JUNE
2011

Internet Freedom
A Foreign Policy Imperative in the Digital Age

By Richard Fontaine and Will Rogers

Center for a New American Security

Acknowledgments

We express our gratitude to our colleagues at the Center for a New American Security (CNAS) for their assistance with this study. Jackie Koo provided exceptional research assistance throughout the writing process. Kristin Lord's efforts in editing and shaping this report and the overall CNAS Internet freedom project were invaluable. Nora Bensahel devoted significant time and effort to improving the writing. Liz Fontaine provided typically excellent design and layout help on a short timeline.

We owe a great deal of thanks to Ambassador David Gross, who shared his unique insights throughout the entirety of this project. We also owe a large debt of gratitude to those who reviewed all or part of this paper in draft form, including Ken Berman, Daniel Calingeart, Andrew Lewman, Sarah Labowitz, Marc Lynch, Rebecca MacKinnon, Jeff Pryce, Ben Scott and several anonymous reviewers. We thank the Harvard Law School National Security Research Group for its extraordinary help in researching the international legal implications of Internet freedom. The group, which is directed by Ivana Deyrup, includes Gracye Cheng, Morgan Cohen, Josh Green, Carlos Oliveira and Mark Stadnyk. Finally, we would like thank the many experts who patiently spoke with us about Internet freedom issues over the last year, whether in government, the private sector or academia, here in Washington, in Silicon Valley, or elsewhere.

This publication was made possible through the support of grants from the John Templeton Foundation and the Markle Foundation. The opinions expressed in this publication are those of the authors and do not necessarily reflect the views of the John Templeton Foundation or the Markle Foundation. Readers should note that some organizations that are mentioned in the report or that otherwise have an interest in the issues discussed here support CNAS financially. CNAS maintains a broad and diverse group of more than 100 funders, including private foundations, government agencies, corporations and private individuals, and retains sole editorial control over its ideas, projects and products. A complete list of the Center's financial supporters can be found on our website at www.cnas.org/support/our-supporters.

The authors of this report are solely responsible for the analysis and recommendations contained herein.

Cover Image
A man takes pictures with his cell phone on Tahrir, or Liberation Square, in Cairo on January 31, 2011.

(BEN CURTIS/Associated Press)

TABLE OF CONTENTS

JUNE 2011

Internet Freedom

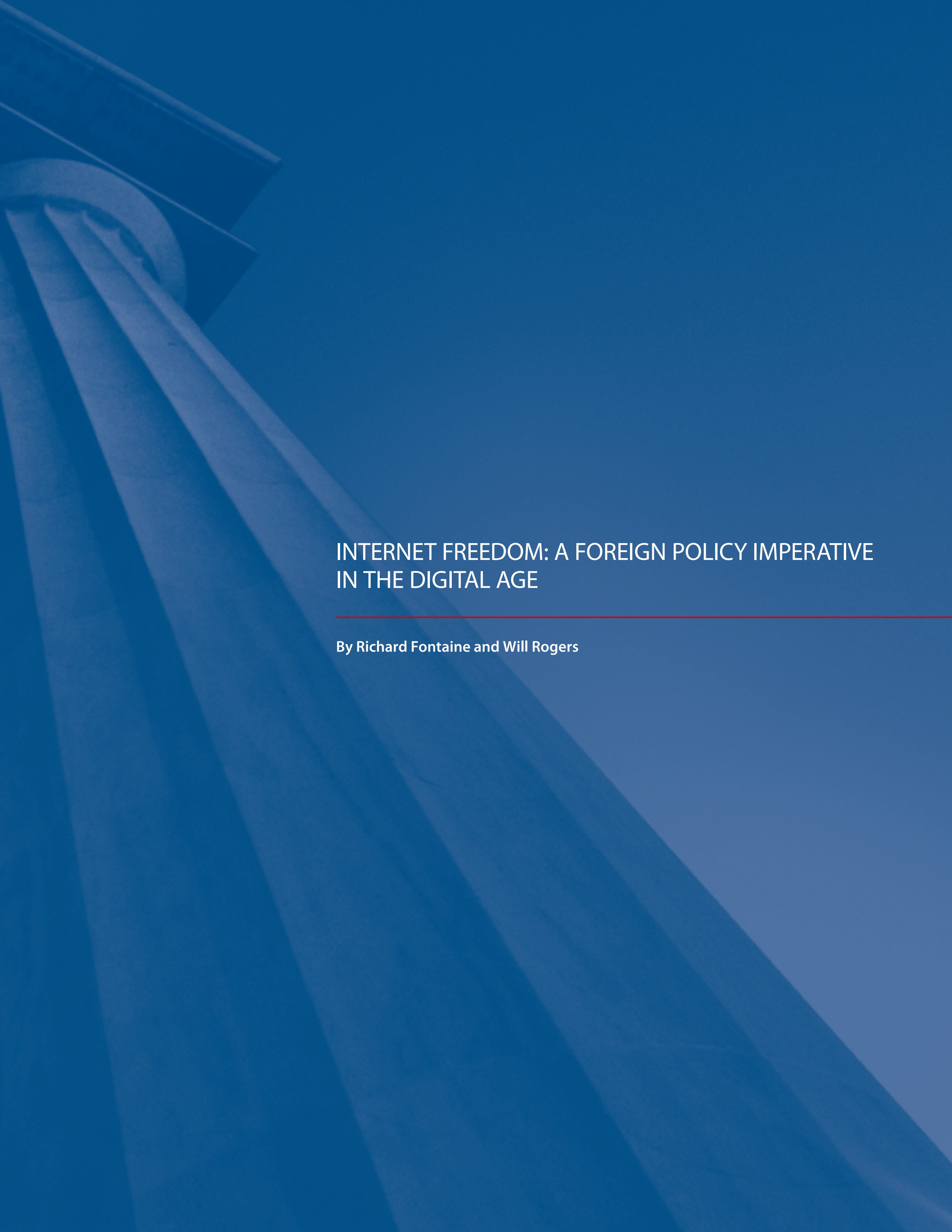
A Foreign Policy Imperative in the Digital Age

By Richard Fontaine and Will Rogers

About the Authors

Richard Fontaine is a Senior Fellow at the Center for a New American Security.

Will Rogers is a Research Associate at the Center for a New American Security.



INTERNET FREEDOM: A FOREIGN POLICY IMPERATIVE IN THE DIGITAL AGE

By Richard Fontaine and Will Rogers

JUNE 2011

Internet Freedom

A Foreign Policy Imperative in the Digital Age

I. EXECUTIVE SUMMARY

By Richard Fontaine and Will Rogers

America needs a comprehensive Internet freedom strategy, one that tilts the balance in favor of those who would use the Internet to advance tolerance and free expression, and away from those who would employ it for repression or violence.

This requires incorporating Internet freedom as an integral element of American foreign policy. As recent events in the Middle East demonstrate, the Internet has emerged as a major force in international affairs, one that will have lasting implications for the United States and the international community. But new communications technologies are a double-edged sword. They represent both a medium for individuals to communicate, form groups and freely broadcast their ideas around the world, and a tool that empowers authoritarian governments. U.S. policymakers should better appreciate the complex role new communications technologies play in political change abroad, and how those technologies intersect with the array of American foreign policy objectives.

Internet freedom typically includes two dimensions. Freedom *of* the Internet denotes the freedoms of online expression, assembly and association – the extension to cyberspace of rights that have been widely recognized to exist outside it. Promoting freedom of the Internet merely expands to cyberspace a tradition of U.S. diplomatic and financial support for human rights abroad. Freedom *via* the Internet, the notion that new communications technologies aid the establishment of democracy and liberal society offline, is at once more alluring and hotly contested. Internet freedom in this sense has captured the imagination of many policymakers and experts who see in these technologies a tool for individuals to help move their societies away from authoritarianism and toward democracy. Though the links between democracy and Internet freedom are indirect and complex, nascent evidence suggests that new communications tools do matter in political change, and that both dissidents and dictators act on that basis.

Most attention has focused on technologies that allow dissidents to penetrate restrictive firewalls and communicate securely. But funding technology comprises just one aspect of America's Internet freedom agenda. The United States also advocates international norms regarding freedom of speech and online assembly and opposes attempts by autocratic governments to restrict legitimate online activity.

The private sector has a critical role to play in promoting Internet freedom, but, given corporate interests in maximizing profits rather than promoting online freedom in repressive environments, efforts to expand its role are difficult. Ethical debates, ranging from whether American companies should be permitted to sell repressive regimes key technologies to the responsibilities of corporations in the face of an autocracies' demand for information, remain unresolved. And the other side of this coin – whether U.S. export controls should prohibit selling technologies that could be used to promote online freedom – is often overlooked.

To date, the U.S. government has shied away from articulating fully the motivations behind its Internet freedom agenda. Administration officials emphasize that their policy supports freedom *of* the Internet, not freedom *via* the Internet, and that the Internet freedom agenda is not part of a broader strategy to support democratic evolution. It should be.

Admittedly, promoting Internet freedom is complicated, and involves inherent tensions with other U.S. foreign policy, economic and national security interests. This is particularly true in the area of cyber security. Cyber security experts seek to secure the United States against cyber attacks, for example, by pushing for greater online transparency and attribution, while Internet freedom proponents urge greater online anonymity. While tensions between Internet freedom and cyber security are real, and in some cases will force difficult choices, they should not prevent robust U.S. efforts to advance both.

A robust Internet freedom agenda should reflect the following eight principles:

Principle 1: Embrace a Comprehensive Approach

U.S. policymakers should incorporate Internet freedom into their decision-making (especially on cyber security and economic diplomacy issues); convene private sector professionals, export controls experts, diplomats and others to explore new ways of promoting Internet freedom; and use traditional diplomacy to promote Internet freedom.

Principle 2: Build an International Coalition to Promote Internet Freedom

The U.S. government should convene a core group of democratic governments to advocate Internet freedom in key international fora; urge governments to encourage foreign companies to join the Global Network Initiative (GNI); and ensure that the Secretary of State gives her next major address on Internet freedom in a foreign country, possibly in Europe alongside key European Union (EU) commissioners.

Principle 3: Move Beyond Circumvention Technologies

The U.S. government should continue to fund technologies other than firewall-evasion tools, including those that help dissidents maintain digital security, ensure mobile access and reconstitute websites after a cyber attack. The U.S. government should offer financial awards to foster technological innovation, require that any online tool receiving U.S. funding be subjected to an independent security audit and expand the sources of technology funding to include foreign governments, foundations and the private sector.

Principle 4: Prioritize Training

The State Department, along with the U.S. Agency for International Development (USAID), should continue to foster Internet freedom through targeted training programs, including education on online safety.

Principle 5: Lead the Effort to Build International Norms

The U.S. government should promote a liberal concept of Internet freedom in all relevant fora, and reject attempts by authoritarian states to promote norms that restrict freedoms of information and expression online. It should also pursue an international transparency initiative to encourage governments to publicize their policies on restricting online information.

Principle 6: Create Economic Incentives to Support Internet Freedom

U.S. officials should continue to articulate the economic case for Internet freedom, backed wherever possible by solid quantitative evidence, and push for Internet censorship to be recognized as a trade barrier.

Principle 7: Strengthen the Private Sector's Role in Supporting Internet Freedom

Congress should adopt laws that prohibit American corporations from giving autocratic governments the private data of dissidents when the request is clearly intended to quash legitimate freedom of expression, and that require companies to periodically disclose requests it receives for such data to the U.S. government. U.S. officials should continue to urge companies to join the GNI, but also encourage them to develop broad unilateral codes of conduct consistent with the GNI. They should also publicly highlight specific business practices, both positive and negative.

Principle 8: Reform Export Controls

The U.S. government should relax controls on technologies that would permit greater online freedom while protecting American national security, and educate companies on the precise nature of export control restrictions so that companies do not over-comply and deny legal technologies to dissidents abroad.

In addition, we offer several recommendations for technology companies, including providing dissidents basic technical assistance to better use built-in security functions for software and hardware; better informing users and the public about who may access the data they control and under what conditions; increasing corporate transparency about foreign government requests; and advocating for increased Internet freedom.

II. INTRODUCTION

The world's population is more connected, with more access to new information and ideas than ever before. Today, 2 billion people have access to the Internet. Five billion people use mobile phones, many of them smartphones with Internet access.[1] The Internet has also become an extension of civil society.[2] Digital tools are increasingly used to communicate across borders, organize protests, launch cyber attacks, build transnational coalitions, topple some dictators and possibly strengthen others – actions that all affect U.S. foreign policy. But American policymakers have just begun to incorporate the Internet's role into their broader conceptions of U.S. foreign policy.

Thus far, the discussion among advocates and foreign policy practitioners has revolved around "Internet freedom," a broad rubric that encompasses online freedoms, including the rights of expression and online organization, and the potentially transformative and hotly contested role of the Internet in promoting democratization. The U.S. government now has an Internet freedom agenda, with tens of millions of dollars to implement it. Both the Senate and the House of Representatives boast global Internet freedom caucuses. The Secretary of State has given two major addresses articulating principles and policies for Internet freedom, and newspapers and periodicals have repeatedly pointed to the use of online tools both for popular protest and as a means of repression. In the midst of the 2011 Arab Spring, President Obama went so far as to describe the ability to use social networking as a "core value" that Americans believe is "universal."[3]

The debate over whether and how to promote Internet freedom has been an emotional one, with "cyber utopians" praising the Internet as a singular tool for toppling dictators, and "cyber pessimists" noting all the ways that autocracies use new communications tools to strengthen their own rule. This report seeks to move beyond these two poles by identifying the nuances and tradeoffs involved in promoting online freedom.

This study focuses on the Internet, including Web-based communication platforms such as blogs, social networking and other photo- and video-sharing websites, and proposes an integrated Internet freedom strategy that balances competing U.S. interests.[4] We begin by defining Internet freedom, distinguishing between freedom *of* the Internet and freedom *via* the Internet, and examine why the United States has an interest in preserving an open Internet. We then explore ways in which the Internet can be used both for democratic political change and as a tool of repression. We argue that the United States should actively promote Internet freedom, given not only its potential to aid those seeking liberal political change, but also because doing so accords with America's deepest values. We examine the U.S. government's current efforts to promote Internet freedom abroad and the tensions between these efforts and enhancing cyber security. Finally, we provide a set of interlocking principles that, taken together, will incorporate Internet freedom into American foreign policy.

The paper assumes that the United States has an interest in supporting human rights and democracy abroad. There is a continued healthy debate about this point and it is far from America's only interest. But successive administrations (including those of Presidents Clinton, Bush and Obama) have made promoting democracy an explicit objective of U.S. policy. While the United States should be realistic and modest about what it can achieve, to the extent that a freer online space facilitates a freer offline space, the United States should support Internet freedom. At its heart, an American Internet freedom agenda should actively aim to tilt the balance in favor of those who would use the Internet to advance tolerance and free expression, and away from those who would use it for repression or violence.

This paper also acknowledges the downsides of the Internet. An autocratic regime can use the Internet to strengthen its ability to monitor its citizens and control their behavior. Terrorists can use it to communicate and spread propaganda. Criminals can use new technologies to organize illicit activities. Dissidents can use the Internet to spread their message, but so can extremists advocating violence. There is no certain outcome to this continual push and pull, and the local political context matters enormously.

At its heart, an American Internet freedom agenda should actively aim to tilt the balance in favor of those who would use the Internet to advance tolerance and free expression, and away from those who would use it for repression or violence.

This report examines Internet freedom through the lens of American foreign policy and explores two central questions: What does access to an open Internet mean for U.S. foreign policy, and what should the United States do about it? Our intended audience is not merely those individuals intimately familiar with Internet freedom issues, but also those foreign policy actors and thinkers who should be. As we discuss below, Internet freedom means many things to many people, and to some it suggests a focus on domestic policy – net neutrality, anti-trust law, the role of the Federal Communications Commission, and so on. Except where such domestic concerns impact Internet freedom promotion efforts abroad (as we argue they may), such issues are beyond the ambit of this paper.

The Center for a New American Security (CNAS) initiated this project in March 2010 when it hosted the launch of the Senate Global Internet Freedom Caucus. Over the course of more than a year, CNAS then convened a number of working groups on the role of the private sector, the prospects for international normative agreements, the role of circumvention technology and the tensions between cyber security and Internet freedom. In addition, we consulted with representatives in government, the corporate world, the nonprofit sector, technology firms and academia. The study was conducted alongside CNAS' companion project on cyber security.[5]

What is Internet Freedom?

Internet freedom, broadly defined, is the notion that universal rights, including the freedoms of expression, assembly and association, extend to the digital sphere. Yet policymakers and others often define Internet freedom differently. It is thus useful to differentiate, as a number of experts increasingly have, between two linked but distinct concepts: freedom *of* the Internet and freedom *via* the Internet.

Freedom *of* the Internet refers to the ability to engage in unfettered expression in cyberspace. This vision of Internet freedom, as scholar Evgeny Morozov points out in his book *The Net Delusion*, represents freedom *from* something: censorship, government surveillance, distributed denial of service (DDoS) attacks, and so on.[6] The principles undergirding freedom of the Internet are articulated in documents such as the Universal Declaration of Human Rights (UDHR), which describes as inalienable the right to receive and impart information without interference.[7] In this sense, Internet freedom is little different from the notion of free expression, whose advocacy has been an element of U.S. foreign policy for decades. After all, American ambassadors have long pressed foreign governments to allow a free press, release jailed journalists and cease jamming unwanted broadcasts.

