI. CONCLUSION	563

I. INTRODUCTION

On June 12, 2009, Iran held a presidential election that many believed would be a close race between Mahmoud Ahmadinejad, the incumbent, and Mir Hossein Mousavi, a reformist and former prime

* Harvard Law School, Candidate for J.D., 2011; B.Sc., Queen’s University, 2008. The author would like to thank Christopher Bavitz, Ethan Zuckerman, and other members of the Berkman Center for Internet & Society for bringing this issue to his attention and describing many of the examples of regulatory confusion discussed in Part IV. He would also like to thank Joshua Gruenspecht and the student writing team of the *Harvard Journal of Law & Technology* for their insightful comments on early drafts.

minister.¹ The result, however, was a landslide for Ahmadinejad that was quickly dismissed as a fraud by both the Iranian opposition and members of the Western media.² Enraged, opposition supporters took to the streets in what has been described as the “biggest anti-government protests since the 1979 Islamic revolution.”³ As these initial protests subsided and the Guardian Council refused to annul the results, Mousavi called on his supporters to continue “legal” protests.⁴ Heeding his words, the opposition staged new protests in August,⁵ September,⁶ November,⁷ December,⁸ and February.⁹

1. See, e.g., Colin Freeman, *Iran Election: ‘Unprecedented’ Turnout Boosts Challenge to Mahmoud Ahmadinejad*, DAILY TELEGRAPH (London), June 12, 2009, <http://www.telegraph.co.uk/news/worldnews/middleeast/iran/5515813/Iran-election-unprecedented-turnout-boosts-challenge-to-Mahmoud-Ahmadinejad.html>; Peter Goodspeed, *Election Leaves Iran Polarized*, NAT’L POST (Toronto), June 13, 2009, <http://www.nationalpost.com/m/story.html?id=1693833>.

2. See Glenn Kessler & Jon Cohen, *Signs of Fraud Abound, but Not Hard Evidence*, WASH. POST, June 16, 2009, at A1, available at <http://www.washingtonpost.com/wp-dyn/content/article/2009/06/15/AR2009061503235.html>; Maziar Bahari, *‘It’s a Coup d’Etat’*, NEWSWEEK, June 13, 2009, <http://www.newsweek.com/id/201956>; Colin Freeman, *Iran Elections: Revolt as Crowds Protest at Mahmoud Ahmadinejad’s ‘Rigged’ Victory*, DAILY TELEGRAPH (London), June 13, 2009, <http://www.telegraph.co.uk/news/worldnews/middleeast/iran/5526721/Iran-elections-revolt-as-crowds-protest-at-Mahmoud-Ahmadinejad-rigged-victory.html>.

3. Zahra Hosseini & Hossein Jaseb, *Khamenei Vows No Retreat on Iran Election Result*, REUTERS, June 24, 2009, <http://www.reuters.com/article/idUSTRE55F54520090624>.

4. See Damien McElroy, *Iran Election: G8 Foreign Ministers Condemn Violence*, DAILY TELEGRAPH (London), June 26, 2009, <http://www.telegraph.co.uk/news/worldnews/middleeast/iran/5648281/Iran-election-G8-foreign-ministers-condemn-violence.html>.

5. *New Opposition Protest in Tehran*, BBC NEWS, Aug. 6, 2009, http://news.bbc.co.uk/2/hi/middle_east/8188830.stm (describing protests held as Ahmadinejad was sworn in as president).

6. See Jim Muir, *Clashes Show Unresolved Iran Crisis*, BBC NEWS, Sept. 18, 2009, http://news.bbc.co.uk/2/hi/middle_east/8264075.stm (describing protests held on Qud’s Day).

7. See Andrew Lee Butters, *In Iran, New Protests, but an Ever Harder Line*, TIME.COM, Nov. 4, 2009, <http://www.time.com/time/world/article/0,8599,1934563,00.html> (describing protests held on thirtieth anniversary of the takeover of the U.S. embassy in Tehran).

8. See *Clashes at Montazeri Ceremony, Iran Opposition Says*, BBC NEWS, Dec. 23, 2009, http://news.bbc.co.uk/2/hi/middle_east/8427806.stm (describing protests held during a memorial service for Grand Ayatollah Hoseyn Ali Montazeri); *Iran Opposition Figures Arrested After Protests*, BBC NEWS, Dec. 28, 2009, http://news.bbc.co.uk/2/hi/middle_east/8432297.stm (describing protests held during the Day of Ashura); *Iran Opposition Protesters Clash with Security Forces*, BBC NEWS, Dec. 7, 2009, http://news.bbc.co.uk/2/hi/middle_east/8398615.stm (describing protests held on Student Day). BBC News has assembled a webpage featuring their most recent reports and analyses regarding the “Iran Crisis.” BBC News, Iran Crisis, http://news.bbc.co.uk/2/hi/in_depth/middle_east/2009/iran/default.stm (last visited May 8, 2010).

9. See *Despite Harsh Threats, Iran Protesters Show Their Strength*, CHRISTIAN SCI. MONITOR, Feb. 11, 2010, <http://www.csmonitor.com/Commentary/the-monitors-view/2010/0211/Despite-harsh-threats-Iran-protesters-show-their-strength> (describing opposition protests held on the thirty-first anniversary of the Iranian revolution). See generally BBC News, Iran Crisis, http://news.bbc.co.uk/2/hi/in_depth/middle_east/2009/iran/default.stm (last visited May 8, 2010). A timeline of the protests is also available on Wikipedia. See Wikipedia, *Timeline of the 2009 Iranian Election Protests*,

These protestors are unique not only in their uncharacteristic boldness, but also in the degree to which they have made use of new online communications platforms to organize and share information, both amongst themselves and with the outside world. Twitter in particular has emerged as a technological “white knight,” lauded by the media as a source of information on the protest movement.¹⁰ It was seen as so instrumental to the Iranian protestors that the State Department asked the company to delay a network upgrade so that service would not be interrupted during waking hours in Tehran.¹¹ Given the significance of the protests, it is perhaps understandable that an awkward fact was overlooked: at the time, providing Twitter to users in Iran was illegal.¹²

The U.S. is the world leader in unilateral trade sanctions.¹³ Despite a great deal of scholarship from a wide variety of disciplines condemning such measures as ineffective and harmful,¹⁴ the U.S. maintains a complex system of sanctions programs.¹⁵ Regulations

http://en.wikipedia.org/wiki/Timeline_of_the_2009_Iranian_election_protests (as of May 8, 2010, 08:52 GMT).

10. See, e.g., David Batty, *Iran: Twitter Becomes Focal Point of Protests*, GUARDIAN NEWS BLOG (London), Dec. 28, 2009, <http://www.guardian.co.uk/world/blog/2009/dec/28/iran-protests-twitter>; *Current Twitter Trends: ‘Lose My Number’, ‘Iran Election’*, INDEPENDENT (London), Nov. 4, 2009, <http://www.independent.co.uk/news/media/current-twitter-trends-lose-my-number-iran-election-1814568.html>; *Iranian Protesters Cling to Twitter as Key Lifeline Amid Crackdown*, FOX NEWS, June 18, 2009, <http://www.foxnews.com/story/0,2933,527068,00.html>.

11. See Mike Musgrove, *Twitter Is a Player in Iran’s Drama*, WASH. POST, June 17, 2009, at A10, available at <http://www.washingtonpost.com/wp-dyn/content/article/2009/06/16/AR2009061603391.html>; Lev Grossman, *Iran Protests: Twitter, the Medium of the Movement*, TIME.COM, June 17, 2009, <http://www.time.com/time/world/article/0,8599,1905125,00.html>.

12. See Prohibited Exportation, Reexportation, Sale or Supply of Goods, Technology, or Services to Iran, 31 C.F.R. § 560.204 (2009) (prohibiting “the exportation, reexportation, sale, or supply, directly or indirectly, from the United States, or by a United States person, wherever located, of any goods, technology, or services to Iran”); Amendments to the Cuban Assets Control Regulations, Sudanese Sanctions Regulations, and Iranian Transactions Regulations, 75 Fed. Reg. 10,997, 10,998 (Mar. 10, 2010) (codified at 31 C.F.R. §§ 515.578, 538.533, 560.540) (“[T]he exportation of [certain services and software incident to the exchange of personal communications over the Internet] from the United States or by a United States person, wherever located, to Sudan or Iran is prohibited.”); see also Danny O’Brien, *Benefits Without Borders for Tweepers in Tehran*, IRISH TIMES (Dublin), June 19, 2009, at 6, available at <http://www.irishtimes.com/newspaper/finance/2009/0619/1224249108131.html> (noting that U.S. attorneys specializing in export regulations have recommended that services such as Twitter and Facebook not offer their services in countries subject to U.S. sanctions); Posting of Clif Burns to ExportLawBlog, *Will the Revolution Be Twitterized?*, <http://www.exportlawblog.com/archives/521> (June 17, 2009, 11:08 EST).

13. Sarah H. Cleveland, *Norm Internalization and U.S. Economic Sanctions*, 26 YALE J. INT’L L. 1, 4 (2001); see also GARY CLYDE HUFBAUER ET AL., *ECONOMIC SANCTIONS RECONSIDERED* 17 (3d ed. 2007) (noting that the U.S. deployed sanctions, alone or with allies, 109 times since World War I and that the next most prolific employer of sanctions, the United Nations, deployed them only twenty times during the same time period).

14. See *infra* Part III.

15. See *infra* Part II.

administered by the Office of Foreign Assets Control (“OFAC”) in the Department of the Treasury targeting Iran, Cuba, and certain areas of Sudan are particularly egregious, often effectively prohibiting all exports of any goods, technologies, or services.¹⁶

Confronted with the example provided by the protesters’ use of U.S.-developed online communications platforms in post-election Iran, however, the U.S. government has recognized that prohibiting citizens in autocratic regimes from accessing such technology is inimical to the foreign policy objectives that animate the U.S. sanctions regime. In light of this revelation, the Department of the Treasury has recently amended the Cuban, Sudanese, and Iranian sanctions programs to authorize the export of publicly-available mass market online services “incident to the exchange of personal communications over the Internet” without a license.¹⁷

While these measures represent a good first step in reforming the sanctions programs affecting information and communication technologies (“ICT”), they do not go far enough. The “Twitter Revolution” in Iran may have focused government attention on the pernicious effects of export controls on ICT in that country and spurred the Department of the Treasury to address this issue, but similar effects may still be present elsewhere due to export controls maintained by the Department of Commerce on mass market software.¹⁸ Moreover, these recent OFAC amendments do not authorize the export of software or services for use in circumventing the Internet censorship imposed by many autocratic regimes.¹⁹ This Note argues that all U.S. sanctions programs should include exceptions for the export of software and online services that facilitate communication and information-exchange or permit circumvention of Internet censorship to citizens of sanctioned nations. Furthermore, sanctions regulations must be clarified, especially with regard to software containing en-

16. See 31 C.F.R. § 515.201 (2009) (Cuba); 31 C.F.R. §§ 538.204–538.210 (2009) (Sudan); 31 C.F.R. § 560.204 (2009) (Iran). Sanctions targeting Cuba are administered by both OFAC and the Bureau of Industry and Security in the U.S. Department of Commerce, with the former controlling the export of services and the latter controlling the export of goods and technologies. See Amendments to the Cuban Assets Control Regulations, Sudanese Sanctions Regulations, and Iranian Transactions Regulations, 75 Fed. Reg. 10,997, 10,998, 10,999 (Mar. 10, 2010) (codified at 31 C.F.R. §§ 515.578, 538.533, 560.540). For more information on sanctions targeting Cuba, see *infra* Part III.B.

17. Amendments to the Cuban Assets Control Regulations, Sudanese Sanctions Regulations, and Iranian Transactions Regulations, 75 Fed. Reg. 10,997, 10,998 (Mar. 10, 2010) (codified at 31 C.F.R. §§ 515.578, 538.533, 560.540). These amendments also explicitly authorize the export of certain free, publicly-available software necessary to enable these services to Iran and Sudan. *Id.* The export of software to Cuba is controlled by the Department of Commerce. See *infra* Part III.B.

18. See *infra* note 48 and accompanying text.

19. See Nate Anderson, *US Eases Restrictions on Web Services Exports to Iran, Cuba*, ARS TECHNICA, Mar. 10, 2010, <http://arstechnica.com/tech-policy/news/2010/03/us-eases-restrictions-on-web-services-exports-to-iran-cuba.ars>. On the benefit of circumvention software for dissidents and human rights activists, see *infra* Part V.B.

ryption. The complexity of the current regulations and the high penalties for violations disincentivize U.S. companies from offering their services to citizens of certain countries even when doing so does not violate any export controls.²⁰ Simplifying the sanctions programs will allow U.S. companies to provide their products and services to dissidents, human rights activists, and ordinary citizens without fear of liability.

Part II outlines the policy rationales and regulatory framework for the relevant U.S. trade sanctions regulations. Part III briefly reviews the literature on trade sanctions, highlighting common criticisms that are particularly pertinent to the context of ICT. Part IV describes situations where the lack of clarity in U.S. regulations has dissuaded companies from providing their services to dissidents, human rights groups, and other citizens in countries under limited sanctions. Part V describes the benefits of ICT for pro-democracy and human rights activists through a series of case studies. Part VI concludes with recommendations for changes to current sanctions regulations.

II. THE LANDSCAPE OF U.S. TRADE SANCTIONS

A. Policy Rationales

Trade sanction programs may be described using two metrics: the policies animating them and the particular means by which those policies are implemented. The policies may be specific and well-defined or broad and ambiguous; they may remain constant throughout the sanctions episode or change over time to reflect new circumstances and the evolving relationship between the sending and target countries.²¹

The U.S. administers a wide variety of sanctions programs guided by myriad underlying policy rationales. Such policies have included settling expropriation claims;²² punishing a regime for supporting terrorism, violating human rights, or other wrongdoing;²³ and blocking

20. See *infra* Part IV.

21. See MICHAEL P. MALLOY, UNITED STATES ECONOMIC SANCTIONS: THEORY AND PRACTICE 343–44 (2001) (discussing the evolving policies underlying U.S. sanctions against Vietnam). The policies underlying the sanctions against Cuba have also shifted over the past fifty years, from punishment for the expropriation of property held by U.S. citizens and companies, to containing communism, to the protection of human rights and aiding a transition to democracy. See Alberto R. Coll, *Harming Human Rights in the Name of Promoting Them: The Case of the Cuban Embargo*, 12 UCLA J. INT'L L. & FOREIGN AFF. 199, 202–27 (2007); see also Cuban Democracy Act, 22 U.S.C. § 6002 (2006) (describing the policy motivating the Act). For a comprehensive overview of the history of U.S. economic sanctions, see MALLOY, *supra*, at 31–142.

22. HUFBAUER ET AL., *supra* note 13, at 14.

23. See Cleveland, *supra* note 13, at 5 (citing the punishment of human rights violations as one purpose behind labor rights sanctions); Harry Wolff, Note, *Unilateral Economic Sanctions: Necessary Foreign Policy Tool or Ineffective Hindrance on American Busi-*

the export of sensitive technologies for national security reasons.²⁴ Sanctions were also employed during the Cold War to curb the spread of communism.²⁵ Although not an explicitly stated goal of sanctions, they may also serve an important role in the definition, refinement, and internalization of international human rights norms, especially in recalcitrant target countries.²⁶

In the paradigmatic sanctions episode, the sending nation imposes sanctions to induce the target nation to curtail behavior that it finds objectionable, under the theory that the economic loss engendered by these measures will foster discontent among the target population, which will then either overthrow the target government or pressure it into adopting the changes desired by the sending nation.²⁷ Sanctions may also be implemented to deter non-target nations from pursuing policies or behaviors similar to those pursued by the target nation.²⁸ The extent to which unilateral sanctions may have the desired effect on the target nation has been severely criticized, however, especially in cases where the target government is authoritarian or the target population otherwise lacks the means to challenge its government.²⁹ There may also be unstated political reasons for the imposition of sanctions. Politicians may see the imposition of sanctions as an attractive and relatively low-cost way to satisfy domestic pressure to “do something” in response to objectionable behavior by the target nation.³⁰ Similarly, sanctions may be used to signal, to both global and domestic audiences, the sending nation’s opposition to the target nation’s behaviors or policies.³¹ Such political considerations may interact with the policy rationales noted above to shape the final form of the sanctions regulations.

nesses?, 6 HOUS. BUS. & TAX L.J. 329, 339 (2006) (noting that trade sanctions were enacted against Libya in response to its support for international terrorism directed at U.S. interests in the Middle East).

24. Philip M. Nichols, *Using Sociological Theories of Isomorphism To Evaluate the Possibility of Regime Change Through Trade Sanctions*, 30 U. PA. J. INT’L L. 753, 758–59 (2009).

25. Wolff, *supra* note 23, at 335–37.

26. *See* Cleveland, *supra* note 13, at 6.

27. Thihan Myo Nyun, *Feeling Good or Doing Good: Inefficacy of the U.S. Unilateral Sanctions Against the Military Government of Burma/Myanmar*, 7 WASH. U. GLOBAL STUD. L. REV. 455, 467 (2008); *see also* HUFBAUER ET AL., *supra* note 13, at 13–14 (providing examples of successful and unsuccessful attempts at promoting regime change through the use of sanctions). Regime change, brought about through the mechanism described, is one of the explicit policy goals of U.S. sanctions against Cuba. *See* Cuban Liberty and Democratic Solidarity (Libertad) Act of 1996, 22 U.S.C. §§ 6021–91 (2006).

28. *See* Adam Smith, *A High Price To Pay: The Costs of the U.S. Economic Sanctions Policy and the Need for Process Oriented Reform*, 4 UCLA J. INT’L L. & FOREIGN AFF. 325, 330–31 (2000).

29. *See* Myo Nyun, *supra* note 27, at 467–68.

30. *See id.* at 458.

31. *See* HUFBAUER ET AL., *supra* note 13, at 5–6; MALLOY, *supra* note 21, at 20 (describing sanctions with “communicative” objectives).

B. Regulatory Framework

Table 1: Agencies and Regulations Involved in Export Controls	
BIS	Bureau of Industry and Security, U.S. Department of Commerce; administers the EAR
EAR	Export Administration Regulations; export control regulations administered by BIS
OFAC	Office of Foreign Assets Control, U.S. Department of the Treasury; administers country-specific controls and the SDN list
SDN list	Specially Designated Nationals list; a list of entities with whom U.S. entities may not transact, administered by OFAC

The U.S. sanctions regime is a fragmented and complicated system. As of 2003, more than five agencies enforced a variety of export controls pursuant to over forty statutes.³² Within the context of ICT, however, there are two agencies whose sanctions programs are most pertinent: the Bureau of Industry and Security (“BIS”) in the Department of Commerce and the Office of Foreign Assets Control (“OFAC”) in the Department of the Treasury.³³ BIS and OFAC sanctions are generally administered under the Trading with the Enemy Act (“TWEA”) and the International Emergency Economic Powers Act,³⁴ although specific OFAC sanctions have been supplemented with additional statutes.³⁵

BIS administers far-reaching export controls in order to further its mission of “[a]dvanc[ing] U.S. national security, foreign policy, and

32. Christopher F. Corr, *The Wall Still Stands! Complying with Export Controls on Technology Transfers in the Post-Cold War, Post-9/11 Era*, 25 HOUS. J. INT’L L. 441, 445 (2003).

33. For detailed explanations of BIS and OFAC export controls, especially with regard to software and technology, see James E. Bartlett III et al., *Export Controls and Economic Sanctions*, 43 INT’L LAW. 311 (2009); Lillian V. Blageff, *Overview of U.S. Sanctions and Embargoes Programs, Including 2006 Update*, INT’L HR J., Summer 2007; Corr, *supra* note 32; and Benjamin H. Flowe, Jr., *Exporting Technology and Software, Particularly Encryption*, 910 PLI/COMM 279 (2008).

34. Blageff, *supra* note 33, at § II.A.

35. See, e.g., Cuban Democracy Act, 22 U.S.C. § 6001 *et seq.* (2006); Cuban Liberty and Democratic Solidarity (Libertad) Act, 22 U.S.C. §§ 6021–91 (2006); Darfur Peace and Accountability Act of 2006, Pub. L. No. 109-344 (2006); Iran and Libya Sanctions Act of 1996, H.R. 3107, 111th Cong. (2006) (renamed the Iran Sanctions Act in 2006).

economic objectives by ensuring an effective export control and treaty compliance system and promoting continued U.S. strategic technology leadership.”³⁶ It is responsible for implementing and enforcing the Export Administration Regulations (“EAR”), a set of relatively complex regulations that control the export and re-export of so-called “dual-use”³⁷ commodities, software, and technology by U.S. entities.³⁸ Depending on the nature of the product to be exported, the country or end-user to which the product is being exported, and the product’s intended end-use, BIS authorization may be required prior to export.³⁹ Destination countries are sorted into “country groups” under the EAR, with those in group E:1 — currently Iran, Cuba, North Korea, Syria, and Sudan — subject to the strictest export restrictions.⁴⁰ BIS also publishes lists of individuals and entities that have been denied export privileges, as well as an unverified list and an entity list. The involvement in a transaction of an individual on the unverified list constitutes a “Red Flag” requiring further due diligence on the part of the exporter, while involvement of a party on the entity list may trigger licensing requirements under the EAR.⁴¹

In contrast to the EAR’s wide-ranging export controls, OFAC programs are targeted at specific countries, geographic regions, or types of goods.⁴² Within each of the country-specific sanctions programs, however, the scope of the controlled activities and restricted products is generally much broader than under the EAR. For example, the “exportation, reexportation, sale, or supply . . . of *any* goods, technology, or services to Iran,” barring certain closely circumscribed exemptions, is prohibited without an OFAC license.⁴³ OFAC also

36. Bureau of Industry & Security, U.S. Department of Commerce, BIS Mission Statement, <http://www.bis.doc.gov/about/mission.htm> (last visited May 8, 2010).

37. 15 C.F.R. § 730.3 (2009) (defining dual-use items as generally items that have both civilian and military uses).

38. Export Administration Regulations, 15 C.F.R. ch. VII, subch. C.

39. *See* 15 C.F.R. §§ 744.1–20 (2009).