Freedom *via* the Internet is at once both a more alluring and complicated idea. Its advocates suggest that more online freedom can lead to more offline freedom; that is, the free flow of ideas over the Internet promotes democratization. Freedom via the Internet has captured the imagination of many in Congress, the media and elsewhere (including dissidents and dictators) who have witnessed the Internet's seemingly transformative effects on autocratic governments. Protesters, democratic activists and average citizens are increasingly using Facebook, Twitter and other applications to communicate and organize – most recently in Tunisia and Egypt, but in other countries as well.

Internet Freedom and U.S. National Interests

The United States has a long history of providing diplomatic and financial support for the promotion of human rights abroad, including the right to free expression. While each presidential administration emphasizes human rights to differing degrees, during recent decades they have all consistently held that human rights are a key U.S. interest. Promoting freedom of the Internet expands human rights support into cyberspace, an environment in which an ever-greater proportion of human activity takes place. The United States advocates for freedom of the Internet because it accords not only with American values, but also with rights America believes are intrinsic to all humanity.

For years, the U.S. government has programmatically and rhetorically supported democracy promotion abroad. The State Department routinely disburses millions of dollars in funding for democracy-building programs around the world, many of which are aimed explicitly at expanding free expression. Presidential and other speeches regularly refer to the American belief in the universality of this right; to cite but one example, a March 2011 White House statement on Syria noted that, "The United States stands for a set of universal rights, including the freedom of expression and peaceful assembly."[8] The Obama administration's 2010 National Security Strategy specifically called for marshaling the Internet and other information technologies to support freedom of expression abroad,[9] and the Bush administration adopted a policy of maximizing access to information and ideas over the Internet.[10]

America's interest in promoting freedom *via* the Internet comes from the same fundamental belief in democratic values and human rights. Despite inevitable inconsistencies and difficult tradeoffs, the United States continues to support democracy. The Bush administration's 2006 National Security Strategy committed to support democratic institutions abroad through transformational diplomacy.[11] President Obama, after entering office with an evident desire to move away from the sweeping tone of his predecessor's "freedom agenda," nevertheless told the U.N. General Assembly in 2009 that "there are basic principles that are universal; there are certain truths which are self-evident – and the United States of America will never waver in our efforts to stand up for the right of people everywhere to determine their own destiny."[12]

To the extent that supporting Internet freedom advances America's democracy-promotion agenda, the rationale for promoting online freedom is clear. However, cause and effect are *not* perfectly clear and the United States must choose its policies under conditions of uncertainty. Both the Bush and Obama administrations have wagered that by promoting global Internet freedom the United States will not only operate according to universal values but will promote tools that may, on balance, benefit societies over the autocrats that oppress them. Secretary of State Hillary Rodham Clinton urged countries to "join us in the bet we have made, a bet that an open Internet will lead to stronger, more prosperous countries."[13] Given the evidence we discuss throughout this report, this bet is one worth making.

Yet promoting Internet freedom inevitably requires the U.S. government to make tradeoffs with other national security and economic interests – a perennial challenge for a government pursuing competing priorities. After all, it is easier to support Internet freedom in countries in which the United States discerns few overarching strategic and economic interests than in countries where the United States has a robust and complex agenda.

Consider China, for example. China engages in widespread Internet repression and hosts the world's largest population of online users. But promoting Internet freedom there complicates American efforts to win Beijing's support on an array of other issues, ranging from North Korea to Iran. And strengthening controls over the sale of American technologies to China could mean shutting U.S. companies out of the world's largest Internet market at a time when the American economy is still recovering from the recent financial crisis.

The United States should promote Internet freedom abroad, but this policy does incur costs. Funding for Internet freedom programs uses scarce dollars. The Internet can empower violent radicals as well as peaceful reformers. There is no guarantee that supporting Internet freedom will enhance freedom or lead to greater democracy. Yet it is virtually certain that if the United States ceases its Internet freedom-related activities, the balance of online power would shift toward autocracies seeking to restrict their populations' freedom. This alone should compel American officials to take Internet freedom seriously.

A Brief History of the U.S. Government's Internet Freedom Efforts

The U.S. government started pursuing an Internet freedom agenda during the second term of the George W. Bush administration. Congress began scrutinizing Internet freedom issues in 2005, focusing particularly on the private sector. Reports that a local Yahoo affiliate gave the email records of a journalist to Chinese authorities, which led to his 10-year prison sentence, prompted congressional hearings that also included Microsoft and Google.[14] The same year, Congressman Chris Smith, R-N.J., introduced the first version of his Global Internet Freedom Act, which would prohibit exporting certain hardware and software to repressive regimes.[15] In 2008, representatives from Cisco Systems, Inc. were asked to appear before the Senate Judiciary Committee to determine if the company knowingly sold routers to China for the purpose of controlling political dissent and strengthening the state's Great Firewall.[16] The Yahoo incident, together with Cisco's sales and Google's agreement to censor its search results in China, generated a larger discussion on Capitol Hill about whether the government should prohibit American technology companies from responding to politically motivated information requests or selling technology that could help governments commit human rights violations. After the so-called Twitter revolution in Iran in 2009, Congress passed the Victims of Iranian Censorship (VOICE) Act, which authorized (but did not appropriate) 55 million dollars for State Department programs that would help the Iranian people overcome electronic censorship and digital oppression.[17]

The executive branch has also been increasingly active. In February 2006, then-Secretary of State Condoleezza Rice established the Global Internet Freedom Task Force (GIFT) as a way to coordinate State Department efforts to promote Internet freedom and respond to Internet censorship.[18] Soon thereafter, then-Under Secretary of State for

Democracy and Global Affairs Paula Dobriansky announced that the State Department would henceforth include a country-level assessment of Internet freedom in its annual human rights reports.

Like its predecessor, the Obama administration's Internet freedom agenda goes well beyond funding firewall-evading technology. The State Department has bolstered its capacity to use its diplomatic, economic and technological resources to promote a free Internet. Clinton has established a team of experts, including a senior advisor for innovation, to develop creative ways to blend technology with traditional diplomatic and development efforts. In addition, the State Department re-launched its Internet freedom task force in 2010, rebranding it the "NetFreedom" Taskforce, and established a Coordinator for Cyber Issues in early 2011. The White House established a deputy chief technology officer for Internet policy within the Office of Science and Technology Policy (OSTP) to coordinate government-wide Internet and technology policy, including issues related to cyber security and Internet freedom.

Clinton has led efforts to promote Internet freedom in the Obama administration. Evoking President Franklin Delano Roosevelt's 1941 Four Freedoms speech, in 2010 Clinton added a fifth, the "freedom to connect – the idea that governments should not prevent people from connecting to the Internet, to websites or to each other."[19] In a second speech a year later, she pledged America's "global commitment to Internet freedom, to protect human rights online as we do offline," including the freedoms of expression, assembly and association.[20]

These speeches represent the clearest and most complete articulation of the U.S. government's Internet freedom strategy, but questions remain. For example, does the government aim to promote the online freedoms of expression, assembly and association as intrinsic goods, regardless of whether their exercise engenders democratic change offline? Or does the U.S. government believe that, on balance, a freer Internet will promote democratic political change? The administration still lacks a clear message for precisely *why* it is undertaking efforts to promote online freedom in the first place, which has produced confusion about its overall approach to Internet freedom.

Crafting the Message

In her 2011 speech, Clinton said, "There is a debate currently under way in some circles about whether the Internet is a force for liberation or repression. But I think that debate is largely beside the point."[21] In fact, that is the key point – if the Internet is a force for repression, why should the United States support its freer use?

Administration officials emphasize that their policies support freedom of the Internet, not freedom via the Internet; these policies are not part of a broader democracy-promotion strategy. In her 45-minute speech, Clinton used the term "democracy" just once, when defending the administration's position on WikiLeaks. Instead, she said that the United States supports a free Internet because it helps build "strong" and "prosperous" states. She did not say that the Internet helps build freer or more democratic states.[22] Yet that is a key reason why the administration supports Internet freedom. It is the central motivation behind the State Department's training and technology programs, which are aimed at online activists, dissidents and democracy-related NGOs.

The U.S. government should clearly state why it promotes Internet freedom: Doing so accords with America's longstanding tradition of promoting human rights, including freedoms of expression, association and assembly, and the United States is betting that access to an open Internet can foster elements of democracy in autocratic states. Officials can acknowledge the potential downsides, but they need not shy from publicly acknowledging the U.S. interest in democratization and the hope that promoting Internet freedom can assist those who are pressing for liberal change abroad. The government should not discredit dissidents by suggesting that they are an arm of U.S. foreign policy, but refraining entirely from mentioning democracy in connection with Internet freedom risks undermining domestic support for its policies – including on Capitol Hill. And the current rhetorical ambivalence belies the increasingly robust – indeed, increasingly impressive – U.S. efforts to promote Internet freedom.

At the same time, the United States should counter the view that Internet freedom is merely an American project cooked up in Washington, rather than a notion rooted in universal human rights. The United States promotes Internet freedom more actively than any other country, and is one of the only countries that actively funds circumvention technologies. It leads in promoting international norms and has made a greater effort than most to incorporate Internet freedom into its broader foreign policy. This has provoked concerns that American advocacy will taint the efforts of local activists. For example, Sami ben Gharbia, a prominent Netherlands-based Tunisian blogger, has said, "Many people outside of the U.S., not only in the Arab world, have a strong feeling that the Internet Freedom mantra emitting from Washington D.C. is just a cover for strategic geopolitical agendas" and that this could threaten activists who accept support and funding.[23] Autocratic governments routinely denounce Internet freedom-related activities as imposing American values, and some technology companies and foundations have shied away from supporting circumvention and anonymity technologies because of their perceived tie to U.S. foreign policy.

The response to such concerns should not be to avoid any suggestion that Internet freedom is related to American support of democracy and human rights, but rather to internationalize the effort. Despite reservations from some, more than 5,000 foreign activists and others have accepted Internet-related training funded by the State Department, and many more employ U.S. government-funded technology. [24] Many governments have not yet formulated policies in this area, but some are expressing growing interest in doing so, including several European countries and the EU. To the extent that foreign governments advocate for Internet freedom and foreign corporations join such efforts as the GNI and international organizations promote new norms, the United States will be able to make a stronger argument that Internet freedom is truly a global effort.

III. INTERNET FREEDOM AND POLITICAL CHANGE

The Internet's potential as a tool for political change captivated top foreign policy officials in 2009 during what was quickly dubbed Iran's Twitter Revolution. The new awareness grew as protestors used the Internet and text messages to spread information and coordinate efforts, and was crystallized by the viral movement of a video depicting the brutal slaying of a young Iranian student, Neda Agha-Soltan. The video, which was captured on a mobile phone and uploaded to YouTube, traveled across the Web and onto local and satellite television, prompting Obama to express his outrage at the killing. When the president of the United States uses a White House press conference to address material uploaded to YouTube, something fundamental has changed in the nature of modern communications.

The focus on Internet freedom grew as the Arab Spring gathered momentum a year and a half later. The wave of revolts across the Arab world, beginning in Tunisia, then sweeping across Egypt and into Libya, Bahrain, Yemen, Syria and elsewhere were fueled in part by activists using tools such as Facebook, Twitter, SMS (text messaging) and other platforms. Several regimes took draconian steps to stop online organizing and communication. The sense grew that the Internet mattered, but just *how* it mattered was not totally clear.

In a sense, the Internet represents just the latest part of a story that has unfolded for centuries. Communication technologies have played significant roles in political movements since antiquity, from the printing press that empowered the Reformation, cassette tapes distributed by Iranian revolutionaries in 1979, to fax machines used by Poland's Solidarity movement and satellite television today. But the global nature of the Internet, its very low barrier to entry, its speed and the degree to which it empowers the individual all make it qualitatively different from earlier technologies. The Internet itself has become the focus of attention by dictators, democracy activists and observers around the world.

Does Internet Freedom Lead to Democracy?

The United States promotes Internet freedom because Americans believe in the freedom of expression, in any medium. The country also promotes it because American leaders have bet that, on balance, the increased availability of new, unfettered communications technologies abets the spread of democracy. But does it?

Here we use the term "democracy" to mean a political system that is transparent and accountable to the public through free and fair elections; includes active political participation by the citizenry; protects human rights; and maintains a rule of law that is fair to all citizens.[25] This is obviously an ideal, and democratic systems exhibit many variations, but this definition offers a useful standard for measuring potential progress.

Experts remain deeply divided, as shown in the text box on the following page, as to whether unbridled access to the Internet can help transform authoritarian regimes over time and bring greater freedom to once-closed societies. Most attempts to assess its impact rely on case studies, anecdotes or theory. The novelty of the phenomenon and the few and widely varying data points pose notable analytical challenges, and assessments require a certain amount of subjective interpretation. Facebook clearly played a major role in building an opposition to the Hosni Mubarak regime in Egypt and in organizing protests. But after the government shut off the Internet, protests became bigger, not smaller. So did this demonstrate the Internet's limited role as a tool of agitation? Or did the shutoff of cherished online tools itself spur enraged citizens to demonstrate instead of staying home (possibly in front of a computer)?

Does the Internet Promote Democracy?

OPTIMISTS

"The Internet is above all the most fantastic means of breaking down the walls that close us off from one another. For the oppressed peoples of the world, the Internet provides power beyond their wildest hopes."[26]

Bernard Kouchner
Former French Foreign Minister

"It does make a difference when people inside closed regimes get access to information – which is why dictatorships make such efforts to block comprehensive Internet access … [promoting Internet freedom] would be a cheap and effective way of standing with Iranians while chipping away at the 21st-century walls of dictatorship."[27]

Nicholas Kristof
The New York Times *columnist*

"The Internet is possibly one of the greatest tools for democratization and individual freedom that we've ever seen."[28]

Condoleezza Rice
Former Secretary of State

"Without Twitter, the people of Iran would not have felt empowered and confident to stand up for freedom and democracy."[29]

Mark Pfeifle
Former Deputy National Security Advisor

"If you want to liberate a society, just give them the Internet."[30]

Wael Ghonim
Egyptian Google Executive
and democracy activist

SKEPTICS

"The idea that the Internet favors the oppressed rather than the oppressor is marred by what I call cyber-utopianism: a naïve belief in the emancipatory nature of online communication that rests on a stubborn refusal to admit its downside."[31]

Evgeny Morozov
Author of The Net Delusion

"The platforms of social media are built around weak ties … weak ties seldom lead to high-risk activism."[32]

Malcolm Gladwell
The New Yorker *staff writer*

"Democracy isn't just a tweet away."[33]

Jeffrey Gedmin
Former President of Radio Free Europe/Radio Liberty

"It is time to get Twitter's role in the events in Iran right. Simply put: There was no Twitter Revolution inside Iran."[34]

Golnaz Esfandiari
Senior Correspondent for Radio Free Europe/Radio Liberty

"Techno-optimists appear to ignore the fact that these tools are value neutral; there is nothing inherently pro-democratic about them. To use them is to exercise a form of freedom, but it is not necessarily a freedom that promotes the freedom of others."[35]

Ian Bremmer
President of the Eurasia Group

It has become axiomatic to say that the Internet does not itself create democracies or overthrow regimes; people do. This is obviously true, but if new communications tools do matter – and there appears to be at least nascent evidence that they do – then they can play a role in several distinct ways. An important report issued by the United States Institute of Peace (USIP) presented a useful framework for examining how new communications technologies might affect political action. The paper identifies five distinct mechanisms through which the Internet might promote (or be used by regimes to block) democratic progress.[36] Here we deepen the analysis of these mechanisms and add two additional factors that affect them.

The Internet may affect **individuals**, by altering or reinforcing their political attitudes, making them more attuned to political events, and enabling them to participate in politics to a greater degree than they could otherwise. This does not automatically translate into a more activist population; as the USIP study notes, it could actually make citizens more passive by diverting their attention away from offline political activism and toward less significant online activity.[37] Some have called this "slacktivism," exemplified by the millions of individuals who signed online petitions to end genocide in Darfur but who took no further action.[38] At the same time, individuals freely expressing themselves on the Internet are exercising a basic democratic right. As democracy scholar Larry Diamond points out, used in this way, the Internet can help "widen the public sphere, creating a more pluralistic and autonomous arena of news, commentary and information."[39] It can also serve as an instrument through which individuals can push for transparency and government accountability, both of which are hallmarks of mature democracies.[40]

New media might also affect **intergroup relations**, by generating new connections among individuals, spreading information and bringing together people and groups. (Some have worried about the opposite effect – the tendency of the Internet to polarize individuals and groups around particular ideological tendencies.)[41] This may occur not only within countries, but also among them; the protests in Tunisia sparked a clear rise in political consciousness and activism across the Arab world – much of it facilitated by Internet-based communications and satellite television.[42] It may also take place over a long period of time; Clay Shirky, an expert at New York University, argues that a "densifying of the public sphere" may need to occur before an uprising turns into a revolution.[43]

New communications technologies could also affect **collective action**, by helping change opinion and making it easier for individuals and groups to organize protests in repressive countries. Unconnected individuals dissatisfied with the prevailing politics may realize that others share their views, which might form the basis for collective action.[44] Relatively small groups, elites or other motivated dissidents might use the Internet to communicate or organize protests. Even if the number of committed online activists is small, they might nevertheless disseminate information to the general population or inspire more widespread protests.[45] Again, it is important to distinguish such action from group "slacktivism;" as the successful protests in Egypt showed, the regime only began to teeter when thousands of citizens physically occupied Tahrir Square. Though initial protests may have been organized via Facebook, the Mubarak government would still be in power if the protests had been confined only to cyberspace.