40. *See* Country Groups, 15 C.F.R. § 740, Supplement No. 1 (2009); Embargoes & Other Special Controls, 15 C.F.R. § 746 (2009) (outlining special restrictions against embargoed nations). Cuba and Iran are subject to the strictest restrictions, with OFAC and/or BIS authorization required for any export to those countries. *See* 15 C.F.R. §§ 746.1, 746.2, 746.7 (2009).

41. *See* Bureau of Industry & Security, U.S. Department of Commerce, Lists to Check, <http://www.bis.doc.gov/complianceand enforcement/liststocheck.htm> (last visited May 8, 2009).

42. *See* Office of Foreign Assets Control, U.S. Treasury, Sanctions Program Summaries, <http://www.treas.gov/offices/enforcement/ofac/programs> (last visited May 8, 2009).

43. Prohibited Exportation, Reexportation, Sale or Supply of Goods, Technology, or Services to Iran, 31 C.F.R. § 560.204 (2009) (emphasis added); Exempt Transactions, 31 C.F.R. § 560.210 (2009). Similarly broad restrictions are imposed against Cuba and certain parts of Sudan. *See supra* note 16 and accompanying text. With respect to exports to Cuba, OFAC has licensed these transactions insofar as they are regulated under the EAR. *See infra* note 46 and accompanying text. OFAC has imposed more targeted sanctions, limited to specific types of goods or end-users, against North Korea, Syria, other parts of Sudan, Bela-

maintains a list of Specially Designated Nationals (“SDN”), with whom U.S. entities may not transact.⁴⁴

Given the broad scope of the EAR, it is inevitable that they will overlap with OFAC regulations for certain transactions. Items that are “exclusively controlled for export or reexport” by OFAC and certain other agencies, however, are not subject to the EAR,⁴⁵ while OFAC automatically licenses transactions “ordinarily incident” to the export of U.S.-origin goods to Cuba that are authorized under the EAR.⁴⁶ Despite these provisions, BIS has explicitly noted that authorization is required from both agencies for exports to certain regions jointly covered by the EAR and OFAC regulations.⁴⁷

Although the EAR contain provisions specifically addressing software, most OFAC regulations do not, and neither clearly delineates rules for providers of online services based in the U.S. The EAR only apply to certain types of software; so-called “mass market” software may be exported without a license to most countries,⁴⁸ while certain publicly available software is exempt from the EAR entirely.⁴⁹

rus, Burma/Myanmar, Côte d’Ivoire, the Democratic Republic of the Congo, Lebanon, and Zimbabwe. See Office of Foreign Assets Control, *supra* note 42.

44. The SDN list contains “individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries” and “individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific.” Office of Foreign Assets Control, U.S. Treasury, Frequently Asked Questions and Answers, “What is an SDN?”, <http://www.ustreas.gov/offices/enforcement/ofac/faq/answer.shtml#17> (last visited May 8, 2009). The SDN list may be found at <http://www.treas.gov/offices/enforcement/ofac/sdn> (last visited May 8, 2009).

45. Items Subject to the EAR, 15 C.F.R. § 734.3(b)(1) (2009).

46. Transactions Incident to Exportations From the United States and Reexportations of 100% U.S.-Origin Items to Cuba; Negotiation of Executory Contracts, 31 C.F.R. § 515.533 (2010); see also Amendments to the Cuban Assets Control Regulations, Sudanese Sanctions Regulations, and Iranian Transactions Regulations, 75 Fed. Reg. 10,997, 10,999 (Mar. 10, 2010) (describing the applicability of 31 C.F.R. § 515.533 to the authorization of certain software exports to Cuba).

47. See, e.g., BUREAU OF INDUSTRY & SECURITY, DEPARTMENT OF COMMERCE, EXPORTS AND REEXPORTS TO SUDAN 1 (2003), <http://www.bis.doc.gov/policiesandregulations/regionalconsiderations/sudan.pdf> (“[E]xporters must seek authorization from both OFAC and BIS for the export and reexport of items subject to the Export Administration Regulations (EAR).”). But see Iran, 15 C.F.R. § 746.7(a)(2) (2009) (“To avoid duplication, exporters or reexporters are not required to seek separate authorization from BIS for an export or reexport subject both to the EAR and to OFAC’s Iranian Transactions Regulations.”). See generally Embargoes & Special Controls, 15 C.F.R. § 746 (2009) (advising exporters to assume that authorization from both OFAC and BIS is required unless otherwise specified in the special controls section of the EAR).

48. Mass market software that is both (a) generally available to the public by being sold from stock, without restrictions, and (b) “[d]esigned for installation by the user without further substantial support by the supplier” is subject to the EAR, but may be exported without a license under License Exception TSU. Technology and Software — Unrestricted (TSU), 15 C.F.R. § 740.13(d) (2009); General Technology and Software Notes, 15 C.F.R. § 774 Supplement No. 2 (2009). This license exception is unavailable for exports to Cuba, Iran, North Korea, Syria, and Sudan. Country Groups, 15 C.F.R. § 740 Supplement No. 1 (2009).

49. Specifically, publicly available software is not subject to the EAR if it has been or will be published, arises during or results from fundamental research, is educational, or is

In contrast, any software downloaded or purchased by a user on the SDN list or in Iran or non-specified areas of Sudan is subject to OFAC controls.⁵⁰ The export of software and technology that incorporates encryption is subject to its own complex regulations within the EAR, due to the special national security concerns implicated by such technology.⁵¹ Most such software and technology is subject to notification and prior review by BIS, even if formal authorization is not required prior to export.⁵² Although services are likely not controlled under the EAR,⁵³ OFAC sanctions apply if the end-user is on the SDN list or is in Iran, Cuba, or non-specified areas of Sudan.⁵⁴ As of March 8, 2010, the export of services “incident to the exchange of personal communications over the Internet” has been authorized by OFAC to citizens of Iran, Sudan, and Cuba, while the export of most free, publicly-available software necessary to enable these services has been further authorized to citizens of Iran and Sudan.⁵⁵ Penalties for violations of either the EAR or OFAC sanctions are severe and may result in civil or criminal fines as well as the imprisonment of company executives.⁵⁶

III. A CRITICAL ANALYSIS OF SANCTIONS

In contrast to the U.S. government’s continued enthusiasm for trade sanctions, most commentators have become increasingly critical of such measures. To the extent that they support trade sanctions at

included in certain patent applications. Items Subject to the EAR, 15 C.F.R. § 734.3(b)(3) (2009). *See generally* Questions and Answers — Technology and Software Subject to the EAR, 15 C.F.R. § 734 Supplement No. 1 (2009).

50. *See supra* notes 43–44 and accompanying text. Certain “Specified Areas” of Sudan are exempt from most of the prohibitions administered by OFAC. *See* Exempt Transactions, 31 C.F.R. § 538.212(g)(1) (2009). The “Specified Areas” include Southern Sudan, Southern Kordofan/Nuba Mountains State, Blue Nile State, Abyei, Darfur, and the Mayo, El Salaam, Wad El Bashir, and Soba camps for internally displaced persons. Specified Areas of Sudan, 31 C.F.R. § 538.320 (2009).

51. *See* Flowe, *supra* note 33, at 308–32.

52. *See* 15 C.F.R. §§ 740.17, 742.15(b) (2009).

53. The EAR regulate only the export of goods, software, and technology. *See* Items Subject to the EAR, 15 C.F.R. § 734.3 (2009).

54. *See* 31 C.F.R. §§ 515.201(b)(1), 515.311 (2009) (Cuba); Prohibited Exportation and Reexportation of Goods, Technology, or Services to Sudan, 31 C.F.R. § 538.205 (2009); Prohibited Exportation, Reexportation, Sale or Supply of Goods, Technology, or Services to Iran, 31 C.F.R. § 560.204 (2009); *supra* note 44 and accompanying text (SDN list).

55. Amendments to the Cuban Assets Control Regulations, Sudanese Sanctions Regulations, and Iranian Transactions Regulations, 75 Fed. Reg. 10,997, 10,998 (Mar. 10, 2010) (codified at 31 C.F.R. §§ 515.578, 538.533, 560.540). This authorization does not extend to transactions where the exporter knows or has reason to know that the services or software are intended for prohibited officials of the Government of Cuba or members of the Cuban Communist Party, the Government of Sudan, or the Government of Iran. *Id.* at 10,999–11,000. The export of software to Cuba is controlled by the EAR. *See supra* note 46 and accompanying text.

56. *See* Corr, *supra* note 32, at 509–14.

all, academic commentators and the international community generally advocate more targeted “smart” sanctions.⁵⁷ Unfortunately, a number of BIS and OFAC sanctions remain “dumb,” broadly covering essentially all exports or interactions with specific nations and their citizens.⁵⁸ While there is some anecdotal evidence suggesting that such broad trade sanctions were instrumental in effecting regime change in Idi Amin’s Uganda, Somoza’s Nicaragua, and apartheid South Africa,⁵⁹ one influential study has found that sanctions imposed globally between 1914 and 1990 were successful only one-third of the time.⁶⁰ U.S. unilateral sanctions since 1970 have been even less successful, achieving their foreign policy goals in only 13% of cases.⁶¹

Given this poor track record and the substantial negative effects of sanctions, discussed *infra*, it is questionable whether the U.S. should maintain its sanctions programs at all. Eliminating the entire regime of U.S. sanctions, however, is both unwise and politically infeasible. Certain targeted programs, such as OFAC’s limits on the proliferation of weapons of mass destruction or the trading of “blood diamonds,”⁶² are both necessary as implementations of international

57. See HUFBAUER ET AL., *supra* note 13, at 138–39; see also KOENRAAD VAN BRABANT, OVERSEAS DEV. INST., CAN SANCTIONS BE SMARTER? THE CURRENT DEBATE 36 (1998).

58. OFAC regulations against Iran, Cuba, and non-specified areas of Sudan, and regulations regarding E:1 countries (Iran, Cuba, Sudan, North Korea, and Syria) under the EAR are examples of such sanctions. OFAC has made a move toward more targeted sanctions in some areas, such as its relaxation of North Korean sanctions in 2000 and 2007, and its targeting of sanctions on Zimbabwe against the Mugabe regime itself. See Foreign Assets Control Regulations, 65 Fed. Reg. 38,165 (June 19, 2000) (amending OFAC Foreign Assets Control Regulations for North Korea); OFFICE OF FOREIGN ASSETS CONTROL, U.S. TREASURY, NORTH KOREA: WHAT YOU NEED TO KNOW ABOUT SANCTIONS (2008), <http://www.treas.gov/offices/enforcement/ofac/programs/nkorea/nkorea.pdf> (explaining recent changes to OFAC regulations regarding North Korea, including the termination of the applicability of the TWEA); OFFICE OF FOREIGN ASSETS CONTROL, U.S. TREASURY, ZIMBABWE: WHAT YOU NEED TO KNOW ABOUT U.S. SANCTIONS (2005), <http://www.treas.gov/offices/enforcement/ofac/programs/zimbabwe/zimb.pdf> (explaining imposition of comprehensive sanctions on specific entities found to be “undermin[ing] democratic institutions and processes in Zimbabwe,” as well as their families and associated entities).