These new technologies clearly affect **regime policies** as well. Governments have employed a huge array of techniques aimed at controlling the Internet and ensuring that their political opponents cannot use it freely. This goes well beyond censorship, which garners the bulk of popular attention. Autocracies also regularly monitor dissident communications; mobilize regime defenders; spread propaganda and false information designed to disrupt protests and outside groups; infiltrate social movements; and disable dissident websites, communications tools and databases. These and other practices can also induce self-censorship and other forms of self-restraint by publishers, activists, online commentators and opposition politicians.

Autocrats can also turn dissidents' use of the Internet against them. In Iran, for example, users of social media – which linked their accounts to those of other protestors – inadvertently created a virtual catalogue of political opponents that enabled the government to identify and persecute individuals. The regime established a website that published photos of protestors and used crowd sourcing to identify the individuals' names.[46]

Similarly, the Revolutionary Guard reportedly sent intimidating messages to those who posted pro-opposition messages and forced some citizens entering the country to open their Facebook accounts upon arrival.[47] In the midst of the Arab protests, Syria allowed its citizens to access Facebook and YouTube for the first time in three years. Some human rights activists suspected that the government made the change precisely in order to monitor people and activities on these sites.[48]

Similarly, shortly after the Egyptian government lifted its Internet blackout in early 2011, pro-Mubarak supporters disrupted planned demonstrations by posting messages on Facebook and Twitter saying that the protests had been canceled.[49] The government reportedly sent Facebook messages to citizens urging them not to attend protests because doing so would harm the Egyptian economy.[50] In the same vein, the Chinese government employs an estimated 250,000 "50 Cent Party" members who are paid a small sum each time they post a pro-government message online.[51] And after an anonymous post on the U.S.-based Chinese language website Boxun.com called on activists to stage China's own "Jasmine Revolution," no demonstrators turned up at the rally point – but it was flooded with security teams and plainclothes officers.[52] Some speculated that Chinese officials themselves may have authored the anonymous posting in an effort to draw out political dissidents.[53] While no evidence has emerged to support the claim, it is not hard to imagine such an attempt taking place in the future.

Autocracies are engaged in "offline" attempts to repress Internet use, as well. Saudi Arabia, for example, has not only blocked websites but also placed hidden cameras in Internet cafes aimed at monitoring user behavior and required cafe owners to give their customer lists to government officials.[54] China requires users to register their identification upon entry to a cybercafe.[55] And Libyan officials simply demanded that refugees fleeing the recent fighting turn over their cellphones or SIM cards at border checkpoints.[56]

Beyond these effects, new media can affect **external attention**, by transmitting images and information to the outside world, beyond the control of government-run media and regime censorship and spin. Such attention can mobilize sympathy for protestors or hostility toward repressive regimes,[57] as occurred when the video of Neda Agha-Soltan moved from YouTube to mainstream media. Digital videos and information may also have a rebound effect; information transmitted out of Egypt and Libya by social networking and video-hosting sites during the protests in those countries made its way back in via widely watched satellite broadcasts. This effect could be particularly pronounced in countries like Yemen, where Internet penetration is low but Al Jazeera is widely viewed. Similarly, print journalists have found sources and stories through social media and have used the same media to push their articles out to the world.

In addition to the five mechanisms laid out by USIP and noted above, we observe two additional factors that affect them in various ways.

The **economic impact** of the Internet might affect the degree of democratization in a country. The Internet has increased labor productivity and corresponding economic growth, which may help middle classes emerge in developing countries.[58] Because new middle classes tend to agitate for democratic rights, new technologies could indirectly promote democratization. In 2011, Clinton referenced a related dynamic, the "dictator's dilemma," stating that autocrats "will have to choose between letting the walls fall or paying the price to keep them standing … by resorting to greater oppression and enduring the escalating opportunity cost of missing out on the ideas that have been blocked and people who have been disappeared."[59] In other words, an autocrat can either repress the Internet or enjoy its full economic benefits, but not both.

Whether the "dictator's dilemma" actually exists remains unknown. There are certainly clear individual instances where Internet repression has damaged a nation's economy; Experts from the Organisation for Economic Co-operation and Development (OECD) have estimated that Egypt's five-day Internet shutdown cost the country at least 90 million dollars, a figure that does not include e-commerce, tourism or other businesses that rely on Internet connectivity.[60] But China seems to provide a powerful counterexample since it severely represses the Internet while enjoying extraordinarily high rates of sustained economic growth. Indeed, China appears to have used its restrictive Internet practices to squeeze out international competition and generate conditions where only domestic companies – ones that adhere to the government's stringent censorship and monitoring practices – can thrive. China's largest domestic search engine, Baidu, exercises strict controls on content but has thrived since Google pulled out of China in January 2010. China may be an outlier; the massive financial and human resources it devotes to online control may not be replicable elsewhere. Other countries may be left with blunter forms of repression that degrade both the Internet's economic and political effects.

In addition to the political and economic effects described above, **new technologies can accelerate** each of them. Google's Eric Schmidt and Jared Cohen have argued that faster computer power combined with the "many to many" geometry of social media empowers individuals and groups at the expense of governments and that this, in turn, increases the rate of change.[61] Dissidents can identify one another, share information, organize and connect with leaders and with external actors, all easier and faster than ever before.[62] Indeed, one hallmark of the 2011 Arab Spring was the astonishing rate of change as popular protests threatened or toppled governments that had been in power for decades in a matter of weeks.[63]

Again, the local political context is critical. The medium may be global, but whether and how it enables individuals to foster democratic change largely depends on a wide array of local variables, including opposition leadership, the existence of civil society institutions, the willingness of the regime to crack down on dissident activity, and so forth. In Tunisia and Egypt for example, tens of thousands of protestors responded to protest event pages on Facebook by taking to the streets. Yet in other Arab states, a call on Facebook for a "day of rage" did not have the same pronounced influence. The degree of openness in the local political system, the discontent among the population, the willingness of the government to use coercive means to stop democratic activism, the role of minorities and other local factors all matter greatly.

> *Experts from the Organisation for Economic Co-operation and Development have estimated that Egypt's five-day Internet shutdown cost the country at least 90 million dollars, a figure that does not include e-commerce, tourism or other businesses that rely on Internet connectivity.*

The Internet does not automatically promote democratization; Iran's Twitter revolution led to no reforms while Egypt's Facebook revolution toppled the Mubarak regime. Furthermore, the technology itself is agnostic; the same online tools that empower dissidents can aid dictators in their oppression. In the short run, at least, a freer Internet does not automatically translate into more liberal political systems.

Yet some case studies do demonstrate the Internet's profound potential: that access to an open Internet can help countries slide away from authoritarianism and toward democracy. Events in Iran, Tunisia, Egypt and elsewhere suggest that the Internet and related technologies (such as SMS) have indeed served as critical tools for organizing protests, spreading information among dissident parties and transmitting images and information to the outside world – some of which moved onto satellite television channels, further boosting their influence.[64] And while experts continue to argue about the precise effect, they tend to agree that social media tools have made revolutions in the Middle East easier and speedier than they would have otherwise been.[65]

Perhaps the most compelling link between a free Internet and democratization is also the simplest: Both dissidents and dictatorships abroad seem to believe that the Internet can have a transformative role, and they act on that basis. Dictatorships expend enormous time and resources to clamp down on online activity, and more than 40 countries actively censor the Internet or engage in other forms of significant Internet repression.[66] Meanwhile, millions of individuals use proxy servers and other circumvention and anonymity tools to evade censorship and monitoring. During the 2009 presidential campaign in Iran, for example, both President Mahmoud Ahmadinejad and his opponent, Mir-Hussein Mousavi, cited the Internet as a tool through which the liberal opposition could mobilize support.[67] It is unlikely they were both wrong. While the effect of the Internet will depend on local conditions, there are indeed reasonable grounds for believing that a free Internet can help empower individuals to press for more liberal political systems.

IV. HOW THE U.S. GOVERNMENT PROMOTES INTERNET FREEDOM

The U.S. government promotes Internet freedom in five main ways: providing Internet technologies, shaping international norms, encouraging the private sector to expand its role, using economic diplomacy and reforming export controls.

Providing Internet Technologies

As autocracies attempt to censor, identify, intimidate and monitor online users, the U.S. government provides technologies that allow individuals living in repressive environments to freely access online information. The U.S. government funds these technologies because, at present, the marketplace is highly unlikely to supply them on its own. The private sector has few financial incentives to do so – it is difficult to charge anonymous subscribers or sell ads in closed societies – and very few foreign governments, NGOs or foundations have funded them to date.

A variety of circumvention technologies enable dissidents to penetrate firewalls and access blocked websites and censored information. Each tool employs the same basic method: It routes a user's request through an unblocked webpage in order to access banned content. For instance, a user in China who cannot access *The New York Times* website could instead reach a proxy site that could then obtain information from the *Times* website.

Freegate and Ultrasurf, for example, were designed to circumvent China's Great Firewall by taking advantage of open proxies – proxy servers available to anyone on the Internet – which serve as a forwarding service to bypass restrictive firewalls. Though Freegate and Ultrasurf, both of which have received U.S. government funding, were designed for use in China, some users are located in other countries, including Iran.[68]

Psiphon is another circumvention tool that relies on a worldwide network of servers to enable

The Role of the Internet in Political Movements: A Brief History

By Jacqueline Koo,
Joseph S. Nye, Jr. Intern

The 2009 Green Revolution in Iran and the 2011 Arab Spring represented watershed events for many foreign policy makers who are only beginning to grapple with issues surrounding Internet freedom. Yet using new communications technologies as a tool for political transformation began over a decade ago. Numerous examples demonstrate how Internet and mobile phone technology can be used to facilitate protests and even revolution in countries around the world. Some succeeded in bringing about change, while others did not.

In January 2001, while **Philippine** President Joseph Estrada was on trial for impeachment, thousands of Filipinos protested the unwillingness of loyalist senators to present the evidence against him. The protests were partly organized by text messaging – some seven million messages were sent during the week of the trial – which helped assemble over one million protesters at a major crossroad in Manila. Startled by the protests, the senators reversed the decision and released the evidence, resulting in Estrada's impeachment.[69]

In fall 2004, a series of popular uprisings that became known as the Orange Revolution in **Ukraine** were largely shaped by pro-democracy activists using the Internet to protest a fraudulent presidential election. Social activists used the Internet and text messaging on mobile phones as platforms for uncensored political dialogue and as a way to organize protests. The activists also set up election-monitoring training through pro-democracy websites, which was pivotal in helping collect evidence of the fraudulent election.[70] The street protests forced a new election that brought Viktor Yushchenko, a democratic reformer, to power.[71]

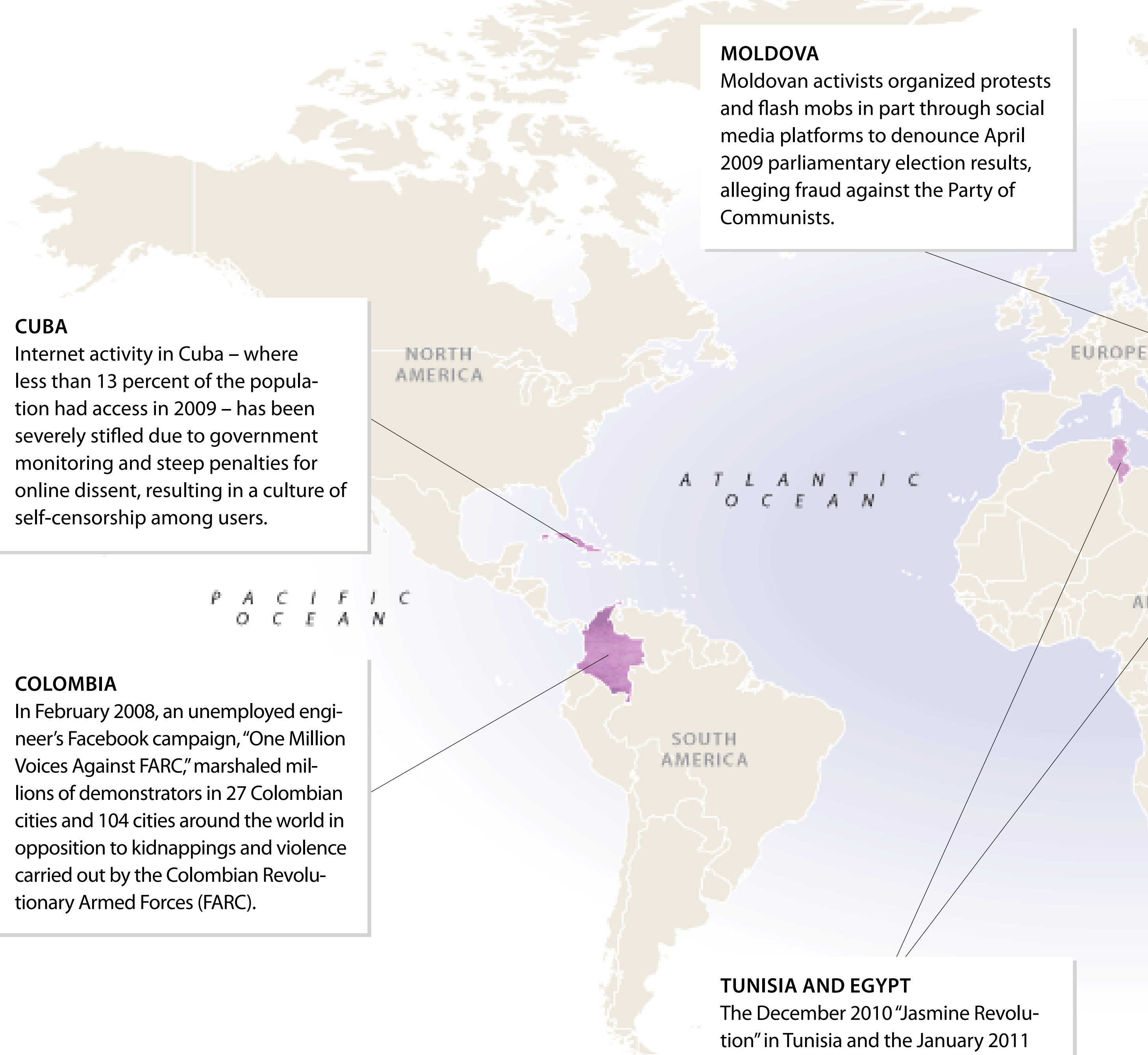
In February 2005, the assassination of former **Lebanese** Prime Minister Rafik Hariri sparked a series of anti-Syrian demonstrations, known collectively as the Cedar Revolution, that were reportedly organized via text messages and emails. The demonstrators used cellphones equipped with digital cameras to take on-the-ground pictures, which were then sent to news organizations and friends who uploaded them to websites in order to show what was happening to the rest of the world.[72] The demonstrations ultimately led to the withdrawal of all Syrian troops from Lebanon.

In February 2008, an unemployed engineer began a campaign via Facebook, "One Million Voices Against FARC," to marshal millions of protestors opposed to the violent tactics of the **Colombian** Revolutionary Armed Forces' (FARC) and its holding of some 700 hostages. The organizers utilized email, Google Docs, instant messaging systems and Skype to communicate with other organizers in other cities and with members of the Colombian diaspora abroad,[73] resulting in simultaneous demonstrations in 27 Columbian cities and 104 cities around the world.[74] The FARC has been weakened, largely through Colombian government operations, but remains the hemisphere's largest insurgent group.

In April 2008, young **Egyptian** activists protested to support a labor strike in an industrial town. The campaign was organized via Facebook and was called the "April 6 Youth Movement," after the day that the labor strike was held. In spring 2008, the Facebook group boasted over 100,000 members. The protest itself was quickly contained by security forces, which dampened the overall enthusiasm of the movement among its members.[75] Nevertheless, the online forum retained a membership of over 70,000 youth by January 2009, most of whom were not politically involved before joining the movement, and facilitated heated political dialogue among its members.