59. See Cleveland, *supra* note 13, at 5.

60. Alan Einisman, *Ineffectiveness at Its Best: Fighting Terrorism with Economic Sanctions*, 9 MINN. J. GLOBAL TRADE 299, 312–13 (2000). During this period, the U.S. imposed or helped impose 70% of the sanctions, but most of these sanctions were unilateral. *Id.* at 313.

61. Meghan McCurdy, Note, *Unilateral Sanctions with a Twist: The Iran and Libya Sanctions Act of 1996*, 13 AM. U. INT’L L. REV. 397, 434 (1997).

62. See Office of Foreign Assets Control, U.S. Treasury, Weapons of Mass Destruction/Non-Proliferation Sanctions, <http://www.treas.gov/offices/enforcement/ofac/programs/wmd/wmd.shtml> (last visited May 8, 2010); Office of Foreign Assets Control, U.S. Treasury, Rough Diamond Trade Sanctions, <http://www.treas.gov/offices/enforcement/ofac/programs/diamonds/diamond.shtml> (last visited May 8, 2010).

agreements⁶³ and good policy. This Note merely argues that overly broad sanctions should be more narrowly tailored to avoid their most egregious negative effects.⁶⁴ Specifically, since export restrictions on ICT cause harm to the target population and hinder the efforts of human rights activists and dissidents, while not significantly impacting the target government itself, they should be eliminated.

Askari et al. have outlined a cogent summary of the major failings of sanctions, which is particularly salient for unilateral measures imposed by the U.S.:

1. Sanctions impose such suffering and deprivation on innocent citizens of other countries that they can end up solidifying the power of authoritarian rulers.
2. Sanctions can be bypassed through reexport from third countries.
3. Loss of exports to target countries imposes significant economic costs on the citizens of sender countries through lost output and jobs.
4. Loss of imports from target countries imposes higher costs on businesses in sender countries and affords fewer choices to consumers.
5. Sanctions can inadvertently inflict damage on third countries.
6. Sanctions rarely cause the target to modify its behavior.⁶⁵

In the context of the ICT that are most valuable to dissidents and human rights activists, many of which are developed by American companies and distributed free of charge online, the most relevant

63. See, e.g., Rough Diamonds Control Regulations, 69 Fed. Reg. 56,936 (Sept. 23, 2004) (codified at 31 C.F.R. § 592) (describing revisions to the Rough Diamonds Control Regulations, which implements the multilateral Kimberley Process Certification Scheme).

64. The Zimbabwean sanctions, which target only those undermining democracy in that country and not the population as a whole, are a model for how regulations may be more narrowly tailored. See *supra* note 58 and accompanying text. Despite this tailoring, the Zimbabwean sanctions still have pernicious effects due to their complexity and ambiguity. See *infra* Part IV. As a result, this Note further argues that U.S. sanctions programs must be clarified to prevent such effects.

65. HOSSEIN G. ASKARI ET AL., ECONOMIC SANCTIONS: EXAMINING THEIR PHILOSOPHY AND EFFICACY 66 (2003). Askari offers a scathing review of U.S. unilateral economic sanctions, finding the philosophy that underpins them to be “flawed in concept and in logic” and reflecting a “hubris, naïvete [sic], or disingenuousness (or all three) in U.S. foreign policy.” *Id.* at 67–76.

criticisms involve the lack of efficacy and unintended consequences of sanctions and sanctions' negative effects on the citizens of the target nation.⁶⁶

A. Sanctions Are Ineffective and May Have Unintended Consequences

It is both simplistic and unrealistic to expect that trade sanctions alone will directly induce regime change.⁶⁷ Each specific sanctions episode is unique, and the success or failure of any given program of sanctions is dependent upon a combination of the characteristics of the sanctions imposed, the end sought to be achieved, and the geopolitical context.⁶⁸ Furthermore, there is some doubt as to whether the economic effectiveness of sanctions can be accurately measured, and the methodology of major efficacy studies has been questioned.⁶⁹ Despite these caveats, "most contemporary analysts agree that unilateral sanctions . . . are ineffective tools in compelling target countries to change their policies."⁷⁰

The logic underlying the paradigmatic sanctions episode, in which economic hardship induces the target population to force their government to change policy, contains major flaws. As described previously, such sanctions cannot have any effect if the target population lacks sufficient power to influence the decision-making of their government.⁷¹ The resilience of the regimes in Burma/Myanmar and Iran in the face of major anti-government protests demonstrates that popular uprisings may be ineffective in promoting regime change. When sanctions are imposed unilaterally, third parties can fill the vacuum created by the sending nation, becoming "black knights" for the target nation.⁷² Thus the economic deprivation caused by U.S. sanctions against Cuba was initially softened by Soviet aid during the Cold

66. These two broad categories incorporate most of the Askari's criticisms of U.S. sanctions. His third criticism is inapposite in the context of ICT, as U.S. technology firms often find profit elusive in developing countries. See *infra* note 112 and accompanying text. Since this Note focuses on U.S. *export* restrictions on ICT, the effects of *import* restrictions outlined in his fourth criticism will not be discussed. Nor is it a particularly strong criticism in the context of software and online services, which do not require components sourced from sanctioned nations. Askari's fifth criticism largely addresses extraterritoriality provisions present in certain sanctions legislation, and is beyond the scope of this Note.

67. Cf. Myo Nyun, *supra* note 27, at 481 ("A blank statement that unilateral sanctions are ineffective tools of foreign policy is overly simplistic and often misleading.").

68. See *id.*; see also ASKARI ET AL., *supra* note 65, at 67.

69. See Richard W. Parker, *The Problem with Scorecards: How (and How Not) To Measure the Cost-Effectiveness of Economic Sanctions*, 21 MICH. J. INT'L L. 235 (2000) (describing methodological flaws in influential studies, such as the one performed by Hufbauer *et al.*).

70. Myo Nyun, *supra* note 27, at 465.

71. See *id.* at 467.

72. See HUFBAUER ET AL., *supra* note 13, at 8.

War, and more recently has been partially offset by highly favorable trade agreements with Venezuela and China.⁷³

Sanctions may be ineffective in another manner, by failing to prevent the target government from accessing controlled goods or reasonable alternatives. As noted above, countries that are not participating in the sanctions episode may act as alternative sources of sanctioned goods. But even where the sending nation is the only source of a particular good or service, a regime will often have access to alternative means of achieving its goals. This is particularly true with respect to the communications and circumvention technologies that are most useful for human rights activists. Many repressive regimes have extensive propaganda networks, and often tightly control their domestic mainstream media.⁷⁴ Autocratic governments do not need Skype, Twitter, social networking sites, or blogs in order to broadcast their message. Nor do they require U.S.-developed tools to circumvent Internet censorship. These tools, however, are essential to dissidents and human rights groups for organizing protests, developing alternative media environments, and accessing censored information.⁷⁵

Moreover, sanctions may have unintended effects that undermine the very policies that are meant to guide them. The economic havoc wreaked by sanctions may retard the emergence of a middle class and the development of civil society, both key elements in the transition to democracy.⁷⁶ They may also have the perverse effect of strengthening the sanctioned regime, which may use sanctions to its advantage, either to foment nationalist sentiment or to serve as a scapegoat for all economic and social hardships suffered by the target population.⁷⁷ The response of the military junta in Burma/Myanmar to the Burmese Freedom and Democracy Act⁷⁸ provides a prime example of these unintended consequences: Nobel laureate Aung San Suu Kyi was placed under house arrest; her National League for Democracy, which had won a 1990 election that was subsequently nullified, was excluded from national conventions; and a moderate member of the junta was removed in favor of a hardliner.⁷⁹ The junta also blamed

73. See CARMELO MESA-LAGO, CUBA TRANSITION PROJECT, THE CUBAN ECONOMY TODAY: SALVATION OR DAMNATION? 8–13 (2005).

74. See, e.g., Burma Country Card, Reporters Without Borders, <http://en.rsf.org/report-burma,53.html?annee=2009> (noting that “the two television and radio channels and the daily newspapers are under direct control of the military junta” while “[t]he privately-owned press is under military censorship”) (last visited May 8, 2010).

75. See *infra* Part V.

76. See Richard N. Haass, *Sanctioning Madness*, FOREIGN AFFS., Nov./Dec. 1997, at 79.

77. See HUFBAUER ET AL., *supra* note 13, at 8 (listing episodes where sanctions unified the target country behind their government).

78. Burmese Freedom & Democracy Act of 2003, Pub. L. No. 108-61, 117 Stat. 864 (2003).

79. See Myo Nyun, *supra* note 27, at 485–86.

U.S. sanctions for economic failures in the country and used them to stoke nationalism.⁸⁰ Such opportunistic use of a sanctions episode is not restricted to the Burmese junta — the Cuban government has also used U.S. sanctions as a cover to continue its own repressive policies and to sideline domestic activists by portraying them as U.S. lackeys.⁸¹

*B. Sanctions Impose Suffering on
Innocent Citizens of the Target Country*

The paradigmatic sanctions episode is intended to cause economic loss to the target nation. This invariably imposes hardships on innocent civilians living there. While the most readily apparent effect of export controls is to prevent members of the target population from acquiring essential goods, broad sanctions programs may also have severe secondary effects that can exacerbate existing humanitarian crises or beget new ones.⁸² Even when humanitarian exceptions allow the export of essentials such as food, medicine, and other aid items, distribution may be impossible due to the unavailability or high cost of fuel or the deterioration of public infrastructure, including communications infrastructure.⁸³ Economic loss may also harm the target population by causing its government to redistribute funds to the military and other institutions that support the regime to the detriment of public institutions such as health care and education.⁸⁴

These human costs of sanctions are demonstrated most clearly by the situation in Cuba, which is subject to one of the most comprehensive U.S. sanctions programs. When the Soviet Union fell, Cuba lost its primary source of aid and, without access to U.S. exports, plunged into a severe food shortage that caused widespread nutritional deficiencies and disease.⁸⁵ Although the Cuban sanctions regulations include limited exemptions for medication and medical supplies, the arduous licensing process dissuades U.S. firms from exporting these products.⁸⁶ Public education also suffers due to U.S. sanctions. Cuban schools must pay higher prices to obtain supplies that do not contain

80. *See id.*

81. *See Coll, supra note 21, at 253 n.366, 253–54.*

82. *See Myo Nyun, supra note 27, at 507–08.*

83. *See Smith, supra note 28, at 346–50; see also VAN BRABANT, supra note 57, at 25–28 (describing the inadequacy of humanitarian exemptions from sanctions regimes to prevent suffering in targeted countries).*

84. *See Myo Nyun, supra note 27, at 494–96.*

85. *See Coll, supra note 21, 238–41.*

86. *See id.* at 241–43. In a similar manner, regulatory confusion with regard to export controls has led some technology companies to refuse to offer their ICT to foreign nationals living in sanctioned countries, even when it would be legal for them to do so. *See infra* Part IV.

any components made in the U.S.⁸⁷ Universities unable to access sub-aquatic fiber-optic cables to connect to the Internet must instead pay for a costly satellite connection.⁸⁸ Tight visa restrictions prevent Cuban scientists and other academics from attending conferences in the U.S., thereby limiting information exchange and scientific cooperation.⁸⁹ Despite these hardships endured by the Cuban people, the sanctions programs have failed in their primary goal: to topple the Castro regime and promote the transition to a democratic government.⁹⁰

Restrictions on the export of ICT are not likely to result in mass starvation. But they may still cause harm to citizens in sanctioned countries, as demonstrated by the increased cost of Internet access for Cuban universities.⁹¹ Given that communications networks built upon even rudimentary ICT can bring substantial gains in the field of public health, restricting the export of U.S. technology to sanctioned nations may even cost lives.⁹² Such restrictions may also stifle the development of alternative media environments and prevent citizens from accessing censored information, thus impoverishing the public's knowledge and increasing the efficacy of government propaganda.⁹³ Finally, by reducing the ability of human rights activists to communicate effectively with the global community, trade sanctions on ICT may exacerbate human rights abuses by removing the risk of global opprobrium.⁹⁴

IV. REGULATORY CONFUSION PREVENTS THE LEGAL EXPORT OF ICT

While much of the research regarding the operation of U.S. software and technology companies in non-democratic countries has focused on their compliance with requests from those governments to censor their offerings or spy on their users,⁹⁵ much less has been writ-

87. See Coll, *supra* note 21, at 244.

88. See *id.* at 244–45.

89. See *id.* at 245–47.

90. See Cuban Democracy Act, 22 U.S.C. § 6002 (2006) (describing the policy motivating the Act).

91. See *supra* note 88 and accompanying text.

92. SEE JEFFREY JAMES, INFORMATION TECHNOLOGY AND DEVELOPMENT: A NEW PARADIGM FOR DELIVERING THE INTERNET TO RURAL AREAS IN DEVELOPING COUNTRIES 72–75 (2004) (discussing some benefits of U.S. ICT in the health sector in developing nations).

93. See *infra* Part V.A. (discussing the value of alternative media environments for civil society and the preservation of political rights); *infra* Part V.B. (discussing the value of circumvention technologies for the same).

94. Cf. *infra* notes 116–18 and accompanying text, describing how Zapatista rebels used ICT to focus global attention on their military standoff with the Mexican government to avoid being quietly wiped out.

95. For example, in 2008, it was discovered that the Chinese version of Skype was filtering messages based on a government-provided list of banned keywords and monitoring its

ten about their refusal to offer their services in certain countries for fear of violating U.S. sanctions regulations. A number of recent episodes in which risk-averse technology companies have proactively refused to transact with users in nations subject to U.S. sanctions, even when such activity is perfectly legal, suggest that this problem may be disturbingly common.

In 2009 Bluehost, a major webhosting company, was involved in several such incidents. Citing OFAC sanctions, it suspended a number of Persian-language blogs in various countries,⁹⁶ cut service to sites in Zimbabwe,⁹⁷ and even shut down the blog of the Washington, D.C. chapter of the Belarussian American Association.⁹⁸ The disruption of service to Zimbabwean blogs provides a particularly salient demonstration of how the structure of U.S. sanctions regulations may work against their own aims. Zimbabwe is not subject to broad U.S. sanctions; instead, OFAC regulations are targeted at specific individuals and entities, including senior officials of Robert Mugabe's government, individuals who have attempted to "undermine Zimbabwe's democratic processes or institutions," and those who have participated in "human rights abuses related to political repression."⁹⁹ Some of the blogs that Bluehost forced offline, such as Kubatana, Women of Zimbabwe Arise, and Island Hospice and Bereavement Service, are run by human rights NGOs and activist organizations that are frequent critics of the Mugabe government.¹⁰⁰ These communities should be natural allies of the U.S. in its attempts to curb human rights abuses and promote democratic institutions in Zimbabwe; instead, they were silenced

users' voice calls. See NART VILLENEUVE, INFORMATION WARFARE MONITOR, BREACHING TRUST: AN ANALYSIS OF SURVEILLANCE AND SECURITY PRACTICES ON CHINA'S TOM-SKYPE PLATFORM (2008), available at <http://www.nartv.org/mirror/breachingtrust.pdf>; STEPHANIE WANG, OPENNET INITIATIVE, INTERNET FILTERING IN CHINA 15-16 (2009), available at <http://opennet.net/research/profiles/china>; Ben Charny, *Chinese Partner Censors Skype Text Messages*, PC MAG., Apr. 20, 2006, <http://www.pcmag.com/article2/0,2817,1951637,00.asp>. Yahoo! was also the subject of global opprobrium when its willingness to provide subscriber information to the Chinese authorities led to the arrest of Shi Tao, a journalist who was sentenced to ten years in prison for "divulging state secrets abroad." See *Information Supplied by Yahoo! Helped Journalist Shi Tao Get 10 Years in Prison*, REPORTERS WITHOUT BORDERS, Sept. 6, 2005, http://en.rsf.org/spip.php?page=article&id_article=14884.

96. See Kamangir, *Persian Blogs on Bluehost Will be Going Down*, <http://kamangir.net/2009/02/23/persian-blogs-on-bluehost-will-be-going-down/> (Feb. 23, 2009, 7:04 EST).

97. See Kubatana.net, *Curve Balls and Blue Beards*, <http://www.kubatanablogs.net/kubatanana/?p=1261> (Feb. 17, 2009, 10:28 EST); *My Heart's in Accra, Bluehost Censors Zimbabwean Blogger*, <http://www.ethanzuckerman.com/blog/2009/02/13/bluehost-censors-zimbabwean-bloggers> (Feb. 13, 2009, 17:54 EST).

98. See Evgeny Morozov, *Do-It-Yourself Censorship*, NEWSWEEK, Mar. 16, 2009, at 10, available at <http://www.newsweek.com/id/188184>.

99. Exec. Order No. 13,469 § 1(a), 73 Fed. Reg. 43,841 (July 25, 2008).

100. See Ethan Zuckerman, *Intermediary Censorship*, in ACCESS CONTROLLED: THE SHAPING OF POWER, RIGHTS, AND RULE IN CYBERSPACE 74-76 (Ronald Deibert et al. eds., 2010).

as a result of U.S. sanctions. Efforts by the cofounder of Kubatana to explain the scope of OFAC regulations to Bluehost and demonstrate that the blogs and their operators were not targets of the Zimbabwean sanctions fell on deaf ears.¹⁰¹ Although Bluehost eventually offered to reinstate the accounts after the U.S. Treasury Department notified the company that the Zimbabwean website operators were not subject to sanctions, Kubatana had moved to a new webhosting service in the interim.¹⁰² While Bluehost received the lion's share of public attention, other providers of webhosting services have also suspended user accounts in countries subject to U.S. sanctions.¹⁰³

Webhosting service providers are not the only companies that have refused service to users based on flawed interpretations of OFAC regulations. Last year, the business-oriented social networking site LinkedIn began deleting Syrian accounts and prohibiting users in Syria, Iran, Cuba, North Korea, and Sudan from registering.¹⁰⁴ Although OFAC regulations prohibit the provision of online services to Iran, Cuba, and non-specified areas of Sudan, users in Syria and North Korea are not subject to such restrictions.¹⁰⁵ As news of the ban began to spread on Twitter and blogs, including prominent sites like the Huffington Post, LinkedIn quickly restored access to Syrian users, citing "human error [which] led to over compliance with respect to export controls."¹⁰⁶ It is unclear whether access has been restored to users in Iran, Cuba, North Korea, or Sudan.¹⁰⁷ Instant messenger clients have been affected as well, with Microsoft refusing to offer its Windows Live Messenger application to users in Iran, Cuba, Syria, Sudan, and North Korea, also purportedly to comply with OFAC sanctions.¹⁰⁸

101. See Kubatana.net, *supra* note 97.

102. See My Heart's in Accra, *supra* note 97.

103. See Morozov, *supra* note 98.

104. See Jillian York, *LinkedIn Alienates Syrian Users: Why Now?*, THE HUFFINGTON POST, Apr. 20, 2009, http://www.huffingtonpost.com/jillian-york/linkedin-alienates-syrian_b_188629.html; Daily Clarity, *Foreign Bloggers Denied Service by US Host*, <http://mydailyclarity.com/2009/04/3215> (last visited May 8, 2010); Posting of Gaith Saqer to ArabCrunch, *LinkedIn Kicks Off Syrian Users!*, <http://arabcrunch.com/2009/04/breaking-linkedin-kicks-off-syrian-users.html> (Apr. 17, 2009, 4:39 EST).

105. See *supra* note 54 and accompanying text.

106. York, *supra* note 104; My Heart's in Accra, *LinkedIn Briefly Blocks Syria, More Confusion Over Trade/Commerce Regulations*, <http://www.ethanzuckerman.com/blog/2009/04/20/linkedin-briefly-blocks-syria-more-confusion-over-trade-commerce-regulations> (Apr. 20, 2009, 15:50 EST); see also Posting of Mary Joyce to DigiActive, *Why LinkedOut Syrians Are LinkedIn Again*, <http://www.digiactive.org/2009/04/21/why-linkedout-syrians-are-linkedin-again> (Apr. 21, 2009, 19:17 EST).

107. See Joyce, *supra* note 106.

108. See Matthew Sugrue, *A License to Chat*, THE HUFFINGTON POST, Oct. 30, 2009, http://www.huffingtonpost.com/matthew-sugrue/a-license-to-chat_b_340443.html; *US Sanctions Sees Live Messenger Blocked in Syria*, ITP.NET, May 25, 2009, <http://www.itp.net/556637-us-sanctions-sees-live-messenger-blocked-in-syria>; niacINSight, *Cutting Off Communication One Messenger at a Time*, <http://niacblog.wordpress.com/2009/05/27/cutting-off-communication-one-messenger-at-a-time> (May 27, 2009, 12:34 EST).

These episodes are all indicative of a dark reality: “the high costs and uncertainty involved in complying with the myriad of confusing sanctions regulations can deter companies from engaging in even permissible trade with a sanctioned country.”¹⁰⁹ This is particularly problematic in the context of ICT since users are increasingly dependent upon intermediaries such as webhosting service providers, blogging platforms, and social networking sites for their ability to speak online.¹¹⁰ And while regulatory uncertainty and companies’ resulting risk-averse behavior are not limited to the context of ICT,¹¹¹ the lack of clear rules regarding software and online services makes ICT a particularly difficult area.

Many ICT firms struggle to turn a profit when serving users in developing countries.¹¹² So long as regulatory uncertainties persist, these meager returns are insufficient to justify the expense of determining the legality of any given transaction or the risk of inadvertently violating sanctions regulations.¹¹³ Where firms’ reluctance to offer their products to users in sanctioned countries is merely a result of regulatory ambiguity, clarifying amendments or advisory opinions may be sufficient to solve this problem. But where sanctions regulations actually prohibit the export of software or online services, these pernicious effects are not so easily addressed. This is particularly unfortunate given that ICT are powerful tools for dissidents and human rights activists whose objectives are aligned with the policies underlying many U.S. sanctions programs.