In April 2009, anti-communist activists in **Moldova** protested allegedly fraudulent parliamentary elections in which the Party of Communists won a majority of seats. The activists organized protests through a variety of social media platforms, including Twitter, LiveJournal (a popular eastern European social networking site) and Facebook. Demonstrators reportedly organized flash mobs – large, brief demonstrations assembled suddenly in a public space – by text message.[76] In response to the week-long protests, President Vladimir

THE PROMISE AND PERILS OF THE INTERNET

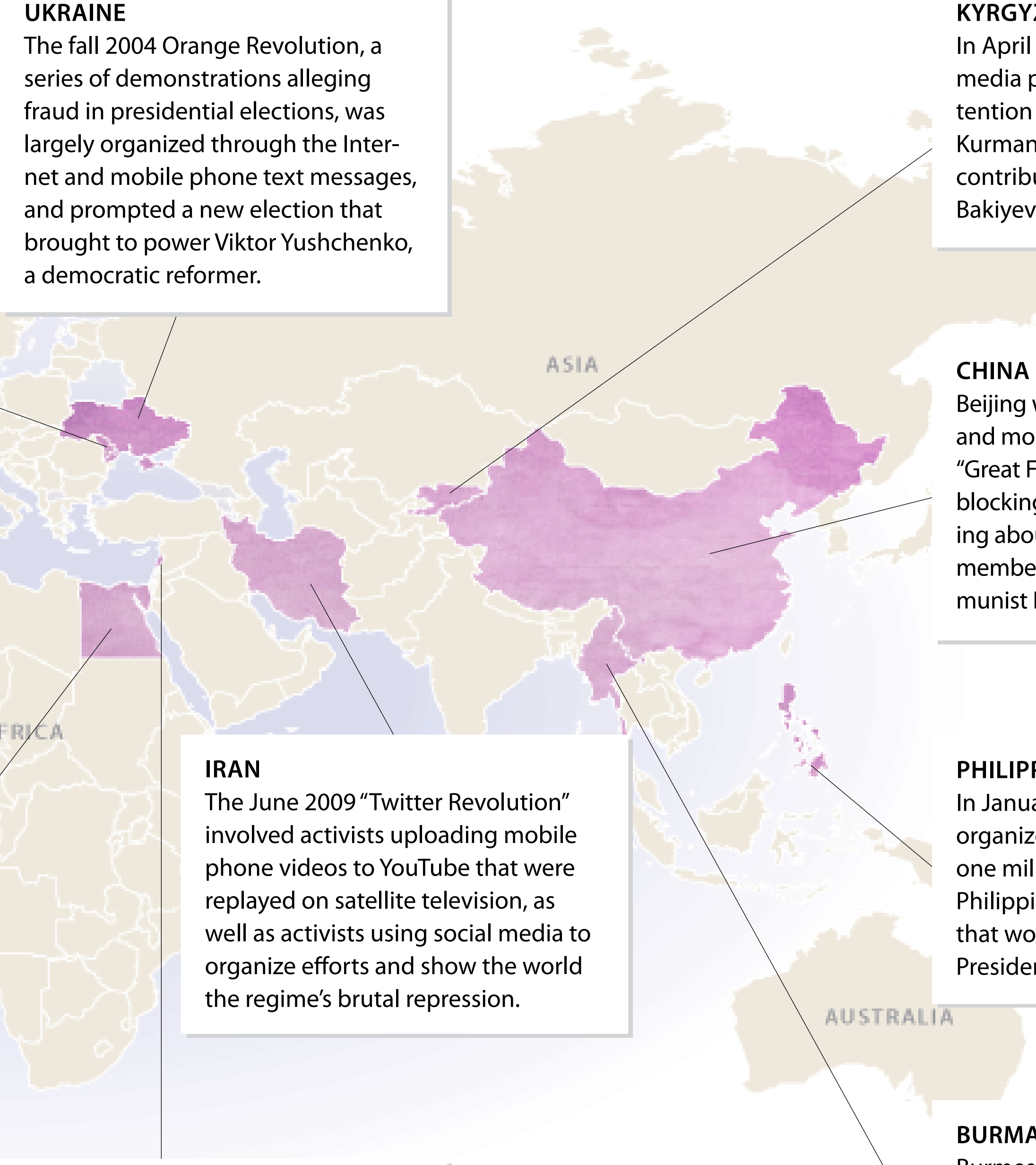


MOLDOVA
Moldovan activists organized protests and flash mobs in part through social media platforms to denounce April 2009 parliamentary election results, alleging fraud against the Party of Communists.

CUBA
Internet activity in Cuba – where less than 13 percent of the population had access in 2009 – has been severely stifled due to government monitoring and steep penalties for online dissent, resulting in a culture of self-censorship among users.

COLOMBIA
In February 2008, an unemployed engineer's Facebook campaign, "One Million Voices Against FARC," marshaled millions of demonstrators in 27 Colombian cities and 104 cities around the world in opposition to kidnappings and violence carried out by the Colombian Revolutionary Armed Forces (FARC).

TUNISIA AND EGYPT
The December 2010 "Jasmine Revolution" in Tunisia and the January 2011 revolution in Egypt witnessed activists employing Facebook and other social media platforms to organize demonstrations against authoritarian rule.



UKRAINE
The fall 2004 Orange Revolution, a series of demonstrations alleging fraud in presidential elections, was largely organized through the Internet and mobile phone text messages, and prompted a new election that brought to power Viktor Yushchenko, a democratic reformer.

KYRGYZSTAN
In April 2010, Twitter and other social media platforms helped bring attention to protests against President Kurmanbek Bakiyev's administration, contributing to pressure for President Bakiyev's resignation.

CHINA
Beijing wields one the world's largest and most sophisticated systems – the "Great Firewall" – for filtering and blocking Internet traffic, while employing about 250,000 "Fifty Cent Party" members who post pro-Chinese Communist Party propaganda online.

IRAN
The June 2009 "Twitter Revolution" involved activists uploading mobile phone videos to YouTube that were replayed on satellite television, as well as activists using social media to organize efforts and show the world the regime's brutal repression.

PHILIPPINES
In January 2001, text message-organized protests brought together one million demonstrators urging the Philippine Senate to release evidence that would later be used to impeach President Joseph Estrada.

BURMA
Burmese cyber dissidents have used the Internet to upload videos of anti-government demonstrations and, as during the 2007 Saffron Revolution, have been known to send digital files across the border to be uploaded from foreign computers.

LEBANON
In February 2006, following the assassination of former Lebanese Prime Minister Rafik Hariri, anti-Syrian demonstrations, organized in part by text messages and emails, ultimately led to the withdrawal of all Syrian troops from Lebanon.

Voronin called for a recount, and the electoral commission found no evidence of fraud. The Party of Communists proceeded to take the majority of seats in Parliament but, weakened by the protests, failed to elect a prime minister.[77] The president dissolved Parliament three months later.

In June 2009, supporters of the opposition candidate, Mir-Hossein Mousavi, staged massive protests challenging the results of the **Iranian** presidential election that named the incumbent President Mahmoud Ahmadinejad the winner. The protests known as the Green Revolution were also nicknamed the "Twitter Revolution" for the role that Twitter and other Internet-based social networking sites reportedly played in facilitating communication within Iran and with the rest of the world. The demonstrations were put down with brutal force and the revolution failed.

In April 2010, a series of riots and demonstrations took place in **Kyrgyzstan** stemming from dissatisfaction and anger against President Kurmanbek Bakiyev's administration. Observers have offered differing perspectives on the role social media played during the Kyrgyz protests (with some, for instance, arguing that platforms such as Twitter were more effective in broadcasting the demonstrations than in organizing them).[78] A general consensus exists, however, that Twitter and other social media platforms helped bring attention to the revolt and contributed to mounting pressure for Bakiyev to step down.

In December 2010, **Tunisians** took to the streets protesting high unemployment, high food prices, corruption and the lack of freedom of speech, and called for President Zine el-Abidine Ben Ali to step down. These protests were dubbed the "Jasmine Revolution," but were also called the "Facebook Revolution."[79] The protests were spearheaded by a number of young bloggers that employed Facebook, Twitter, blogging sites and email to organize protests nation-wide.[80] On January 14, 2011, after 28 days of protests, Ben Ali dissolved the Parliament and then resigned, ending his 23-year rule.

In January 2011, **Egyptians** took part in peaceful mass demonstrations and strikes calling for President Hosni Mubarak to step down, actions that escalated into violent clashes with the police. The protests were organized through the "We Are All Khaled Said" Facebook page, named after a young blogger who was beaten to death by police in June 2010, and whose death fueled the outrage surrounding the initial revolts.[81] Over 2 million people protested in Cairo's Tahrir Square and protests were held in several other major Egyptian cities.[82] Observing the protestors' use of social media, the Mubarak regime shut down nearly all Internet and cellphone service within the country for five days.[83] The shutdown backfired – the protests grew enormously and the move prompted both international condemnation and domestic outrage.[84] On February 11, Mubarak stepped down after 30 years of power and handed control to military leaders.

As of this writing, mass protests continue in countries across the Middle East. The role of the Internet in influencing and facilitating these demonstrations varies by country, and the extent to which the protests will ultimately cause political change remains unclear. However, these examples show that the Internet gives activists in closed societies tools through which to express dissent and unite individuals at an unprecedented pace and scale, and will undoubtedly serve as a tool for political action – among both protestors and the regimes they oppose – for the foreseeable future.

restricted users to reroute their requests around firewalls. While these tools allow users to puncture firewalls, they do not provide absolute anonymity. Users may still be exposed to state surveillance practices, especially in countries where Internet service providers are required to retain data on user activity – a virtual paper trail of what websites each user has visited.[85] They have another drawback as well: They cannot access content within a country that censors.

Other technologies help users maintain their anonymity in the face of a regime's watchful eye. The Tor Project, which received nearly 750,000 dollars from the U.S. government between 2006 and 2010, has developed one notable tool.[86] Tor uses a network in which encrypted messages pass through several network nodes known as "onion routers" that then peel away layers of encryption as information is transmitted among proxy servers around the world. The network allows users to hide their location from websites they are visiting, enabling them to evade governments and others attempting to trace their location. For example, a Tor user in Iran might appear as on a website registry as a user in Germany if the last proxy server used were located in Germany. In addition, virtual private networks (VPNs) encrypt and tunnel all Internet traffic through a proxy, enabling their users to circumvent firewalls and use webmail, chat and other online communication services.[87] Most VPNs are available for a nominal subscription fee. One popular VPN, Hotspot Shield, uses ads in lieu of a fee, allowing users to subscribe to the service for free.

Other technological tools enhance the ability of dissidents and activists to use the Internet freely. Software exists to help protect websites against DDoS attacks, which can be launched by autocratic regimes or patriotic hackers (individuals or groups who express nationalistic pride by attacking foreign government or dissident websites) by sending millions of page requests per second to a site, thereby overloading and crashing its servers. Other available tools help secure online databases (of human rights abuses, for example), provide mirror sites to keep websites live during an attack and archive uploaded data so that it can be easily reposted after a website returns to service. In addition, as mobile technology increasingly becomes a main platform for online activity, there is greater interest in secure cellphones and encrypted mobile communications. In a positive move, the State Department is supporting the development of an innovative application that would allow pro-democracy activists to hit a "panic button" before their mobile phones are confiscated, erasing their address book and sending emergency alerts to other campaigners.[88]

Yet such tools cannot be used effectively by activists who lack the skills to employ them, and they can actually be dangerous. Used improperly, they may give users a false sense of security or expose their users identities and online actions to authorities. As with other elements of American human rights advocacy, only individuals on the ground can calculate their personal risks and decide which are worth taking. However, the United States has a responsibility to ensure that users of technologies it funds make decisions that are as fully informed as possible. It also has a responsibility to ensure that the tools it supports work as advertised. This requires, in part, subjecting any U.S. government-funded circumvention technologies to rigorous analysis before they are deployed to ensure they do not contain vulnerabilities that could be exploited by authoritarian regimes. To do otherwise potentially subjects dissidents to grave threat. (See "The Dilemmas of Digital Technology" text box.)

Properly using new technologies must also continue to be part of the substantial training programs funded by the U.S. government. Some of this training focuses on building the online resilience of activist organizations, to help them respond when they are victims of an attack and to reboot their systems in a timely fashion. Other

The Dilemmas of Digital Technology: The Cases of Haystack and Freegate

A key element of the U.S. government's Internet freedom agenda involves providing circumvention and anonymity technologies to cyber dissidents in closed societies. However, each of these technologies poses an array of technical and political dilemmas. While such tools can be highly effective in helping individuals living under dictatorship access the uncensored Internet, determining just how to do so can be very difficult indeed. Two technologies – Haystack and Freegate – demonstrate these dilemmas. The former shows the vital importance of ensuring that a digital tool works as advertised; the latter illustrates the diplomatic tensions that result from supporting these technologies.

HAYSTACK

In June 2009, in the midst of widespread protests in Iran, Austin Heap, a 25-year old software engineer in San Francisco, announced that he had developed a circumvention tool called Haystack that would help Iranian dissidents evade their government's draconian Internet censorship filters. "It's completely secure for the user so the government can't snoop on them," Heap said. "We use many anonymizing steps so that identities are masked and it is as safe as possible so people have a safe way to communicate with the world."[89]

Haystack quickly became a sensation in the mainstream media and Heap even received *the Guardian's* "Innovator of the Year Award."[90] Haystack caught the eye of the State Department, and in March 2010 the Treasury Department issued a license to distribute the software in Iran.[91] Yet while Heap touted the software's strong security features, the technology did not undergo rigorous technical testing or peer review and, as a result, it went live in summer 2010 with serious design flaws.[92]

An independent team cracked Haystack's code within six hours of its public release and determined that the government of Iran would have been able to discern users' location and identities.[93] As a result, the Haystack program was disbanded in September 2010. As the U.S. government increases its funding for circumvention and anonymity technologies, it must subject them to rigorous technical review and independent evaluation – including by outside experts when necessary – before they are deployed. To do otherwise risks not only wasting taxpayer dollars, but also putting dissidents and activists at risk.

FREEGATE

Freegate shows the challenges of balancing Internet freedom efforts with broader foreign policy priorities. Freegate is a censorship circumvention tool developed by the U.S.-based Global Internet Freedom Consortium (GIFC), an organization run by the Falun Gong, a Chinese spiritual group that Beijing labels a terrorist organization. The software is aimed at enabling users in China to puncture the regime's Great Firewall, but it has also been accessed by users in other countries; more than a million Iranian users reportedly employed it in June 2009.[94] Freegate and its sister software, Ultrasurf, also developed by the GIFC, report that they have, combined, 500,000 to 1 million monthly users.[95] In 2010, the State Department transferred 1.5 million dollars to the Broadcasting Board of Governors (BBG) to support Freegate and another GIFC tool, Ultrareach, drawing a predictably angry response from Beijing. A Chinese government spokesperson said the GIFC and Falun Gong are "bent on vilifying the Chinese government with fabricated lies, undermining Chinese social stability and sabotaging China-U.S. relations" and that the Chinese government is "strongly opposed to the U.S. government providing whatever assistance to such an anti-China organization."[96] GIFC supporters have lobbied Capitol Hill for financial support to expand its existing infrastructure, noting that GIFC had to restrict use of the software by Iranians not long after the 2009 protests subsided because of limited server capacity.

Funding groups associated with the Falun Gong poses obvious complications for U.S. relations with China. Given Beijing's deeply negative view of the spiritual group, supporting Falun Gong volunteers as they circumvent the Chinese firewall stresses the countries' complex bilateral ties. Indeed, some see the State Department's decision to fund Freegate through the BBG as an attempt to distance its diplomatic efforts from its support for GIFC-related efforts.[97] Given the high performance of these technologies and their popularity, stress on the relationship may be worth the cost to the United States, but as funding for new programming continues to increase, the government should make a concerted effort to diversify the technologies it supports.

basic technical training teaches users how to identify and verify certificate authorities and Secure Socket Layer (SSL) certificates – the pop-up boxes that verify the authenticity and security of a website – to help minimize the number of state surveillance intrusions that users inadvertently authorize. Still other programs teach basic "cyber hygiene" practices to activists who may not be technologically proficient, which include constructing strong passwords, avoiding keystroke logging in Internet cafes, preventing the inadvertent download of malicious code and using Hypertext Transfer Protocol Secure (HTTPS), which encrypts online sessions.

The State Department has spent approximately 20 million dollars since 2008 on programs to develop circumvention technologies and promote digital activism, and planned to award more than 25 million dollars in additional funding in 2011.[98] The State Department has been criticized for delays in disbursing funding for Internet-freedom related technologies. According to a congressional report, the State Department received 50 million dollars in appropriations for Internet freedom programming since Fiscal Year 2008, but had disbursed less than half by February 2011.[99] Partly as a result, in April 2011 Congress reallocated 10 million dollars from the State Department to the Broadcasting Board of Governors (BBG) – which reduced State's Internet freedom budget by a third and more than quintupled the BBG's budget in this area. Separately, the Defense Advanced Research Projects Agency (DARPA), which is part of the Department of Defense, funds the development of circumvention technologies that would allow the U.S. military to access the Internet safely and anonymously.[100]

There are good reasons for the BBG to take the lead on providing most circumvention and anonymity technologies. It is an operational entity that currently provides an array of circumvention technologies, and develops some of them in-house. Should State and the BBG both fund circumvention technologies, they will likely end up funding the same outside groups. State will, however, need to continue supporting circumvention technologies whose use falls outside the BBG's mission of promoting U.S. government-sponsored international broadcasting. State has proposed funding projects such as mobile security applications and ad-hoc mesh networking (decentralized networks that rely on individual nodes to transmit data) for use when the Internet is shut down, which include both circumvention and anonymizing components. State should also retain the lead on supporting other technologies that fall outside the BBG's mission and current technical competence, including tools to establish secure human rights databases, online hubs for censored comment, and so on.[101]

Shaping International Norms

The Bush and Obama administrations have both sought to promote Internet freedom by shaping international norms. Developing international norms is a long-term, global objective. Some countries that currently repress that Internet access – like China, Iran and Burma – are unlikely to be moved by normative trends in the near term; statements at the United Nations and policy declarations supporting Internet freedom are highly unlikely to change their current policies. But promoting Internet freedom is not only a near-term effort, and current efforts may pay off in the long run. Many countries have not yet fully developed their own Internet policies or thought through all of the implications of Internet freedom and repression even in the short run – including states in Central Asia, the Middle East and Africa. Shaping the behavior of those states should be an important goal of the United States and likeminded partners.