V. ICT ARE USEFUL TOOLS FOR THE PROMOTION OF HUMAN RIGHTS

ICT have a long history of use by dissidents and human rights activists; the Internet itself was used as early as 1987 by human rights activists to report on the detention of social activists in Malaysia and Singapore.¹¹⁴ Most early use of ICT by human rights groups was quite rudimentary. Student demonstrators during the 1989 protests in Tiananmen Square in China relied largely on fax machines to relay information about the government’s response to the rest of the world, although the Internet played a small role as well.¹¹⁵ A more controver-

109. Smith, *supra* note 28, at 340.

110. See Zuckerman, *supra* note 100, at 72.

111. See *supra* note 86 and accompanying text.

112. See Brad Stone & Miguel Helft, *In Developing Countries, Web Grows Without Profit*, N.Y. TIMES, Apr. 27, 2009, at B1, available at <http://www.nytimes.com/2009/04/27/technology/start-ups/27global.html>.

113. See Zuckerman, *supra* note 100, at 78.

114. See Loong Wong, *The Internet and Social Change in Asia*, 13 PEACE REV. 381, 384 (2001).

115. See Scott E. Feir, Comment, *Regulations Restricting Internet Access: Attempted Repair of Rupture in China’s Great Wall Restraining the Free Exchange of Ideas*, 6 PAC. RIM

sial early use of ICT involved the Zapatista movement, a group of indigenous peasants that seized seven towns in the southern Mexican state of Chiapas in 1994.¹¹⁶ As the Mexican army moved in to suppress the rebels, Zapatista leaders used faxes and e-mails to inform the world about their grievances and the unfolding military standoff.¹¹⁷ NGOs then built a global, online solidarity movement, focusing international attention on the conflict and pressuring the Mexican government to call a cease-fire.¹¹⁸

Contemporary Internet activists engage in three general types of activities: awareness and advocacy; organization and mobilization; and action and reaction.¹¹⁹ In particular, human rights groups have turned to ICT as tools for mobilizing and organizing exceptionally broad and geographically dispersed constituencies, leveraging such technologies' ability to support sharing, aggregation, and collaborative production.¹²⁰ More controversially, some individuals have engaged in "hacktivism," launching distributed denial of service ("DDoS") attacks, writing computer viruses, and defacing websites to support their cause.¹²¹ This Part chronicles the evolving use of ICT by dissidents through a number of case studies that demonstrate the critical value of such technologies and the harm caused by U.S. policies restricting their export.

A. Online Organization and SMS — Ukraine's Orange Revolution

The ubiquitous spread of mobile phones equipped with short message service ("SMS") and cameras has enabled a revolutionary change in the use of ICT for human rights and development. Without this technological shift, and the parallel development of more sophisticated online platforms for publication and organization, the so-called

L. & POL'Y J. 361, 367 (1997); Trina K. Kissel, Note, *License To Blog: Internet Regulation in the People's Republic of China*, 17 IND. INT'L & COMP. L. REV. 229, 231–32 (2007).

116. See Maria Garrido & Alexander Halavais, *Mapping Networks of Support for the Zapatista Movement*, in CYBERACTIVISM 165, 165–66 (Martha McCaughey & Michael D. Ayers eds., 2003); Corinna Spencer-Scheurich, *A New Model for Globalizing Human Rights Struggles via the Internet: Understanding the Chiapas Example*, INT'L LEGAL PERSP., Spring 2004, at 22, 22.

117. See Spencer-Scheurich, *supra* note 116, at 22.

118. See *id.* at 26.

119. Sandor Vegh, *Classifying Forms of Online Activism*, in CYBERACTIVISM 71, 72 (Martha McCaughey & Michael D. Ayers eds., 2003).

120. Molly Beutz Land, *Networked Activism*, 22 HARV. HUM. RTS. J. 205, 216 (2009).

121. See Vegh, *supra* note 119, at 77–81. A denial of service ("DoS") attack is an attempt to make a computer resource such as a website unavailable, often by inundating the machine hosting the resource with external communications requests. When this is accomplished by sending requests from multiple hosts, this is a distributed DoS ("DDoS") attack. Wikipedia, *Denial-of-Service Attack*, <http://en.wikipedia.org/wiki/Ddos> (as of May 8, 2010, 22:25 GMT).

Orange Revolution in Ukraine, which saw the results of a fraudulent presidential election in 2004 overturned, may never have occurred.¹²²

The Internet was instrumental to activists during both the lead-up to the election and its aftermath. While most of Ukraine's mainstream media engaged in self-censorship, a community of citizen and professional journalists made use of online publishing platforms to create an alternative media environment on the Internet.¹²³ This online presence was then used during the election campaign to solicit donations, coordinate election monitoring, and post exit poll results.¹²⁴ The large discrepancy between these exit polls and the official results was partly responsible for the eruption of fifteen days of protests,¹²⁵ throughout which up-to-date reporting and analysis were constantly available online.¹²⁶ Pora, a pro-democracy movement with a wide political network, made particularly effective use of ICT. It distributed mobile phones to its members and used SMS and the Internet to organize protests and engage in "sousveillance," the covert monitoring of authority figures by grassroots groups.¹²⁷ In the end, the protests helped force another round of elections, which were widely seen as free and fair.¹²⁸

One critical lesson from the Orange Revolution is that ICT can be used to successfully organize massive protests involving hundreds of thousands of people even in a country with very low Internet penetration.¹²⁹ This suggests that access to the ICT currently blocked by U.S. trade sanctions may be able to have a large impact for dissidents in countries such as Cuba, Sudan, and Syria, despite the lack of widespread Internet availability in these countries.¹³⁰

122. See JOSHUA GOLDSTEIN, BERKMAN CENTER FOR INTERNET & SOCIETY, *THE ROLE OF DIGITAL NETWORKED TECHNOLOGIES IN THE UKRAINIAN ORANGE REVOLUTION 1* (2007), http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Goldstein_Ukraine_2007.pdf. *But see* Evgeny Morozov, *Texting Toward Utopia*, BOSTON REV., Mar.–Apr. 2009, at 19, available at <http://bostonreview.net/BR34.2/morozov.php> (cautioning that "drawing conclusions about the democratizing nature of the Internet may still be premature").

123. See GOLDSTEIN, *supra* note 122, at 4–6.

124. See *id.* at 8; Myroslaw J. Kyj, *Internet Use in Ukraine's Orange Revolution*, 49 BUS. HORIZONS 71, 79 (2006).

125. See Kyj, *supra* note 124, at 73, 79.

126. See *id.* at 73–74.

127. See GOLDSTEIN, *supra* note 122, at 8; see also My Heart's in Accra, Draft Paper on Mobile Phones and Activism, <http://www.ethanzuckerman.com/blog/2007/04/09/draft-paper-on-mobile-phones-and-activism> (Apr. 9, 2007, 17:11 EST) (describing the use of SMS and mobile phones by activists in the developing world).

128. See GOLDSTEIN, *supra* note 122, at 3.

129. Only two to four percent of Ukrainians had access to the Internet at the time. See *id.* at 5. Goldstein explains this initially surprising fact by referencing the Two-Step Flow Theory, a sociological theory that posits that information may flow to the general public through a small group of elite opinion makers. See *id.* at 5–6.

130. According to the International Telecommunication Union ("ITU"), Iran, Cuba, Sudan, and Syria had 31.37, 12.94, 10.16, and 16.79 Internet users per 100 inhabitants, respectively, in 2008. INT'L TELECOMM. UNION, INTERNET INDICATORS (2008), <http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx> (follow "Internet indicators:

Although the Orange Revolution demonstrates the democratizing potential of ICT, its broader significance should not be overstated. It is unclear to what extent these events could be replicated in other countries, such as Iran, Syria, Cuba, or Burma/Myanmar, where the government maintains tighter control over its citizens' access to information and is more willing to use force in response to protests. The outgoing Ukrainian government's willingness to tolerate the presence of an online alternative media sphere, instrumental in sustaining the protests, may not be present in these other contexts. The failed Saffron Revolution in Burma/Myanmar provides a cautionary tale about the limits of ICT to support anti-government protests in a regime more repressive than Ukraine's. When images and videos of the monk-led peaceful protests and the government's violent crackdown leaked onto the Internet, the military junta imposed an information blockade, completely shutting down the Internet and disabling most mobile phone services for a number of days.¹³¹ It remains to be seen whether the Green Revolution in Iran, discussed *infra*, will validate the hopeful lesson from the Orange Revolution, or serve as another cautionary tale of unwarranted cyber-optimism alongside the Saffron Revolution.

B. Circumvention Tools — Breaching the Great Firewall of China

China employs both legal and technical means to create a highly sophisticated system for controlling the online information available to its citizens. Internet service providers ("ISPs"), online content providers, and end-users are all prohibited from producing or disseminating information that falls within any of nine broad categories.¹³² Internet news organizations are further prohibited from posting information from two additional categories, and may not post content that they have gathered and edited themselves.¹³³ All non-commercial websites must register with provincial Communications Administration Offices, and all commercial websites must be licensed.¹³⁴ Indi-

subscribers, users and broadband subscribers" hyperlink). Figures were not available for North Korea, and the strict regulation of the Internet under Kim Jong-il may limit the usefulness of ICT in promoting regime change or otherwise benefitting civil society.

131. See MRIDUL CHOWDHURY, BERKMAN CENTER FOR INTERNET & SOCIETY, THE ROLE OF THE INTERNET IN BURMA'S SAFFRON REVOLUTION 13 (2008), http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Chowdhury_Role_of_the_Internet_in_Burmas_Saffron_Revolution.pdf_0.pdf; STEPHANIE WANG, OPENNET INITIATIVE, PULLING THE PLUG: A TECHNICAL REVIEW OF THE INTERNET SHUTDOWN IN BURMA 1, http://opennet.net/sites/opennet.net/files/ONI_Bulletin_Burma_2007.pdf.

132. See WANG, *supra* note 95, at 7.

133. See Kissel, *supra* note 115 at 239–40. News organizations that have been established by a government agency and that post news gathered and reported by employees of that agency are exempt from the latter restriction. *Id.*

134. See *id.* at 237–38; see also Clara Liang, Note, *Red Light, Green Light: Has China Achieved Its Goals Through the 2000 Internet Regulations?*, 34 VAND. J. TRANSNAT'L L.

viduals must register with local police to obtain a license for personal Internet access, and Internet cafés are tightly regulated.¹³⁵ Penalties for violations include fines, content removal, and criminal liability, including imprisonment.¹³⁶ As a result of this legal framework, users, ISPs, and content providers all engage in extensive self-censorship.¹³⁷

For content hosted outside of the country, China supplements its legal controls with a highly sophisticated filtering system, colloquially labeled the “Great Firewall of China.”¹³⁸ Since the Chinese government owns all of the backbone Internet connections serving the country, it has been able to control all traffic entering or leaving China by reconfiguring the backbone routers to implement a complex set of content-filtering and surveillance rules.¹³⁹ Technical measures have also been imposed on domestic businesses when they have been remiss in censoring their users. In March 2004, three domestic blog-hosting sites were forced to shut down until they implemented mechanisms for filtering users’ posts based on a list of sensitive keywords.¹⁴⁰

Sophisticated Chinese Internet users can bypass the Great Firewall by using circumvention software and proxy servers.¹⁴¹ The availability of anti-circumvention technologies such as Triangle Boy, Peekabooty, and Anonymizer are thus critical tools for both cyberactivists and ordinary Chinese citizens who want to access censored information.¹⁴² But because government censors continually update their filtering software to block the latest circumvention tools, developers must constantly release new versions, which are inevitably

1417, 1418–19 (2001) (describing regulations restricting online businesses and information flow over the Internet implemented by China in 2000).