Rather than advocating a new international treaty or new regimes, the U.S. government has argued that the principles of Internet freedom already exist in the UDHR and the International Covenant on

Civil and Political Rights. Article 19 of the UDHR states that the right to free expression exists in any medium and on any frontier, and Article 20 protects the right of everyone to peacefully assemble and associate, a right that Clinton has argued is guaranteed in cyberspace as well.[102]

At the same time, the U.S. government has tried to codify norms that would reinforce free expression and block efforts to restrict it. The 2005 World Summit on the Information Society (WSIS), a U.N.-sponsored gathering of 174 countries, produced a consensus statement recognizing that "freedom of expression and the free flow of information, ideas and knowledge, are essential for the Information Society and beneficial to development."[103] In 2008, the member states of the International Telecommunication Union (ITU) adopted a resolution pledging to "refrain from taking any unilateral and/or discriminatory actions that could impede another Member State to access public Internet sites." According to Ambassador David Gross, then the top State Department official managing communications and information policy, the deliberations made clear that "member states" meant not only governments, but also the civilians of those countries.[104]

Continued U.S. leadership is critical to fill what remains a normative vacuum. Part of the difficulty, however, lies not only with authoritarian regimes, but also with some of America's closest democratic partners. While the U.S. government recognizes some limits on free expression – child pornography, slander, perjury, "fighting words" and certain other forms of expression are illegal, online or off – its commitment to free speech is nevertheless the strongest of any major country. Germany, for instance, prohibits Holocaust denial online; France does not allow the sale of Nazi paraphernalia over the Internet; and Turkey banned YouTube for two years because it refused to remove videos the courts deemed insulting to Mustafa Kemal Ataturk. Governments in Britain, Italy and Germany have also established lists of blocked websites – particularly those containing child pornography, online gambling or hate speech – but these lists are often neither transparent nor accountable to the public.[105]

Authoritarian countries inevitably attempt to shield themselves from criticism and pressure by pointing to democracies that ban online speech. Denying them the opportunity to do so successfully requires the United States and others to articulate, publicly and consistently, the distinction between restrictions on free speech put into place by democratic political systems through due process and those enacted by dictatorships. While Americans may disagree with the limits on online expression enforced by democratic partners, these decisions are nevertheless made through participatory political systems while restrictions imposed by autocratic regimes are not.

Defining "cyber security," and determining the legitimate steps a government may take to ensure it, also poses a significant challenge to America's Internet freedom efforts.[106] Most democratic governments use the term to mean protecting against assaults on and intrusion of cyber systems and critical infrastructure, such as electric utilities, government servers, financial systems and telecommunications networks. In contrast, some other governments argue that the term should include the notion of "information security" – regulating content. Russian officials, for example, have emphasized that information security requires balancing individual, social and state interests.[107] Such notions have real world consequences: Russia's federal security service recently proposed banning Skype, Gmail and other platforms because they are "uncontrolled" platforms that use encryption technology for secure communication.[108] The United Arab Emirates made similar claims in 2010 when it banned the use of BlackBerry services, complaining that it could not access encrypted communications.[109]

Similarly, competing definitions of aggression complicate efforts to develop Internet freedom norms. At an April 2008 U.N. conference, a senior Russian official argued that "any time a government promotes ideas on the Internet with the goal of subverting another country's government – even in the name of democratic reform – it should qualify as 'aggression.'"[110] In 2009, the six-member Shanghai Cooperation Organisation – which includes Russia and China – adopted an accord that reportedly defined "information war," in part, as an effort by a state to undermine another's "political, economic and social systems."[111]

The same tensions exist in working with American partners to combat online crime. The Additional Protocol to the European Convention on Cybercrime, for example, provides a mechanism for states to harmonize their domestic laws relating to various types of cybercrime. At first glance, this would seem precisely the kind of effort that the United States should support on security grounds. Yet the protocol requires signatories to criminalize such activities as distributing xenophobic or racist material through a computer system; expressing denial, "gross minimization" or approval of a genocide or crimes against humanity through a computer; distributing insults to people because of their race, color, religion, national or ethnic origin through a computer system; or aiding and abetting any of these acts. The Additional Protocol has been signed by Albania, Cyprus, Denmark, France, Slovenia and Switzerland. While the United States ratified the underlying convention in 2006, it has declined to join the Additional Protocol, believing it to be inconsistent with U.S. constitutional guarantees.[112]

Efforts to enlist Internet service providers and other technology companies to enforce regulations protecting copyrights and intellectual property also complicate U.S. efforts to build stronger global support for Internet freedom. Intermediaries – including Internet service providers, website hosting companies, social networking and email service providers and search engines – are increasingly pressured by states to regulate content they host. In the United States, an individual posting illegal material is generally held liable rather than the intermediary.[113] In many foreign countries intermediaries do face liability, and the process by which they are notified (by either the government or private actors) is often unclear.

The role of the private sector is the single most complicated issue facing U.S. policymakers as they forge an Internet freedom agenda.

Holding them liable in this way risks chilling free online expression. In countries like France, where Internet service providers and others are increasingly enforcing copyright regulations, hosts may self-police content and respond immediately to takedown notices, even those issued in bad faith or for unscrupulous purposes.[114] The United States and a number of other nations, including the EU, Japan and Mexico, are currently negotiating an Anti-Counterfeiting Trade Agreement that will serve as an international framework for enforcing intellectual property rights. In developing such frameworks, the United States must be very wary of moving beyond current American law. Holding intermediaries responsible could undermine the U.S. Internet freedom agenda by compelling them to err on the side of caution and to proactively censor, ban or remove even legal – let alone questionable – content.

The United States must help formulate acceptable international definitions of cyber security, aggression, cybercrime and copyright enforcement that respect the principles of Internet freedom. It will also need to continually articulate the distinction between political speech permissible under such regimes as the UDHR and truly illicit online activity. This will likely involve opposing efforts to develop restrictive international norms spearheaded by some of America's closest friends.

Enlisting Private Sector Support

The role of the private sector is the single most complicated issue facing U.S. policymakers as they forge an Internet freedom agenda. Private firms have a duty to maximize profits rather than promote online freedom in repressive environments. Yet with the prominent role their products played in Iran, Egypt, China and elsewhere, companies have been dragged into the center of the Internet freedom debate, whether they want to be there or not. Ethical debates about the proper role of the private sector – ranging from whether American companies should be permitted to sell repressive regimes key technologies to the responsibilities of corporations in the face of a regime's demand for information – remain unresolved.

The perception that American companies aid Internet repression abroad clearly makes promoting Internet freedom more difficult. This is particularly true for the most egregious activities, such as turning over the personal data of a dissident to state security services. As we discuss below, Congress should ban such activities and require more transparency into other corporate involvement, such as providing lists of banned websites. Yet nearly seven years after the initial hearings on Internet companies in China began, no legislation in this area has passed.

Both corporations and policymakers are struggling to define the appropriate role of companies in promoting Internet freedom. For example, Cisco has been accused of marketing routers in China that are used to support the Great Firewall.[115] For several years Google censored its own search results in China. More recently, the computer security firm McAfee Inc. provided content-filtering software to Internet service providers in Bahrain, Saudi Arabia and Kuwait.[116] China's Huawei is a significant supplier of filtering technology. Telecommunications giant Nokia allegedly provided the Iranian government with the capability to tap mobile phones, interrupt calls and intercept and scramble SMS text messages to disrupt organized protests.[117] France's Alcatel reportedly sold website filtering and surveillance equipment to Burma,[118] and Canada's Nortel Networks has allegedly provided censorship technology to the Chinese government.[119]

The problem is that companies must follow local laws when they operate in foreign countries, including laws restricting online behavior in authoritarian states. If they do not comply, the firms risk losing their licenses and access to those markets. Many observers have pointed to Google's decision to withdraw from China rather than continue to accept Chinese government restrictions as an example of a principled corporate stand that others should emulate. But industry representatives paint a more complicated picture. Fledgling telecommunications and technology companies without large revenue streams – or even larger firms that do not boast tremendous financial assets – may find the need to stay engaged in China, the world's largest Internet market, a question of life or death.

The perception that American firms themselves are an arm of American foreign policy also jeopardizes their ability to compete in key foreign markets. During the 2009 Iranian revolution, for instance, Jared Cohen, then a member of Clinton's policy planning staff, emailed Twitter founder Jack Dorsey urging the company to forgo a planned site outage so that Iranians could continue tweeting. This action attracted disapproval even in the United States, but it is consistent with the U.S. policy of promoting Internet freedom. The U.S. government routinely reaches out to private firms and this will constitute an increasingly important element of America's Internet freedom agenda. Yet, some of those who have criticized the State Department's outreach to Twitter also call on the government to urge corporations to join the GNI.

Permitting U.S. companies to operate in certain authoritarian countries rather than cede the market to the alternatives can serve America's Internet freedom agenda in the long term. For example, while Google censored its search results in mainland China, Baidu – China's largest domestic search engine – has even more stringent censorship policies, and has taken over much of the market share Google abandoned. A policy change like Google's might lead to less information available online to the average Chinese citizen, not more. And a transaction between two foreign parties over which the United States has no visibility or control could quite conceivably faclitate Internet repression more than the activities of an American company that are, at the end of the day, subject to U.S. law and public opinion pressures.

As technology companies increasingly expand into repressive foreign countries, they will face heightened pressure from Congress and the public to make internal decisions with an eye toward their broader implications. Facebook, for example, has required users to register their accounts under their real names – clearly a deterrent to dissidents who wish to remain anonymous. This has been a particular point of contention between Facebook and Internet freedom advocates, because it potentially allows for regime allies to have activists using aliases suspended from the site.

In 2008, a coalition of nonprofit organizations, universities and financial institutions, nearly all American, joined with Google, Yahoo and Microsoft to form the GNI, which attempts to codify business codes of conduct. GNI members commit to "collaborate in the advancement of user rights to freedom of expression and privacy."[120] Participants agree to adhere to a set of shared principles about how companies should respond to government requests for information, including making those requests transparent and protecting users' rights to privacy. The GNI includes a reporting and enforcement mechanism to ensure that its members meet its compliance and evaluation requirements.[121]

While many view the GNI as a great step forward in the Internet freedom movement, its effects have been significantly limited by the lack of corporate participants. Not a single technology company has joined the three founders, each of which is an American firm. The Secretary of State has publicly called on technology companies to join the initiative, and members of Congress have done the same; in August 2009, Sen. Richard Durbin, D-Ill., wrote to 26 companies urging them to join the GNI.122 All has been for naught. Corporate representatives with whom we spoke observed that their companies agreed with the principles put forth by the GNI, but they simply do not see it in their business interest to join because they do not wish to expend the resources necessary to fulfill the GNI's reporting requirements or submit their corporate practices to external reviews. Others expressed concern that joining the GNI could threaten their access to particular markets because GNI is perceived as an organization for promoting American values.

In an encouraging trend, a few companies have proactively sought to break through Internet repression. When Egypt shut down the Internet almost completely, a French company offered Egyptians anonymous dial-up access via a French phone number.[123] At the same time, Google and Twitter jointly created a tool, Speak2Tweet, which allowed Egyptians to call a dedicated number that translated their voice messages into tweets. Google officials noted that the initiative was a direct response to the events in the Middle East, saying, "We hope this will go some way to helping people stay connected at this very difficult time."[124] During the revolution in Libya, the Moammar Gadhafi regime cut Internet access and jammed cellular networks and satellite phone signals. A Libyan-American telecommunications executive led a team that imported millions of dollars in equipment, hijacked the national network and reestablished communications in the country.[125]

Increasing Economic Incentives

Increasing the economic incentives to promote Internet freedom must be central to any U.S. government strategy. There are three major ways to do this: persuasion, publicity and trade agreements.

U.S. officials are trying to persuade states that Internet repression will chill their economic development, and to persuade companies that Internet freedom issues affect their own financial interests and bottom lines. Clinton has noted that a free Internet, by increasing transparency, can reduce corruption – making a given economy a more predictable and profitable marketplace for business – and that by investing in countries with tough censorship and surveillance policies, companies can see their websites shut down or their staff threatened.[126] Indeed, corporations will increasingly find themselves navigating the complex web of Internet restrictions abroad, some of which will directly affect their balance sheets.

Every time an American company complies with a politically motivated order to block Internet content or share user information, it risks negative publicity in the United States and elsewhere. As negative publicity builds, Congress may pass laws that would prohibit American companies from aiding certain forms of Internet repression which could require companies to withdraw from foreign markets where national laws conflict with U.S. laws. As a result, corporations have an interest in preempting such situations by pressing foreign governments for more liberal Internet environments – or at least fewer constraints – and U.S. government officials should encourage them to do so.

The U.S. government can also promote Internet freedom though trade agreements where Internet repression serves as a trade barrier. When a country blocks access to a U.S. website, for example, it also blocks the site's advertising – and thereby interferes with the trade in products and services advertised.[127] Of the millions of dollars lost during the Internet shutoff in Egypt, it is hard to imagine that American businesses were not also affected.

Employing trade agreements is a more promising strategy than demanding foreign governments to adhere to universal values, because they contain economic incentives (thus giving the United States negotiating leverage) and are at least potentially enforceable. Should Internet censorship become accepted as a non-tariff trade barrier, a censoring government could be vulnerable to dispute arbitration at the World Trade Organization or bilateral trade remedies. And such agreements could be bilateral, multilateral or even global.

The United States should more actively try to insert binding language in agreements that would prohibit Internet censorship or other efforts to limit access to information online. The United States did include a relevant provision in the Korea-U.S. Free Trade Agreement, approved by Congress in December 2010. That agreement states in part: "Recognizing the importance of the free flow of information in facilitating trade, and acknowledging the importance of protecting personal information, the Parties shall endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders."[128] Such language is clearly nonbinding – "shall endeavor to refrain" is a loose commitment at best – but nevertheless suggests how the United States can promote Internet freedom in future trade negotiations.

Reforming Export Controls

The U.S. government can also reform its export controls on information technologies to further its Internet freedom objectives. Discussions about the link between the public and private sectors in promoting Internet freedom have focused on whether the U.S. government should prohibit the supply of technology and equipment to repressive governments. But the government must also ensure that it does not prohibit the export of technology that could be used to promote online freedom.

For years the United States has relied on controls enforced by the Departments of Commerce and Treasury to regulate overseas sales of merchandise and materials to states that pose a threat to U.S. national and economic security. These controls restrict exports of sensitive computer hardware and software, such as cryptographic programs and other technologies that scramble messages and data, in part to prevent unfriendly states from acquiring cyber capabilities that could be used against the United States or its allies. Until recently, basic Internet services (such as email and instant message services) could not be exported to states such as Cuba, Iran, Syria and Sudan.

In March 2010, the Treasury Department issued a general license for Internet service technologies that would allow companies to export photo sharing and other social networking and communications services to users in Cuba, Iran and Sudan – a move administration officials cited explicitly as being part of their Internet freedom agenda.[129] In June 2010, the Commerce Department eliminated export restrictions on most mass-market electronic products with encryption functions, including cellphones, laptops and computer drives, which can now be exported without a license.[130]

Yet export controls remain burdensome for Internet freedom. Administration officials have privately stated that complex and overlapping export control regulations chill commercial activity, especially with technology developers. U.S. export controls currently restrict, for instance, the transferring, transmitting and downloading of open source code that is already widely available for free online. [131] This open source code includes encryption code for secure communications and a suite of other tools that could potentially give cyber-dissidents and other online activists a wider range of options for communicating securely and accessing banned content. But a strict interpretation of current export controls requires websites that host open source code, such as Google and Mozilla, to block access to Internet Protocol (IP) addresses originating in sanctioned countries.

In March 2010, the Treasury Department issued a general license for Internet service technologies that would allow companies to export photo sharing and other social networking and communications services to users in Cuba, Iran and Sudan.

Currently, when the State Department funds a particular technology, the developer receives a specific license that waives export controls on that technology – so that it can, for example, provide circumvention technology to Iranians and Syrians. Yet the license does not apply to the same technology if it is created and exported by an organization that does not receive State Department funds. The U.S. government should quickly fix this glaring inconsistency.

V. NAVIGATING THE TENSIONS BETWEEN INTERNET FREEDOM AND CYBER SECURITY

Balancing the principle of freedom of expression on the Internet, in which users can act anonymously, with the need for a secure environment in which malicious users seeking to do harm can be identified and stopped by responsible governments, is a difficult challenge. Indeed, policymakers today are engaged in two simultaneous and potentially contradictory efforts. Promoting Internet freedom implies advocating privacy and providing tools through which individuals can act anonymously online. Cyber security, by contrast, implies online transparency and attribution. These two efforts create tensions that are not well understood and frequently remain unaddressed. Part of the problem stems from the fact that conversations about America's cyber security and Internet freedom policies have, by and large, taken place in isolation from each other. Cyber security policy has involved the national security community, while Internet freedom policies have involved the technology community and a handful of human rights activists – and now the foreign policy community.

These tensions are real and will sometimes force difficult choices, but they should not prevent the United States from securing cyberspace and promoting Internet freedom at the same time. U.S. policies will have to address two key tensions: anonymity versus attribution, and defending against attacks versus emboldening autocracies.

Anonymity versus Attribution

Cyber security proponents often advocate greater transparency in online behavior and seek to improve the ability of security monitors to reliably identify malicious users and track their activities. "Anonymity is the fundamental problem we face in cyberspace," Stewart Baker, former chief counsel for the National Security Agency (NSA), said at an April 2010 Internet conference in Germany.[132]

Security practitioners argue that online transparency and attribution allows law enforcement to pinpoint the origins of cyber attacks and intrusions and respond to them, which could also deter future malicious activities. Former Director of National Intelligence Mike McConnell has argued for making the Internet more transparent, saying, "We need to re-engineer the Internet to make attribution, geo-location, intelligence analysis and impact assessment – who did it, from where, why and what was the result – more manageable."[133]

Such efforts would conflict with the Internet freedom agenda, which emphasizes online anonymity. The Tor network described previously, for example, does not have a back door through which the U.S. government or other law enforcement agencies can access and monitor the secured communication or Web traffic. Experts argue that because the software is open source, users would identify any back door in the source code, compromising the software's integrity and prompting users to find other programs without a back door. Criminal networks and others seeking to monitor law enforcement users could also exploit any back door that bypasses the controls and auditing functions and hijack information of those monitoring them.