135. See Kissel, *supra* note 115, at 252–54 (describing individual registration requirements and regulations imposed on Internet cafés).

136. See WANG, *supra* note 95, at 7, 9.

137. See Kissel, *supra* note 115 at 242–46.

138. See WANG, *supra* note 95, at 1 (describing China as having “one of the largest and most sophisticated filtering systems in the world”). The term “Great Firewall of China” was first used in a 1997 Wired article discussing Chinese government regulation of the Internet. See Geremie R. Barne & Sang Ye, *The Great Firewall of China*, WIRED, June 1997, at 138, available at <http://www.wired.com/wired/archive/5.06/china.html>.

139. See Kissel, *supra* note 115, at 246–49 (describing technical filtering at the backbone level).

140. See Ronald Deibert & Rafal Rohozinski, *Good for Liberty, Bad for Security? Global Civil Society and the Securitization of the Internet*, in ACCESS DENIED 123, 141 (Ronald Deibert et al. eds., 2008), available at http://opennet.net/sites/opennet.net/files/Deibert_07_Ch06_123-150.pdf.

141. See Kissel, *supra* note 115, at 263–64 (describing the use of circumvention technologies by Chinese Internet users); Brad Stone & David Barboza, *Scaling the Digital Wall in China*, N.Y. TIMES, Jan. 16, 2010, at B1, available at <http://www.nytimes.com/2010/01/16/technology/internet/16evade.html>.

142. See Vegh, *supra* note 119, at 77–78 (describing the peekabooty project); Andrew W. Lloyd, Note, *Increasing Global Demand for an Uncensored Internet — How the U.S. Can Help Defeat Online Censorship by Facilitating Private Action*, 41 VAND. J. TRANSNAT’L L. 299, 306–07 (2008).

blocked again, in an endless game of cat and mouse.¹⁴³ Since China is not subject to OFAC sanctions, its citizens have access to U.S. circumvention software, can host their content outside China with U.S. webhosting companies, and can use services like Twitter to relay information remotely.¹⁴⁴ Recognizing the advantages of allowing Chinese citizens to access unfiltered information, the U.S. government has even funded the development of some circumvention software.¹⁴⁵ Given these benefits, it seems incongruous that the U.S. would prohibit the export of these technologies to citizens of countries such as Iran and Syria, whose governments also implement pervasive Internet filtering and online surveillance.¹⁴⁶ Yet, as described earlier, OFAC regulations prohibit users in Iran, Cuba, and parts of Sudan from accessing these tools, while BIS may restrict their export elsewhere if encryption is involved.¹⁴⁷

*C. Social Networks, Twitter, and Modern ICT —
Election Protests in Moldova and Iran*

As online platforms for content-distribution and information-sharing have continued to evolve, the advent of social networking sites, blogs, photo and video hosting sites, and microblogging services such as Twitter have provided an important complement to SMS-enabled camera phones to aid demonstrators in both democratic and autocratic nations.¹⁴⁸ The power of these new technologies has been effectively demonstrated by protesters in Moldova and Iran following disputed elections in each country.

In April 2009, Moldovan youths used Twitter, Facebook, and other ICT to organize a flashmob after the results of a parliamentary election indicated a Communist victory.¹⁴⁹ Protesters used their mo-

143. See Bill Xia, *Cat and Mouse*, 37 INDEX ON CENSORSHIP 114, 117–118 (2008).

144. See Juliet Ye & Geoffrey A. Fowler, *Chinese Bloggers Scale the 'Great Firewall' in Riot's Aftermath*, WALL ST. J., July 2, 2008, at A7, available at <http://online.wsj.com/article/SB121493163092919829.html> (describing the use of foreign hosting, “technical loopholes,” and Twitter by blogger Zhou Shuguang to deliver information to his readers in the aftermath of rioting in Weng’an in 2008).

145. See Eric J. Stieglitz, Note & Recent Development, *Anonymity on the Internet: How Does It Work, Who Needs It, and What Are Its Policy Implications?*, 24 CARDOZO ARTS & ENT. L.J. 1395, 1400 (2007) (describing U.S. government funding of UltraSurf proxy software).

146. See OPENNET INITIATIVE, INTERNET FILTERING IN IRAN (2009), <http://opennet.net/research/profiles/iran>; OPENNET INITIATIVE, INTERNET FILTERING IN SYRIA (2009), <http://opennet.net/research/profiles/syria>.

147. See *supra* note 50–51 and accompanying text. Despite these restrictions, groups such as Human Rights Watch have offered to train NGOs on how to use encryption in the field. See Wong, *supra* note 114, at 382.

148. See *Rioters of the World Unite*, ECONOMIST, Dec. 18, 2008, at 109.

149. See Net Effect, *Moldova's Twitter Revolution*, http://neteffect.foreignpolicy.com/posts/2009/04/07/moldovas_twitter_revolution (Apr. 7, 2009, 14:15 EST); Net Effect, *Moldova's Twitter Revolution Is NOT a Myth*, <http://neteffect.foreignpolicy.com/>

bile phones to capture still and video images and upload them to sites such as Facebook and YouTube, while a Romanian TV station hosted a live stream of the protests.¹⁵⁰ Although there were claims of election fraud,¹⁵¹ the vote was tentatively accepted by election observers from the European Union and the Organization for Security and Cooperation in Europe.¹⁵² A judicially ordered recount, potentially a result of the protests, confirmed the initial results.¹⁵³

A mere two months later, a presidential election in Iran returned Mahmoud Ahmadinejad to power and set off “the largest antigovernment demonstrations since the 1979 revolution.”¹⁵⁴ In contrast to the Moldovan elections, the Iranian vote was widely seen as fraudulent, and street protests have continued intermittently ever since.¹⁵⁵ As in the Moldovan case, Twitter, social networking sites, and photo and video hosting sites such as Flickr and YouTube were crucial tools for protesters in Iran to organize themselves and get information out to the global community.¹⁵⁶ These methods became especially critical once the Iranian government began to crack down on mainstream and foreign media. Foreign journalists were not granted visa extensions, and those whose visas had not expired were banned from leaving their offices.¹⁵⁷ Both domestic and foreign journalists were detained.¹⁵⁸ The

posts/2009/04/10/moldovas_twitter_revolution_is_not_a_myth (Apr. 10, 2009, 21:42 EST); Net Effect, *More Analysis of Twitter’s Role in Moldova*, http://neteffect.foreignpolicy.com/posts/2009/04/07/more_analysis_of_twitters_role_in_moldova (Apr. 7, 2009, 21:12 EST); My Heart’s in Accra, *Unpacking “The Twitter Revolution” in Moldova*, <http://www.ethanzuckerman.com/blog/2009/04/09/unpacking-the-twitter-revolution-in-moldova> (Apr. 9, 2009, 17:42 EST).

150. See Net Effect, *Moldova’s Twitter Revolution*, http://neteffect.foreignpolicy.com/posts/2009/04/07/moldovas_twitter_revolution (Apr. 7, 2009, 14:15 EST).

151. See Ellen Barry, *After Protests, Moldovan Opposition Claims Election Fraud*, N.Y. TIMES, Apr. 10, 2009, at A6, available at <http://www.nytimes.com/2009/04/10/world/europe/10moldova.html>.

152. See Ellen Barry, *Protests in Moldova Explode, with Help of Twitter*, N.Y. TIMES, Apr. 8, 2009, at A1, available at <http://www.nytimes.com/2009/04/08/world/europe/08moldova.html>.

153. *Moldova Recount ‘Confirms Result’*, BBC NEWS, Apr. 17, 2009, <http://news.bbc.co.uk/2/hi/europe/8004603.stm>.

154. Robert F. Worth & Nazila Fathi, *Defiance Grows as Iran’s Leader Sets Vote Review*, N.Y. TIMES, June 16, 2009, at A1, available at <http://www.nytimes.com/2009/06/16/world/middleeast/16iran.html>; see also *Poll Results Prompt Iran Protests*, AL JAZEERA ENG., June 14, 2009, <http://english.aljazeera.net/news/middleeast/2009/06/2009613172130303995.html>.

155. See *supra* notes 1–9 and accompanying text.

156. See Anne-Marie Corley, *The Web vs. The Republic of Iran*, TECH. REV., June 18, 2009, <http://www.technologyreview.com/web/22893/page1>. But see Evgeny Morozov, *Iran: Downside to the “Twitter Revolution”*, DISSENT, Fall 2009, at 10.

157. See David Blair, *Iran Struggles to Censor News of Protests*, DAILY TELEGRAPH (London), June 15, 2009, <http://www.telegraph.co.uk/news/worldnews/middleeast/iran/5543145/iran-struggles-to-censor-news-of-protests.html> (describing efforts of the Iranian government to prevent news of the protests spreading); Catherine Lyons, *Opinion, Iran: Now the World’s Leader in Jailing Journalists*, L.A. TIMES, June 26, 2009, <http://opinion.latimes.com/opinionla/2009/06/iran-jailed-journalists-freedomofspeechelections.html>.

Iranian diaspora and other members of the international community have also made use of Twitter and Facebook to demonstrate their support for the protesters.¹⁵⁹

In response to the protesters' use of ICT, the Iranian government attempted to block access to Twitter, social networks, and SMS.¹⁶⁰ Using many of the same circumvention tools employed by users in China, protesters were able to bypass the government's filters.¹⁶¹ Hacktivists have also used Twitter, Facebook, and other social networks to organize DDoS attacks against websites supporting Ahmadi-nejad and the Iranian government.¹⁶² In an attempt to dissuade protesters, the Iranian government has warned that SMS and e-mail systems were being monitored by police and that individuals using them to organize protests would be prosecuted.¹⁶³ If true, this warning demonstrates that social networking sites, blogs, and similar technological tools may be double-edged swords for activists. Incautious activists using such tools to communicate and organize online may find their activities monitored, their identities revealed, and their protests preempted.¹⁶⁴

This widespread digital civil disobedience did not go unnoticed by the U.S. government. In a highly unusual move, the State Department contacted Twitter directly during the initial round of protests to

158. See Pamela Hess, *Group: Dozens of Journalists Among Jailed in Iran*, ABC NEWS, June 26, 2009, <http://abcnews.go.com/US/wireStory?id=7940259>; Lyons, *supra* note 157.

159. See Corley, *supra* note 156. A group of Chinese democracy activists has established a website and used Twitter and social networking sites to show their solidarity and condemn the Chinese government's complicity in the Iranian crackdown. See Meris Lutz, *Iran: Chinese Activists to Opposition: 'Go, Iranian Friends! Go!'*, L.A. TIMES, Jan. 4, 2010, <http://latimesblogs.latimes.com/babylonbeyond/2010/01/iran-chinese-cyberactivists-back-iranian-opposition.html>.

160. Associated Press, *Iranians Turn to Twitter as Censors Clamp Down*, THE INDEPENDENT (London), June 16, 2009, <http://www.independent.co.uk/news/world/middle-east/iranians-turn-to-twitter-as-censors-clamp-down-1706373.html>.