Anonymous Internet use not only causes cyber security concerns; it can also threaten other aspects of American national security. Technologies such as Tor, for instance, could be used not only by dissidents and democracy activists, but also by criminals and terrorists.[134] The very anonymizing tools and point-to-point encrypted communication technology funded by the State Department and BBG could, some experts caution, be used by international terrorist organizations to coordinate and carry out attacks undetected by U.S. government security agencies.[135] Although not reacting specifically to government-funded anonymity tools, for years the FBI has warned about the potential risks associated with the spread of sophisticated encryption technologies.[136] As early as 1993, the NSA developed a "Clipper chip" designed for telecommunications companies to use in secure voice transmissions – but with a back door for the U.S. government.[137] (After a public outcry by privacy activists, the program was abandoned.)

Other technologies pose potential challenges as well. BBG programs are intended to provide foreigners access to its own online materials – so, for instance, a Chinese citizen can access news stories on the Voice of America website that is blocked in China. However, while BBG-provided proxy servers and other technologies enable a user to access BBG websites, they do not require users to stay there. This facilitates peer-to-peer communication among users, but it could also enable potential criminals or terrorists to access propaganda or websites that teach bomb making and other illicit skills. Similarly, activists seeking to evade government surveillance can purchase prepaid mobile phones that lack unique identifiers, and the U.S. government reportedly hopes to fund projects that enable mobile phone users to anonymously access the Internet. Because criminals and terrorists also seek to use such phones, however, a number of governments have begun outlawing them.[138]

U.S. government-supplied circumvention tools are not the only option for individuals wishing to communicate anonymously or access banned websites. Criminals and terrorists are far more likely to use botnets (collections of compromised computers running automated software, generally without the knowledge of their users) and other illicit tools instead of using less effective tools offered by the U.S. government (which can be slower than others, have restricted bandwidth and contain other features that make illicit tools more attractive by comparison). "Mujahideen Secrets 2," for example, is a jihadi-developed encryption tool designed to allow al Qaeda supporters to communicate online.[139] While it is clearly impossible to eliminate the possibility that government-sponsored

In drafting legislation intended to protect the nation's cyber systems and infrastructure, the U.S. government must tread carefully and quash perceptions that it is acceptable to use a "national cyber emergency" to trample on freedom of expression.

technologies will be used by bad actors, it is likely that the number of bad actors doing so will pale in comparison to the number of users simply wishing to access neutral media.

Defending Against Attacks versus Emboldening Autocracies

Simple efforts to defend against cyber attacks also affect America's Internet freedom agenda.

The U.S. military has outlined a cyber security strategy based on active defense, which includes blocking malicious software before it attempts to enter military networks.[140] Although hunting down destructive content outside defense networks is likely to be rare, the head of the military's newly established U.S. Cyber Command has argued that the United States must have offensive cyber capabilities to shut down attacking systems.[141] Such moves, which may be entirely justified, could at the same time embolden autocracies wishing to justify their own offensive operations.

The perception that the U.S. government could restrict traffic over large portions of the Internet in the event of a cyber emergency could also complicate its efforts to promote online freedom. Congress debated a bill last year that would authorize greater government control over the U.S. digital infrastructure in the event of a nationwide cyber attack.[142] Though many media reports about a so-called Internet "kill switch" are erroneous (and a newly introduced version explicitly prohibits any government employee from shutting down the Internet), the bill nevertheless raised concerns that such authority would undermine Internet freedom. While interpretations of the bill vary widely, an expert with the Electronic Frontier Foundation warned, "The president would have essentially unchecked power to determine what services can be connected to the Internet or even what content can pass over the Internet in a cyber security emergency."[143] The bill's sponsors dispute this interpretation and note that the president's powers could be exercised only in extreme emergencies and pursuant to limitations.

The U.S. government must establish precise, widely understood scenarios under which it could declare an emergency and the powers it could then exercise. Failing to clearly define what constitutes a national "cyber emergency" that would give national leaders emergency powers to restrict Internet activity could set a precedent by which authoritarian regimes justify shutting off the Internet during their own "cyber emergency" – such as widespread anti-government protests. Again, there is a distinct difference between a presidential order to restrict some forms of Internet traffic in the face of a cyber attack on America's critical infrastructure and President Mubarak's decision to shut down his nation's Internet during the democratic revolt in Egypt. In drafting legislation intended to protect the nation's cyber systems and infrastructure, the U.S. government must tread carefully and quash perceptions that it is acceptable to use a "national cyber emergency" to trample on freedom of expression.

VI. RECOMMENDATIONS – EIGHT PRINCIPLES FOR INTERNET FREEDOM

The principles and policy recommendations below reflect an integrated Internet freedom strategy that balances competing foreign policy, economic and national security priorities, and leverages the tremendous potential of the private sector.

Principle 1: Embrace a Comprehensive Approach

Current efforts to promote Internet freedom are fragmented across the U.S. government, and the issue barely registers among some officials who could make a significant contribution. As a result, **policymakers should incorporate Internet freedom into their decision-making.** Promoting Internet freedom should be linked to other goals, including America's cyber security agenda and its economic diplomacy efforts. The White House's international cyberspace strategy is a step in the right direction, but a comprehensive agenda should combine top-level policy direction with providing technology and training for bloggers and activists, exercising diplomatic support for imprisoned dissidents and online authors, training for foreign service officers and others in new media, integrating Internet freedom issues into country and regional strategies, articulating economic arguments for Internet freedom, treating censorship as a trade barrier, working with the private sector, reforming export controls and actively shaping international norms.

To harness external expertise across fields, **the U.S. government should regularly convene private sector professionals; diplomats; Internet engineers and technical experts; cyber defense officials; export control lawyers; human rights activists; and foreign policy experts to explore new ways of promoting Internet freedom.** The aim should be to share knowledge among these professionally distinct groups and discern potential areas of cooperation or policy change. This type of forum could be modeled after the Obama administration's March 2011 summit on bullying, in which the administration convened civil society activists, educators, policymakers and technology firms to develop strategies to prevent bullying (including cyber bullying).[144]

The U.S. government should use traditional diplomacy to promote America's Internet freedom agenda, including lobbying foreign governments to liberalize restrictions on freedom of speech, advocating for American companies (when they seek such diplomatic assistance) under pressure from foreign regimes to turn over private data, pressing governments to release political prisoners and urging foreign partners to join the United States in pursuing the agenda. As the U.S. government does so, it must continually consider the tradeoffs between promoting Internet freedom and the other items on its foreign policy and economic agenda.

Principle 2: Build an International Coalition to Promote Internet Freedom

The U.S. government should internationalize its Internet freedom efforts. The push for online freedom, which is rooted in universal values, is too heavily identified with the United States alone. Promoting Internet freedom must not be merely an element of American foreign policy, but rather should be an international effort supported by a wide range of actors

- The U.S. government should convene a core group of democratic governments – open to any that wish to join – that would together advocate for Internet freedom. This should include seeking common statements and policy advocacy in international fora where rules and norms are most likely to be set. It should also convene other stakeholders, including international organizations, NGOs and the private sector, for the same purpose.
- The Secretary of State should give her next major address on Internet freedom in a foreign

country, possibly in Europe alongside key EU commissioners.

- The U.S. government should help internationalize the GNI by urging European and other democratic governments to encourage foreign companies to join.

The U.S. government should work to expand the sources of technology funding over the medium to long term. The U.S. government should encourage other actors to fund Internet freedom-related technologies, so that it does not remain the major funder of such technologies indefinitely.

- Officials should work with like-minded governments and NGOs to explain America's Internet freedom-related technology programs, share lessons learned thus far, and encourage them to develop their own programs. They should also urge the private sector to monetize circumvention and anonymity technologies (e.g. by circumventing restrictions so users can access websites with ads).

Principle 3: Move Beyond Circumvention Technologies

The U.S. government should fund a range of technologies beyond those that circumvent online censorship. While breaking down China's Great Firewall has attracted the vast majority of public attention and support on Capitol Hill, circumvention tools should comprise just one (albeit critical) element of a much larger agenda. The State Department has requested proposals for multiple programs that together comprise a quite well-rounded approach to technology, all of which should receive funding. State also plans to establish an emergency fund to help civil society organizations keep their online operations up and running if they are targeted by severe hacking or cyber attacks.[145]

- In addition to funding existing tools, the U.S. government should fund technologies that:
  - » Help dissident and human rights websites protect themselves against DDoS attacks.
  - » Help groups create mirror sites and reconstitute their websites and archives after a takedown.
  - » Facilitate encrypted communications and other forms of digital security.
  - » Ensure mobile access. Mobile platforms are increasingly the locus of online activity, and the State Department should ensure that a disproportionate amount of funding focuses on securing open access to the Internet through mobile devices.
- In order to maximize users' safety, the U.S. government should require any online tool receiving U.S. funding to go through an independent security audit before it is deployed.

The U.S. government should adopt a financial award, akin to the "X Prize" that invites technological competition, and other creative methods to foster technological innovation. The government should offer a financial award to private sector organizations that can develop the lowest-cost, most user-friendly and most resilient circumvention or anonymity technology (e.g., an Internet Freedom Innovation Award for developing best-in-class technologies).

Principle 4: Prioritize Training

The State Department, along with USAID, should continue to foster Internet freedom through targeted training programs. Current or forthcoming training programs include basic training in digital tools for activists and civil society organizations, instruction on using virtual open Internet centers and training in digital security.[146]

- The U.S. government should help activists understand the risks associated with using new communications technologies and develop plans to secure their networks; establish contingency plans for emergencies; and establish processes for putting websites and digital archives back online after an attack. It should also train dissidents in personal security against both cyber and non-cyber monitoring, such as surveillance cameras in Internet cafes.

Principle 5: Lead the Effort to Build International Norms

The U.S. government should press in all relevant fora for a liberal concept of Internet freedom, and counter attempts by authoritarian states to adopt norms that restrict freedom of information and expression online. American officials have wisely tied basic Internet freedom principles to existing international agreements, but they should also seek to articulate these principles in new normative arrangements during meetings of the U.N., the ITU, the G8 and G20 meetings, and other international fora.

- U.S. officials should publicly and clearly distinguish between practices in democracies, which give law enforcement access to otherwise private data pursuant to due process, and those in countries whose governments seize such information without due process.
- The U.S. government should clearly define what constitutes a national security threat in cyberspace. It should emphasize that it will only restrict Internet traffic during a national "cyber emergency" in accordance with clear and transparent principles (e.g., not to target political speech).
- The United States should work with other innovative, economically powerful market democracies to build common principles for domestic Internet use including general principles for the kinds of data governments will block and censor and how they will communicate those decisions.
- The United States should pursue an international transparency initiative to encourage governments to publicly state the categories of online information to which they restrict access, the legal grounds for these restrictions and how those laws can be changed (if this is not self-evident).

Principle 6: Create Economic Incentives to Support Internet Freedom

U.S. officials should continue to articulate the economic case for Internet freedom. The State Department's description of a "dictator's dilemma" should be supported by solid, quantitative evidence of the economic benefits of online freedom and costs of Internet repression. U.S. officials should make the corporate case as well, as the Secretary of State has done in the past. Internet freedom can reduce corruption by increasing transparency, reducing the risk that companies will face politically motivated requests that generate adverse international publicity and limiting the chances that a firm's websites will be shuttered or its staff threatened.

The State Department's description of a "dictator's dilemma" should be supported by solid, quantitative evidence of the economic benefits of online freedom and costs of Internet repression.

The U.S. government should push for Internet censorship to be recognized as a trade barrier.

- The United States should press for a binding clause in any Trans-Pacific Partnership agreement – currently under consideration – that incorporates basic principles about the free flow of digital information, and seek to include such provisions in other trade agreements.

- The United States should examine the legal case for treating extreme cases of Internet repression (e.g. Egypt's shutdown in early 2011) as a violation of World Trade Organization rules, and include information in U.S. Trade Representative (USTR) and Commerce Department reports about the economic harm produced by censorship and other forms of Internet repression.

Principle 7: Strengthen the Private Sector's Role in Supporting Internet Freedom

U.S. government officials should continue to urge companies to join the GNI, while also encouraging companies to develop broad unilateral codes of conduct consistent with the GNI's underlying principles.

Congress should adopt a nuanced legal framework for the proper role of American corporations that:

- Prohibits activities such as giving autocratic governments the private data of dissidents, when the request is clearly intended to quash legitimate freedom of expression.
- Requires American companies to periodically disclose to the U.S. government:
  - Foreign governments' requests for information and services that do not conform to internationally-recognized standards (including information about users, IP blocking, keyword censorship and online surveillance), and whether the companies complied with these requests.
  - Sales of technology and services to government agencies or state-controlled companies that are reasonably expected to aid significant Internet repression.

Congress should continue highlighting specific business practices that both promote and restrict Internet freedom through hearings, resolutions, the bully pulpit and other means. In addition to

Recommendations for Technology Companies

Technology firms should take several measures to promote online freedom, many of which can directly or indirectly benefit their bottom lines. They should:

- Provide basic technical assistance with built-in security functions, such as secure password protection and assess ways in which foreign governments can use their tools or services for Internet repression and explore ways to mitigate those uses.
- Better inform users and the public about who may access data they control and under what conditions, so that users can make informed decisions about whether using particular services in specific contexts will put them in danger.[147]
- Move toward greater transparency when censoring content or sharing private information with governments. Google's transparency report publicizes the number of government inquiries it receives for information about users and requests for the company to take down or censor content. This provides one useful model for increasing transparency, and technology companies should seek to establish industry-wide standards on public disclosure.
- Fund technology personnel at human rights and democracy organizations so that these groups can develop a deeper understanding of the complex issues surrounding new communications technology and political change abroad, and so that companies can increase their understanding of human rights advocacy and the ways in which technology products and features are viewed.
- Advocate for Internet freedom abroad. American companies have an incentive to avoid being caught between the requirements of local law in an autocratic environment and the bad publicity that might result from complying with them. They can work to preempt such dilemmas by pressing foreign governments for more liberal Internet environments – or at the very least resist efforts to aid repression.

naming and shaming, Congress and the executive branch should publicly praise companies that are attempting to uphold universal values while doing business in autocratic environments.

Principle 8: Reform Export Controls

The U.S. government should launch a full review of its export controls on new communications technology, which should aim to:

- Permit the export of otherwise widely available open source code that would be available to foreign users at no cost.
- Ensure that circumvention and other technologies that are identical or very similar to those supported by the U.S. government (and thus exempted from export controls) are also exempted.
- Determine ways (which in some cases will require new legislation) to relax restrictions on exporting relevant technologies to countries like Syria, which was not included in Treasury's 2010 export control revisions.[148]
- Ensure that any export control reforms accounts for the need to maintain safeguards on American technology for national security reasons.

The U.S. government should educate technology companies on the exact requirements of export controls – including any changes – so that companies do not over-comply and deny legal technologies to activists abroad.

VII. CONCLUSION

The U.S. government must develop a truly comprehensive Internet freedom strategy. Over the past several years, it has taken important, positive steps in a number of areas, from providing technologies to shaping norms to engaging the private sector. It must now build on these efforts to integrate other elements, including trade policy, export control reform and others. Underlying all these efforts is a bet – essentially the same bet that the United States placed during the Cold War – that supporting access to information and encouraging the free exchange of ideas is good for America. As we have discussed in this report, we believe this bet is well worth making.

A free Internet, however, is not a silver bullet for social change. Supporting Internet freedom is complicated and poses tradeoffs with other items on the American diplomatic, security and economic agenda. It should be seen as just one, potentially quite important, element in a broader approach to promoting democratic ideals in repressive societies. The net effect of this effort is uncertain, and it will likely remain so for years.

But we should not underestimate the potential power of the Internet. We live in a time when an application like Facebook, designed in 2004 for American university students to share information has, in 2011, helped topple a dictator in Egypt; a time when the best satellite television coverage of demonstrations and conflict can come from online video postings; and a time when dissidents risk imprisonment or worse for blogging their beliefs.

The U.S. government faces a constant challenge in keeping up with new technology and the changing ways that users employ it. Corporations are continually vexed by the many varying demands put upon them by governments around the world. Individuals in autocratic societies face dilemmas

We live in a time when an application like Facebook, designed in 2004 for American university students to share information has, in 2011, helped topple a dictator in Egypt.

in determining how to proceed online. Though the debate is complicated, the longstanding American commitment to basic human rights and freedoms should remain clear. And on that basis, the United States has a responsibility to promote Internet freedom, which is key to ensuring a greater degree of human liberty in an ever-more-contested space.

ENDNOTES

1. "Over 5 Billion Mobile Phone Connections Worldwide," BBC News (9 July 2010), http://www.bbc.co.uk/news/10569081.

2. The authors thank Rebecca MacKinnon for the insight that the cyber domain constitutes an extension of civil society.

3. President Barack Obama stated that, "There are certain core values that we believe in as Americans that we believe are universal: freedom of speech, freedom of expression, people being able to use social networking or any other mechanisms to communicate with each other and express their concerns." David Jackson, "Obama: 'Violence is Not the Answer' in Egypt," *USA Today* (28 January 2011), http://content.usatoday.com/communities/theoval/post/2011/01/obama-violence-is-not-the-answer-in-egypt/1?csp=34.