161. Doug Gross, *Iranians Dodging Government's Internet Crackdown*, CNN, June 18, 2009, <http://www.cnn.com/2009/TECH/06/18/iran.dodging.crackdown/index.html>. The Pirate Bay and Anonymous, an Internet collective, have set up a forum called Anonymous Iran at <http://iran.whyweprotest.net> to discuss the Iranian protests and provide information on how to circumvent government Internet censorship. See Jack Hawke, *Internet Underground Takes on Iran*, 9NEWS, June 18, 2009, <http://news.ninemsn.com.au/technology/827036/internet-underground-takes-on-iran>; Posting of Noah Shachtman to Danger Room, Iran Activists Get Assist From 'Anonymous,' Pirate Bay, <http://www.wired.com/dangerroom/2009/06/iran-activists-get-assist-from-anonymous-pirate-bay> (June 18, 2009, 9:25 EST).

162. See Angela Moscaritolo, *Iran Election Protesters Use Twitter To Recruit Hackers*, SC MAGAZINE, June 15, 2009, <http://www.scmagazineus.com/iranian-election-protesters-use-twitter-to-recruit-hackers/article/138545>; Peter Wilkinson, *Briton's Software a Surprise Weapon in Iran Cyberwar*, CNN, June 17, 2009, <http://edition.cnn.com/2009/WORLD/meast/06/17/iran.elections.hackers>.

163. See *Iran Issues Warning on Opposition Internet Use*, BBC NEWS, Jan. 16, 2010, http://news.bbc.co.uk/2/hi/middle_east/8462857.stm. Iran's police chief is quoted as saying that protesters "should not think using proxies will prevent their identification." *Id.*

164. See Morozov, *supra* note 156, at 12.

request that the company postpone scheduled maintenance so as not to disrupt service for the Iranian protesters.¹⁶⁵ As protests continued and the role of ICT was given greater media coverage, both the legislative and executive branches proposed changes to the Iranian sanctions program that would allow Iranian citizens to access U.S. communication, information exchange, and circumvention technologies. In July 2009, the Senate passed the Victims of Iranian Censorship Act as part of a defense authorization bill, which authorizes the U.S. government to develop proxy servers and allow Iranian citizens to use them.¹⁶⁶ In December, Representative Jim Moran targeted export controls more directly by introducing the Iranian Digital Empowerment Act, which would authorize the export to Iran of “software and related services” that enable personal communication or allow citizens to bypass government censorship.¹⁶⁷ More directly still, the State Department issued a report to Congress, pursuant to Section 1606 of the Iran-Iraq Arms Non-Proliferation Act of 1992,¹⁶⁸ stating that sanctions on mass-market software for personal Internet-based communications that can be downloaded for free would be waived with respect to Iran.¹⁶⁹ This waiver was implemented by OFAC, and expanded to include Cuba and Sudan, on March 8, 2010.¹⁷⁰

VI. CONCLUSION

The development of new technological means of communication, organization, and information exchange has been a great boon to pro-democracy dissidents, human rights activists, and ordinary citizens around the globe. But by maintaining comprehensive trade sanctions programs, the U.S. government has withheld these technologies from

165. See Musgrove, *supra* note 11, at A10; Grossman, *supra* note 11.

166. See Eli Lake, *Senate OKs Funds To Thwart Iran Web Censors*, WASH. TIMES, July 26, 2009, at A1, available at <http://www.washingtontimes.com/news/2009/jul/26/senate-help-iran-dodge-internet-censorship>.

167. The Iranian Digital Empowerment Act, H.R. 4301, 111th Cong. (2009); see also Press Release, Office of Congressman Jim Moran, *New Moran Measure Calls for ‘Smarter’ Sanctions on Iran* (Dec. 14, 2009), http://moran.house.gov/apps/list/press/va08_moran/SmartSanctions.shtml.

168. 50 U.S.C. § 1701 note (2006).

169. See Letter from Richard R. Verma, Assistant Secretary of Legislative Affairs, U.S. Department of State, to The Honorable Carl Levin, Chairman of the U.S. Senate Committee on Armed Services (Dec. 15, 2009), available at <http://levin.senate.gov/newsroom/supporting/2009/SASC.IranReport.121509.pdf>; see also Steptoe & Johnson LLP, *International Law Advisory — U.S. To Waive Iranian Sanctions on Export of Certain Personal Communications Software* (Dec. 18, 2009), <http://www.steptoe.com/publications-6534.html>; ExportLawBlog, @Ahmadinejad: Twitter Is Coming to Town. #IranElection, <http://www.exportlawblog.com/archives/1099> (Dec. 17, 2009, 21:31 EST) (discussing the State Department report to Congress).

170. Amendments to the Cuban Assets Control Regulations, Sudanese Sanctions Regulations, and Iranian Transactions Regulations, 75 Fed. Reg. 10,997 (Mar. 10, 2010) (codified at 31 C.F.R. §§ 515.578, 538.533, 560.540).

those who need them the most, often frustrating its own foreign policy goals in the process. Recent government action in the wake of elections protests in Iran, however, offers some hope. Given the concrete example of U.S. software and services helping citizens in a sanctioned country protest the abuse of their civil, political, and human rights, the U.S. government has acknowledged the pernicious effects of the current trade sanctions regulations affecting ICT. Encouragingly, it has implemented reforms that would benefit citizens and activists in Iran, Sudan, and Cuba.¹⁷¹

However, these reforms do not go far enough. The U.S. government should take advantage of this opportunity to carefully scrutinize and refine its entire set of sanctions programs. At the very least, BIS should follow OFAC's lead and amend the EAR to authorize the export of similar communications-enabling mass market software to citizens in Cuba, Syria, and North Korea. Moreover, both BIS and OFAC should amend their sanctions programs to allow citizens in sanctioned nations to access the online services and software necessary to circumvent government-imposed Internet censorship. By proactively extending these benefits, the U.S. might further its foreign policy objectives by giving dissidents the tools to organize in the face of repressive regimes.

The complexity of the current export control regulations regarding ICT must also be reduced. In particular, BIS-administered controls on the export of encryption must be modified. Human rights groups that promote the use of encryption by activists and NGOs in the field may find their work frustrated if the companies that develop encryption software are reluctant to make it widely available for fear of violating U.S. export controls.¹⁷² Although this problem affects all software and online service, it is especially acute with regard to encryption because of the complexity of the regulations that deal with such technology.¹⁷³ BIS must thus continue to clarify and liberalize its encryption controls. In a 2009 Advisory Opinion, it noted that “[p]ublishing ‘mass market’ encryption software to the Internet where it may be downloaded by anyone neither establishes ‘knowledge’ of a prohibited export or reexport nor triggers any ‘red flags’ necessitating the affirmative duty to inquire under the ‘Know Your Customer’ guidance.”¹⁷⁴ This exception only applies, however, for anonymous

171. See *supra* note 170 and accompanying text.

172. See *supra* Part IV (providing examples of U.S.-based companies refusing to offer software and services to users in countries under U.S. trade sanctions).

173. See *supra* notes 51–52 and accompanying text.

174. Advisory Opinion, Bureau of Industry & Security, U.S. Dept. of Com., Sept. 11, 2009, http://www.bis.doc.gov/policiesandregulations/advisoryopinions/encryption_internet_ao.pdf; see also 15 C.F.R. § 740.13(e) note (2009) (“Posting [publicly available] encryption source code and corresponding object code on the Internet . . . where it may be downloaded by anyone neither establishes ‘knowledge’ . . . nor triggers any ‘red flags’ necessitating the

downloads.¹⁷⁵ There is no principled reason for this restriction, and it may have pernicious effects on the efficacy of encryption-enabled software. Circumvention tools, which require constant updating, offer a prime example.¹⁷⁶ Given that censorship authorities are constantly blocking sites where such tools are made available, one of the most effective ways to disseminate updates is via e-mail. But since the Advisory Opinion makes clear that asking for a user's e-mail address renders the export non-anonymous,¹⁷⁷ most exporters are unlikely to take the risk. At the very least, then, BIS should expand the rule in this Advisory Opinion to cover the collection of user e-mail addresses in conjunction with the download of mass market encryption software.

In any analysis of the role of ICT in promoting human rights and development, there is a danger of succumbing to cyber-utopianism. The benefits of technology can certainly be exaggerated; in the Iranian context, critics have questioned whether Twitter has been as instrumental as the media has portrayed it.¹⁷⁸ Furthermore, such technologies do not represent an unmitigated good; they can also be used to subvert democracy and human rights. The Zapatista movement in Mexico and the violent protests in Moldova demonstrate that ICT may be used to support armed rebellion or undermine a legitimate election.¹⁷⁹ Mobile phone SMS networks were used in Kenya after a disputed election in 2007 to distribute messages promoting ethnic-based mob violence.¹⁸⁰ The Great Firewall of China was built with Cisco hardware.¹⁸¹ It has even been suggested that the Iranian gov-

affirmative duty to inquire under the 'Know Your Customer' guidance provided in Supplement No. 3 to part 732 of the EAR.")

175. See Advisory Opinion, *supra* note 174 (explaining that non-anonymous distribution includes, *inter alia*, requiring user registration or tracking data, but not collection of downloaders' IP addresses if not later used or tracked by the provider).

176. See *supra* notes 141–42 and accompanying text.

177. See Advisory Opinion, *supra* note 174 (stating that, if the export requires the provision of a name and e-mail address, "the download of the software would not be considered anonymous").

178. See, e.g., Morozov, *supra* note 156, at 10.

179. See *supra* notes 116–18, 149–53 and accompanying text.

180. See JOSHUA GOLDSTEIN & JULIANA ROTICH, BERKMAN CENTER FOR INTERNET & SOCIETY, DIGITALLY NETWORKED TECHNOLOGY IN KENYA'S 2007–2008 POST-ELECTION CRISIS 4 (2008), http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Goldstein&Rotich_Digitally_Networked_Technology_Kenyas_Crisis.pdf. ICT were also used for constructive ends during the post-election turmoil. Most notable was Ushahidi, a website that allowed users to report incidents of violence via mobile phone or Internet browser and associate them with a location using Google Maps. See *id.* at 5–6; see also Ushahidi: Crowdsourcing Crisis Information, About, <http://www.ushahidi.com/about> (last visited May 8, 2010).

181. See Posting of Sarah Lai Stirland to Threat Level, Cisco Leak: 'Great Firewall' of China Was a Chance To Sell More Routers, <http://www.wired.com/threatlevel/2008/05/leaked-cisco-do> (May 20, 2008, 16:50 EST).

ernment could use a service like Amazon's Mechanical Turk to hire global Internet users to unwittingly identify protesters.¹⁸²

Despite these cautions, technologies and online services for communication, information-exchange, and the circumvention of Internet censorship are valuable tools for dissidents and human rights activists. In contrast, U.S.-developed ICT are not essential for repressive regimes, which will always have alternative methods available to oppress their citizens.¹⁸³ Prohibiting the use of software and online services by citizens living under such regimes merely reinforces their repression while doing nothing to thwart those in power. U.S. trade sanctions programs must be changed to reflect this reality.

182. See Jonathan Zittrain, Berkman Ctr. for Internet & Soc'y, *Minds for Sale* (Nov. 18, 2009), available at <http://www.youtube.com/watch?v=Dw3h-rae3uo> (Mechanical Turk is discussed at 0:33:21–0:34:58).

183. See *supra* notes 74–75 and accompanying text.