4. For the purposes of this study, we use the term "Internet" and "new communications technologies" interchangeably, defining them to include a broad collection of new digital communication technologies that are connected in some form to the Internet, including SMS text, Skype and other voice-over-the-Internet protocols (VOIP), as well as web-based platforms (e.g., Facebook and Twitter).

5. The authors paid particular attention to examining the potential tensions between Internet freedom and cyber security; these tensions are explored in greater depth in "America's Cyber Future: Security and Prosperity in the Information Age," Center for a New American Security (June 2011).

6. Evgeny Morozov, *The Net Delusion* (New York: PublicAffairs Books, 2011): 230.

7. Universal Declaration of Human Rights, Article 19. The International Covenant on Civil and Political Rights also articulates basic freedoms of expression applicable to Internet-based activity, as described below.

8. "Statement by the Press Secretary on Violence in Syria" (24 March 2011), http://www.whitehouse.gov/the-press-office/2011/03/24/statement-press-secretary-violence-syria.

9. The White House, *National Security Strategy of the United States,* Section 3 (May 2010): 39, http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

10. U.S. Department of State, *State Summary of Global Internet Freedom Task Force: Group Seeks to Maximize Freedom of Expression, Free Flow of Information and Ideas* (20 December 2006), http://www.america.gov/st/democracyhr-english/2006/December/20061220173640xjsnommis0.7082331.html.

11. The White House, *National Security Strategy of the United States*, Section 7.C.1 (March 2006),http://georgewbush-whitehouse.archives.gov/nsc/nss/2006/sectionVII.html.

12. "Remarks by the President to the United Nations General Assembly" (23 September 2009), http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-to-the-United-Nations-General-Assembly/.

13. Hillary Rodham Clinton, "Internet Rights and Wrongs: Choices & Challenges in a Networked World," The George Washington University, Washington (15 February 2011), http://www.state.gov/secretary/rm/2011/02/156619.htm.

14. "Yahoo Chief Apologizes to Chinese Dissidents' Relatives," *The New York Times* (7 November 2007), http://www.nytimes.com/2007/11/07/business/worldbusiness/07iht-yahoo.1.8226586.html.

15. The bill has subsequently been introduced in different versions, but has not been passed as of this writing. *Global Internet Freedom Act,* Govtrack.us (10 May 2005), http://www.govtrack.us/congress/billtext.xpd?bill=h109-2216.

16. Glenn Kessler, "Cisco File Raises Censorship Concerns," *The Washington Post* (20 May 2008), http://www.washingtonpost.com/wp-dyn/content/article/2008/05/19/AR2008051902661.html.

17. In full disclosure, one of the authors of this report helped draft this act while serving in government.

18. U.S. Department of State, *State Summary of Global Internet Freedom Task Force* (20 December 2006), http://www.america.gov/st/democracyhr-english/2006/December/20061220173640xjsnommis0.7082331.html.

19. Hillary Rodham Clinton, "Remarks on Internet Freedom," the Newseum, Washington (21 January 2010), http://www.state.gov/secretary/rm/2010/01/135519.htm.

20. Hillary Rodham Clinton, "Internet Rights and Wrongs: Choices & Challenges in a Networked World," The George Washington University, Washington (15 February 2011), http://www.state.gov/secretary/rm/2011/02/156619.htm.

21. Ibid.

22. Ibid.

23. Sami ben Gharbia, "The Internet Freedom Fallacy and the Arab Digital Activism," Samibengharbia.com (17 September 2010), http://samibengharbia.com/2010/09/17/the-internet-freedom-fallacy-and-the-arab-digital-activism/.

24. Lachlan Carmichael, "U.S. Trains Activists to Evade Security Forces," *Agence France Press* (8 April 2011), http://www.google.com/hostednews/afp/article/ALeqM5h-zfvaYJftSfafM8whfpxycifTaQ?docId=CNG.2bbf1732398d8832e67b0555c508f609.a01.

25. We draw from the work of Larry Diamond, a leading democracy scholar. In his book, *The Spirit of Democracy,* he describes at length the "thick conception" of democracy and lists several attributes that distinguish democracies from other political systems. Larry Diamond, *The Spirit of Democracy* (New York: Times Books, 2008): 22.

26. Bernard Kouchner, "The Battle for the Internet," *The New York Times* (13 May 2010), http://www.nytimes.com/2010/05/14/opinion/14iht-edkouchner.html?_r=1.

27. Nicholas D. Kristof, “Tear Down This Cyberwall!” *The New York Times* (17 June 2009), http://www.nytimes.com/2009/06/18/opinion/18kristof.html?_r=1.

28. Under Secretary of State for Democracy and Global Affairs Paula Dobriansky, “New Media vs. New Censorship: The Assault,” remarks to Broadcasting Board of Governors, Washington (10 September 2008).

29. Mark Pfeifle, “A Nobel Peace Prize for Twitter?” *The Christian Science Monitor* (6 July 2009), http://www.csmonitor.com/Commentary/Opinion/2009/0706/p09s02-coop.html.

30. Alexei Oreskovic, “Egyptian Activist Creates Image Issue for Google,” *Reuters* (12 February 2011), http://www.reuters.com/article/2011/02/12/us-egypt-google-idUSTRE71B0KQ20110212.

31. Evgeny Morozov, *The Net Delusion* (New York: PublicAffairs Books, 2011): xiii.

32. Malcom Gladwell, “Why the Revolution Won’t be Tweeted,” *The New Yorker* (4 October 2010), http://www.newyorker.com/reporting/2010/10/04/101004fa_fact_gladwell?currentPage=1.

33. Jeffrey Gedmin, “Democracy isn’t just a tweet away,” *USA Today* (22 April 2010).

34. Golnaz Esfandiari, “Misreading Tehran: The Twitter Devolution,” *Foreign Policy* (7 June 2010), http://www.foreignpolicy.com/articles/2010/06/07/the_twitter_revolution_that_wasnt.

35. Ian Bremmer, “Democracy in Cyberspace,” *Foreign Affairs* (November/December 2010), http://www.foreignaffairs.com/articles/66803/ian-bremmer/democracy-in-cyberspace.

36. Sean Aday, Henry Farrell, Marc Lynch, John Sides, John Kelly and Ethan Zuckerman, “Blogs and Bullets: New Media in Contentious Politics,” United States Institute of Peace (August 2010): 9. Much of the discussion of theories of change in this section draws upon this important work.

37. Ibid.: 9.

38. Evgeny Morozov, “From Slacktivism to Activism,” Foreign Policy Net Effect blog (5 September 2009), http://neteffect.foreignpolicy.com/posts/2009/09/05/from_slacktivism_to_activism.

39. Larry Diamond, “Liberation Technology,” *Journal of Democracy* (July 2010): 70.

40. Ibid.

41. Sean Aday, Henry Farrell, Marc Lynch, John Sides, John Kelly and Ethan Zuckerman, “Blogs and Bullets: New Media in Contentious Politics,” United States Institute of Peace (August 2010): 10.

42. Steve Coll, “The Internet: For Better or for Worse,” *The New York Review of Books* (7 April 2011).

43. Lauren Kirchner, “‘Information Wars’ on Al Jazeera English,” *Columbia Journalism Review* (14 February 2011).

44. Sean Aday, Henry Farrell, Marc Lynch, John Sides, John Kelly and Ethan Zuckerman, “Blogs and Bullets: New Media in Contentious Politics,” United States Institute of Peace (August 2010): 10-11. The authors point out that social media in particular may reduce the transaction costs for organizing collective action, for example by making communication easier across physical and social distance, or by undermining top-down movements in favor of flatter social movements.

45. Ibid.: 18.

46. This website has evidently garnered little interest. Evgeny Morozov, “Think Again: The Internet,” *Foreign Policy* (May/June 2010), http://www.foreignpolicy.com/articles/2010/04/26/think_again_the_internet.

47. “‘Haystack’ Gives Iranian Opposition Hope for Evading Internet Censorship,” *The Christian Science Monitor* (16 April 2010).

48. Jennifer Preston, “Syria Restores Access to Facebook and YouTube,” *The New York Times* (9 February 2011).

49. Spencer Ackerman, “Trolls Pounce on Facebook’s Tahrir Square,” *Wired* (4 February 2011), http://www.wired.com/dangerroom/2011/02/trolls-pounce-on-facebooks-tahrir-square/.

50. Tarek Amr, “The Middle East, the Revolution and the Internet,” Remarks at AccessNow web symposium (3 February 2011), https://www.accessnow.org/policy-activism/press-blog/The-Middle-East-The-Revolution-And-The-Internet.

51. Daniel Calingaert, “Authoritarianism vs. the Internet,” *Policy Review* (1 April 2010): 6.

52. Brianna Lee, “Chinese Government Issues Preemptive Crackdown of ‘Jasmine Revolution’ Protests,” PBS.org (3 March 2011), http://www.pbs.org/wnet/need-to-know/the-daily-need/chinese-government-issues-preemptive-crackdown-of-jasmine-revolution-protests/7697/.

53. Quincy Yu, “Aborted Chinese ‘Jasmine Revolution’ a Trap Say Analysts,” *The Epoch Times* (22 February 2011), http://www.theepochtimes.com/n2/china/aborted-chinese-jasmine-revolution-a-trap-say-analysts-51732.html.

54. 2010 Reporters Without Borders report cited in “New Media: A Force for Good or Evil?” *The Layalina Review* (12-25 March 2010), http://www.layalina.tv/publications/review/PR_VI.6/article2.html.

55. Rebecca MacKinnon, “China, the Internet, and Google,” testimony before the Congressional-Executive Commission on China (1 March 2010): 7.

56. Scott Peterson, “On Libya-Tunisia Border, Refugees Plead for Help to Go Home,” *The Christian Science Monitor* (3 March 2011).

57. Ibid.: 12.

58. The Organisation for Economic Co-operation and Development published a 2007 study on the economic impact of broadband Internet access based on

the work done by its Working Party on the Information Economy. The study notes that Internet communication technologies (ICTs) enable measurable economic growth: "Broadband is also increasingly important as an enabling technology for structural changes in the economy, most notably via its impact on productivity growth, but also by raising product market competition in many sectors, especially in services. ICTs and broadband are facilitating the globalisation of many services, with broadband making it feasible for producers and consumers of services to be in different geographical locations." Organisation for Economic Co-operation and Development, "Broadband and the Economy" (5 May 2007): 5, http://www.oecd.org/dataoecd/62/7/40781696.pdf.

59. Hillary Rodham Clinton, "Internet Rights and Wrongs: Choices & Challenges in a Networked World" (15 February 2011), http://www.state.gov/secretary/rm/2011/02/156619.htm.

60. The Organisation for Economic Co-operation and Development , "The Economic Impact of Shutting Down Internet and Mobile Phone Services in Egypt" (4 February 2011), http://www.oecd.org/document/19/0,3746,en_2649_34223_47056659_1_1_1_1,00.html.

61. Eric Schmidt and Jared Cohen, "The Digital Disruption: Connectivity and the Diffusion of Power," *Foreign Affairs* (November/December 2010).

62. Doyle McManus, "Did Tweeting Topple Tunisia?" *Los Angeles Times* (23 January 2011).

63. As is true when evaluating the effect of new technologies along other dimensions of political change, here too it is important to temper exuberance with caution. Historian Simon Sebag Montefiore, for instance, notes that while Facebook "certainly accelerates the mobilization of crowds . . . technology's effect is exaggerated: in 1848, the revolution that most resembles today's, uprisings spread from Sicily to Paris, Berlin, Vienna and Budapest in mere weeks without telephones, let alone Twitter. They spread through the exuberance of momentum and the rigid isolation of repressive rulers." Simon Sebag Montefiore, "Every Revolution is Revolutionary in Its Own Way," *The New York Times* (27 March 2011).

64. Stephen Williams, the BBC's executive editor for the Asia Pacific Region, emphasized the reciprocal information flows between online media and television during the 2009 Iranian protests. At the height of the protests, he notes, the BBC's Persian television offices in London received between six and eight Internet photos, emails and text messages every minute. "The influence of Internet social media was huge in disseminating pictures and messages round the world," Williams says, and it "has undoubtedly helped the opposition contact other like-minded voices inside Iran. But the most impact making pictures and reports could only be seen by a wider public in Iran through Persian-speaking TV, because Internet activity is limited." Stephen Williams, "The Power of TV News: An Insider's Perspective on the Launch of BBC Persian TV in the Year of the Iranian Uprising," Joan Shorenstein Center on the Press, Politics and Public Policy, Harvard University, Discussion Paper Series #D-54 (February 2010).

65. See Lauren Kirchner, "'Information Wars' on Al Jazeera English," *Columbia Journalism Review* (14 February 2011).

66. Jillian York, "More Than Half a Billion Internet Users are Being Filtered Worldwide," Open Net Initiative (19 January 2010), http://opennet.net/blog/2010/01/more-half-a-billion-internet-users-are-being-filtered-worldwide.

67. Sean Aday, Henry Farrell, Marc Lynch, John Sides, John Kelly and Ethan Zuckerman, "Blogs and Bullets: New Media in Contentious Politics," United States Institute of Peace (August 2010): 13.

68. Hal Roberts, Ethan Zuckerman, Jillian York, Robert Faris and John Palfrey, "2010 Circumvention Tool Usage Report," Berkman Center for Internet and Society, Harvard University (October 2010): 6, http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/2010_Circumvention_Tool_Usage_Report.pdf.

69. Clay Shirky, "The Political Power of Social Media: Technology, the Public Sphere, and Political Change," *Foreign Affairs* (January-February 2011).

70. Joshua Goldstein, "The Role of Digital Networked Technologies in the Ukrainian Orange Revolution," Berkman Center for Internet and Society, Harvard University (December 2007).

71. Myroslaw J. Kyj, "Internet Use in Ukraine's Orange Revolution," *Business Horizons*, Issue 49 (2006): 71-80, http://web.reed.edu/alumni/images/AC_2010/pdfs/Internet%20Use%20in%20Orange%20Revolution.pdf.

72. Marwan M. Kraidy, "Saudi Arabia, Lebanon and the Changing Arab Information Order," *International Journal of Communication* (2007), http://ijoc.org/ojs/index.php/ijoc/article/viewFile/18/22.

73. Brannon Cullum, "Oscar Morales and One Million Voices Against FARC," Movements.org (no date), http://www.movements.org/case-study/entry/oscar-morales-and-one-million-voices-against-farc/.

74. Maria Camila Pérez, "Facebook Brings Protest to Columbia," *The New York Times* (8 February 2008), http://www.nytimes.com/2008/02/08/business/worldbusiness/08iht-protest11.html?_r=3.

75. "Carnegie Guide to Egypt's Elections – The April 6 Youth Movement," Carnegie Endowment for International Peace, http://egyptelections.carnegieendowment.org/2010/09/22/the-april-6-youth-movement.

76. Nathan Hodge, "Moldova Calm after Twitter Storm," Wired Danger Room blog (10 April 2009), http://www.wired.com/dangerroom/2009/04/moldova-calm-af/.

77. "Moldova recount 'confirms result,'" BBC (17 April 2009), http://news.bbc.co.uk/2/hi/europe/8004603.stm.

78. Evgeny Morozov, "Kyrgyzstan's 'Analog Revolution,'" Foreign Policy's Net Effect blog (8 April 2010), http://neteffect.foreignpolicy.com/posts/2010/04/08/kyrgyzstans_analog_revolution.

79. Lisa Bryant, "Internet Powers Tunisian Protests," Voice of America (17 January 2011), http://www.voanews.com/english/news/africa/Internet-Powers-Tunisian-Protests-113868589.html.

80. Lisa Bryant, “Internet Powers Tunisian Protests,” Voice of America (17 January 2011), http://www.voanews.com/english/news/africa/Internet-Powers-Tunisian-Protests-113868589.html.

81. Jennifer Preston, “Movement Began with Outrage and a Facebook Page That Gave It an Outlet,” *The New York Times* (5 February 2011), http://www.nytimes.com/2011/02/06/world/middleeast/06face.html.

82. “Estimated 2 Million People Protest In, Around Tahrir Square In Cairo Egypt,” Cnewsworld.com, http://www.cnewsworld.com/world-news/middle-east-world-news/estimated-2-million-people-protest-in-_-around-tahrir-square-in-cairo-egypt-mp4/.

83. James Glanz, “How Mubarak Shut Down Egypt’s Internet,” *The Age* (Australia) (17 February 2011), http://www.theage.com.au/world/how-mubarak-shut-down-egypts-internet-20110216-1awjj.html.

84. Grant Gross, “Egyptian Activist: Internet Shutdown Backfired,” *PC World* (3 February 2011), http://www.pcworld.com/businesscenter/article/218630/egyptian_activist_internet_shutdown_backfired.html.

85. See “Data Retention,” Electronic Privacy Information Center, http://epic.org/privacy/intl/data_retention.html.

86. “Tor: Sponsors,” http://www.torproject.org/about/sponsors.html.en.

87. Experts at the Berman Center for Internet and Society at Harvard University examined virtual private networks (VPNs) in a thorough study on circumvention technology in 2010. They explain how these networks operate: “VPN technology has traditionally been used to allow corporate and other institutional users to access internal networks from the public network, but in the past few years there has been tremendous growth in the availability of personal VPN services. Among other uses, these personal VPN services act as circumvention tools as long as the VPN proxy is hosted outside a filtering country. VPN services might or might not require installation of client-side software (many rely on existing VPN support in Windows or Mac OSX and so need no extra client software) and allow the user to access the web directly through the native browser interface. Because VPN services tunnel all Internet traffic, they can be used for email, chat, and any other Internet service in addition to web browsing. Almost all of these tools support themselves through fees charged directly to users (charges of $10 to $30 per month are common), though a few also offer free services with restricted bandwidth.” Hal Roberts, Ethan Zuckerman, Jillian York, Robert Faris and John Palfrey, “2010 Circumvention Tool Usage Report,” Harvard Berkman Center for Internet and Society (October 2010): 4, http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/2010_Circumvention_Tool_Usage_Report.pdf.

88. Andrew Quinn, “U.S. Develops ‘Panic Button’ for Democracy Activists,” *Reuters* (25 March 2011), http://www.reuters.com/article/2011/03/25/us-rights-usa-technology-idUSTRE72O6DH20110325.

89. Maggie Shiels, “On Iran’s Virtual Front Line,” BBC News (6 August 2009), http://news.bbc.co.uk/2/hi/technology/8186761.stm.

90. Aleks Krotoski, “MediaGuardian Innovation Awards: Austin Heap v Iran’s censors,” Guardian.co.uk (20 March 2010), http://www.guardian.co.uk/media/2010/mar/29/austin-heap-megas-innovator-award.

91. William J. Dobson, “Needles in a Haystack,” *Newsweek* (6 August 2010), http://www.newsweek.com/2010/08/06/needles-in-a-haystack.html.

92. Evgeny Morozov, “The Great Internet Freedom Fraud,” *Slate* (16 September 2010), http://www.slate.com/id/2267262.

93. United States Senate Committee on Foreign Relations, *Another U.S. Deficit – China and America – Public Diplomacy in the Age of the Internet* (15 February 2011): 42, http://lugar.senate.gov/issues/foreign/diplomacy/ChinaInternet.pdf.

94. Desmond Ang, “Falun Gong helps crack Iran’s web filter,” ABC News (Australia) (2 July 2009), http://www.abc.net.au/news/stories/2009/07/02/2614914.htm.

95. Hal Roberts, Ethan Zuckerman, Jillian York, Robert Faris and John Palfrey, “2010 Circumvention Tool Usage Report,” Berkman Center for Internet and Society, Harvard University (October 2010): 6, http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/2010_Circumvention_Tool_Usage_Report.pdf.

96. John Pomfret, “U.S. Risks China’s Ire with Decision to Fund Software Maker Tied to Falun Gong,” *The Washington Post* (12 May 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/05/11/AR2010051105154.html.

97. Author conversation with U.S. government official (14 April 2011).

98. Hillary Rodham Clinton, “Internet Rights and Wrongs: Choices & Challenges in a Networked World,” The George Washington University, Washington (15 February 2011), http://www.state.gov/secretary/rm/2011/02/156619.htm.

99. United States Senate Committee on Foreign Relations, *Another U.S. Deficit – China and America – Public Diplomacy in the Age of the Internet* (15 February 2011): 4, http://lugar.senate.gov/issues/foreign/diplomacy/ChinaInternet.pdf.

100. Kathleen Hickey, “DARPA Looks for Stealthier Internet Access,” *Defense Systems* (24 May 2010), http://defensesystems.com/articles/2010/05/21/darpa-safer-solicitation.aspx?admgarea=DS.

101. The State Department has expressed interest in funding some of these technologies. See U.S. Department of State, *Joint Request for Statements of Interest: Internet Freedom Programs* (3 January 2011).

102. Hillary Rodham Clinton, “Internet Rights and Wrongs: Choices & Challenges in a Networked World,” The George Washington University, Washington (15 February 2011), http://www.state.gov/secretary/rm/2011/02/156619.htm.

103. This Tunis Commitment reaffirmed the 2003 Geneva Declaration of Principles, which held, “Communication is a fundamental social process, a basic human need and the foundation of all social organization. It is central to the Information Society. Everyone, everywhere should have the opportunity to participate and no one should be excluded from the benefits the Information Society offers.” “Tunis Commitment,” World Summit on the Information Society (18 November 2005), http://www.itu.int/wsis/docs2/tunis/off/7.html.

104. David A. Gross, “Securing the Future of a Safe and Free Internet,” Remarks at the High Level Segment of the 2008 International Telecommunication Union Council (12 November 2008).

105. Sangamitra Ramachander, “Europe,” Open Net Initiative, http://opennet.net/research/regions/europe.

106. CNAS’ companion study on cyber security employs the term “cyber security” to mean “A blanket term that encompasses both 1) information assurance (measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities) and 2) and information security (protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction).” “America’s Cyber Future: Security and Prosperity in the Information Age,” Center for a New American Security (June 2011).

107. “The Information Security Doctrine of the Russian Federation,” Embassy of the Russian Federation in the Kingdom of Cambodia (2 September 2000), http://www.embrusscambodia.mid.ru/doc-information-e.html.

108. Will Englund, “In Russia, Official Proposes Curtailing Internet Freedom,” *The Washington Post* (8 April 2011), http://www.washingtonpost.com/world/in-russia-official-proposes-curtailing-internet-freedom/2011/04/08/AFzUud2C_story.html.

109. After the United Arab Emirates BlackBerry ban, U.S. State Department spokesman P.J. Crowley said, “We think it sets a dangerous precedent… You should be opening up societies to these new technologies that have the opportunity to empower people, rather than looking to see how you can restrict certain technologies.” “U.S. Says UAE BlackBerry Ban Sets Dangerous Precedent,” *Reuters* (2 August 2010), http://www.reuters.com/article/2010/08/02/us-uae-blackberry-usa-idUSTRE67144P20100802.

110. Tom Gjelten, “Seeing the Internet as an ‘Information Weapon,’” National Public Radio (23 September 2010), http://www.npr.org/templates/story/story.php?storyId=130052701.

111. Ibid.

112. Details related to “Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems” come from extraordinary research assistance by the Harvard Law National Security Research Group, under the direction of Ivana Deyrup. For U.S. concerns about the Additional Protocol, see U.S. Department of Justice, *Council of Europe Convention on Cybercrime: Frequently Asked Questions and Answers*, http://www.justice.gov/criminal/cybercrime/COEFAQs.htm.

113. More precisely, the intermediary is generally not liable unless it knowingly hosts illegal material (e.g., content posted in violation of copyright protections) and refuses to remove it when notified.

114. “Intermediary Liability: Protecting Internet Platforms for Expression and Innovation,” Center for Democracy and Technology (April 2010): 8, http://www.cdt.org/files/pdfs/CDT-Intermediary%20Liability_%282010%29.pdf.

115. Sarah Lai Stirland, “Cisco Leak: ‘Great Firewall’ of China was a Chance to Sell More Routers,” *Wired* (20 May 2008), http://www.wired.com/threatlevel/2008/05/leaked-cisco-do/.

116. Paul Sonne and Steve Stecklow, “U.S. Products Help Block Mideast Web,” *The Wall Street Journal* (28 March 2011), http://online.wsj.com/article/SB10001424052748704438104576219190417124226.html?mod=googlenews_wsj.

117. Golnaz Esfandiari, “Nokia Faces Wrath of Iran’s Protestors,” *Radio Free Europe/Radio Liberty* (15 July 2009), http://www.rferl.org/content/Nokia_Faces_Wrath_Of_Irans_Protesters/1777717.html.

118. “Internet Enemies 2011: Burma,” Refworld (11 March 2011), http://www.unhcr.org/refworld/country,,,,MMR,,4d82269028,0.html; and “France, Netherlands Seek to Halt Internet Censorship,” Agence France Presse (8 July 2010), http://www.google.com/hostednews/afp/article/ALeqM5hobAcoL50p4irWBiWSSkmM5BQ7Gg.

119. “Censorship in China,” Amnesty International, http://www.amnestyusa.org/business-and-human-rights/technology/page.do?id=1101572.

120. “Principles - Freedom of Expression,” Global Network Initiative (no date) http://www.globalnetworkinitiative.org/principles/index.php#18.

121. According to the Global Network Initiative’s (GNI) Governance Charter, membership in the GNI can be terminated for “Failure to meet reporting or other participation requirements [and] Failure to meet compliance and evaluation requirements.” “Governance Charter,” Global Network Initiative, Section 4D, http://www.globalnetworkinitiative.org/charter/index.php#83.

122. Office of Senator Richard Durbin, “Durbin, Coburn Continue to Press Tech Companies on Human Rights Code of Conduct” (7 August 2009), http://durbin.senate.gov/showRelease.cfm?releaseId=316922.

123. Chloe Albanesius, “Egypt Turns to Sole Provider, Dial-Up for Internet Access,” *PC Magazine* (31 January 2011), http://www.pcmag.com/article2/0,2817,2378969,00.asp.

124. Chris Lefkow, “Google, Facebook, Twitter sound off on Egypt,” *Agence France-Presse* (2 February 2011).

125. Margaret Coker and Charles Levinson, “Rebels Hijack Gadhafi’s Phone Network,” *The Wall Street Journal* (13 April 2011), http://online.wsj.com/article/SB10001424052748703841904576256512991215284.html.

126. Hillary Rodham Clinton, “Remarks on Internet Freedom,” the Newseum, Washington (21 January 2010), http://www.state.gov/secretary/rm/2010/01/135519.htm.

127. Ed Black, “Google, the Internet and China: A Nexus Between Human Rights and Trade?” Testimony before the Congressional Executive Committee on China (24 March 2010).

128. Korea-U.S. Free Trade Agreement, Article 15.8 “Cross Border Information Flows” (1 June 2007), http://www.ustr.gov/sites/default/files/uploads/agreements/fta/korus/asset_upload_file816_12714.pdf.

129. Mark Lander, “U.S. Hopes Exports Will Help Open Societies,” *The New York Times* (7 March 2010), http://www.nytimes.com/2010/03/08/world/08export.html.

130. “BIS Updates Encryption Export Rule; Revised Rule Streamlines Review Process, Enhances National Security,” Department of Commerce Bureau of Industry and Security (25 June 2010), http://www.bis.doc.gov/news/2010/bis_press06252010.htm.

131. As an example of one way in which U.S. export controls can chill online freedom, Evgeny Morozov cites the case of Yaraslau Kryvoi, a Washington-based Belarusian whose web-hosting firm suspended its blog because Belarus was subject to U.S. trade sanctions. Evgeny Morozov, “Do-It-Yourself Censorship,” *Newsweek* (7 March 2009), http://www.newsweek.com/2009/03/06/do-it-yourself-censorship.html.

132. John Markoff, “At Internet Conference, Signs of Agreement Appear Between U.S. and Russia,” *The New York Times* (15 April 2010), http://www.nytimes.com/2010/04/16/science/16cyber.html.

133. Ryan Singel, “Cyberwar Hype Intended to Destroy the Open Internet,” *Wired* (1 March 2010), http://www.wired.com/threatlevel/2010/03/cyber-war-hype/.

134. David Talbot, “Dissent Made Safer,” *Technology Review* (May/June 2009), http://www.technologyreview.com/printer_friendly_article.aspx?id=22427. Also see question by Harvard Law School’s John Palfrey to Ron Deibert, Director of the University of Toronto’s Citizen Lab: “What’s going to happen when someone does something terrible using Psiphon, plans a terrorist attack, for instance? What’s Psiphon’s liability?” Ethan Zuckerman, “Ron Deibert on the History and Future of Psiphon,” *My Heart’s in Accra* (31 January 2007), http://www.ethanzuckerman.com/blog/2007/01/31/ron-deibert-on-the-history-and-future-of-psiphon/.

135. For example, Robert Vamosi writes that “TOR is endorsed by the Electronic Frontier Foundation (EFF) and is designed for individuals to circumvent Web censorship in countries such as China, however, the network could be used by criminals or even terrorists.” Robert Vamois, “Hacking Anonymity,” *CNET Reviews* (20 October 2006), http://reviews.cnet.com/4520-3513_7-6654986-1.html?tag=untagged.

136. The FBI and other U.S. government agencies have been relatively vocal about their concerns regarding anonymity provided by encryption technologies for over a decade. In 1998, *The Washington Post* reported that “FBI Director Louis Freeh is the most outspoken advocate of encryption restrictions … now, Freeh complains, new technology is helping criminals more than the police. One Freeh proposal is that all users of powerful encryption software be asked to turn over their keys to a third party, so that law-enforcement officials can gain access to them with a court order.” More recently, Dr. Marco Gercke, director of the Cybercrime Research Institute, wrote “Encryption is a classic example of a neutral technology, since as it is not only used to hinder investigations but also to prevent unauthorized access to information … The latest operating systems offer the possibility to encrypt computer data with the click of a mouse, making it difficult for law enforcement agencies to break the encryption and access the data.”Dan Froomkin, “Deciphering Encryption,” *The Washington Post* (8 May 1998) and Dr. Marco Gercke, “From Encryption to Failure of Traditional Investigation Instruments,” *Freedom From Fear Magazine*, http://www.freedomfromfearmagazine.org/index.php?option=com_content&view=article&id=311:from-encryption-to-failure-of-traditional-investigation-instruments&catid=50:issue-7&Itemid=187.

137. “Clipper Trip,” Crypto Museum, http://www.cryptomuseum.com/crypto/usa/clipper.htm.

138. Evgeny Morozov, *The Net Delusion* (New York: PublicAffairs Books, 2011): 176.

139. Jaikumar Vijayan, “U.S. Web Site Said to Offer Strengthened Encryption Tool for Al Qaeda Backers,” *Computerworld* (23 January 2008), http://www.computerworld.com/s/article/9058619/U.S._Web_site_said_to_offer_strengthened_encryption_tool_for_al_Qaeda_backers?taxonomyId=16&intsrc=hm_topic.

140. Ellen Nakashima, “Pentagon Considers Preemptive Strikes as Part of Cyber-Defense Strategy,” *The Washington Post* (28 August 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/08/28/AR2010082803849.html.

141. “We have to have offensive capabilities, to, in real time, shut down somebody trying to attack us,” said GEN Keith Alexander. “You need autonomous decision logic that’s based on the rule of law, the legal framework, to let network defenders know what they are allowed to do in the network’s defense.” C. Todd Lopez, “LandWarNet opens with 4 keys to Internet security,” *Army News Service* (3 August 2010), http://www.army.mil/-news/2010/08/04/43256-landwarnet-opens-with-4-keys-to-internet-security/.

142. See the Protecting Cyberspace as a National Asset Act of 2010, introduced by Senators Joe Lieberman, I-Conn., Susan Collins, R-Maine and Ted Carper, D-Del.; the senators in February 2011 introduced a reworked bill, the Cybersecurity and Internet Freedom Act.

143. Declan McCullagh, “Internet ‘Kill Switch’ Bill Gets a Makeover,” *CNET News* (18 February 2011), http://news.cnet.com/8301-31921_3-20033717-281.html.

144. Shawna Shepherd, “White House conference tackles bullying,” CNN (10 March 2011), http://www.cnn.com/2011/POLITICS/03/10/obama.bullying/index.html.

145. Department of State, *Joint Request for Statements of Interest: Internet Freedom Programs* (3 January 2011).

146. Ibid.

147. As Rebecca MacKinnon has suggested, had Chinese dissident Shi Tao understood that Yahoo could share his email with Chinese police forces, he may have found more secure methods of transmitting articles to dissident websites. Rebecca MacKinnon, “China, the Internet, and Google,” Testimony before the Congressional-Executive Commission on China (1 March 2010): 7.

148. U.S. laws currently restrict exports to Syria. For more on the restrictions and their effects on Syrian Internet users, see Jillian York, “U.S. Gives Iran More Net Freedom – But What About Syria?” Guardian.co.uk (16 June 2010), http://www.guardian.co.uk/commentisfree/libertycentral/2010/jun/16/internet-iran-syria-export-controls.

About the Center for a New American Security

The mission of the Center for a New American Security (CNAS) is to develop strong, pragmatic, and principled national security and defense policies. Building on the expertise and experience of its staff and advisors, CNAS aims to engage policymakers, experts and the public with innovative fact-based research, ideas, and analysis to shape and elevate the national security debate. A key part of our mission is to help inform and prepare the national security leaders of today and tomorrow.

CNAS is located in Washington, D.C., and was established in February 2007 by Co-founders Kurt M. Campbell and Michèle A. Flournoy. CNAS is a 501(c)3 tax-exempt nonprofit organization. Its research is nonpartisan; CNAS does not take specific policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the authors.

Center for a New American Security
1301 Pennsylvania Avenue, NW
Suite 403
Washington, DC 20004

TEL 202.457.9400
FAX 202.457.9401
EMAIL info@cnas.org
www.cnas.org

Production Notes

Paper recycling is reprocessing waste paper fibers back into a usable paper product.

Soy ink is a helpful component in paper recycling. It helps in this process because the soy ink can be removed more easily than regular ink and can be taken out of paper during the de-inking process of recycling. This allows the recycled paper to have less damage to its paper fibers and have a brighter appearance. The waste that is left from the soy ink during the de-inking process is not hazardous and it can be treated easily through the development of modern processes.

PRINTED WITH SOY INK™

Center for a
New American
Security

STRONG, PRAGMATIC AND PRINCIPLED
NATIONAL SECURITY AND DEFENSE POLICIES

1301 Pennsylvania Avenue, NW
Suite 403
Washington, DC 20004

TEL 202.457.9400
FAX 202.457.9401
EMAIL info@cnas.org

www.cnas.org

ISBN 978-1-935087-45-8
50999>
9 781935 087458

PRINTED WITH SOY INK™ Printed on Post-Consumer Recycled paper with Soy Inks