DIPLOMACY
DEVELOPMENT and
SECURITY in the
INFORMATION AGE

Shanthi Kalathil EDITOR

georgetown university school of foreign service institute for the study of diplomacy

Georgetown University

Founded in 1789, Georgetown University is a distinctive educational institution—a national university rooted in the Jesuit tradition of social justice and education of the whole person, committed to spiritual inquiry, engaged in the public sphere, and invigorated by cultural pluralism. Georgetown's location in Washington, D.C. provides a unique platform for Georgetown faculty to make their expertise and talents available both to policy institutes in Washington as well as to a wider international audience. No other American university is better positioned to foster a critical dialogue on global issues.

http://www.georgetown.edu

Edmund A. Walsh School of Foreign Service

Georgetown University and the School of Foreign Service exist in the most fertile international arena in the world, allowing the School to establish globally renowned competitive programs and centers as well as offer first class undergraduate and graduate degrees. Founded in 1919, the School remains committed to educating students and preparing them for leadership roles in international affairs.

http://sfs.georgetown.edu

Institute for the Study of Diplomacy

The Institute for the Study of Diplomacy (ISD), founded in 1978, is the School's primary window on the craft of diplomacy. The Institute's constituencies include diplomats, scholars, and Georgetown students. ISD staff and associates teach courses, organize lectures and discussions, mentor students, and participate in university life. The Institute also convenes conferences and working groups, and sponsors and publishes research. ISD international affairs case studies are used in classrooms across the United States and around the world.

http://isd.georgetown.edu

DIPLOMACY DEVELOPMENT and SECURITY in the INFORMATION AGE

Shanthi Kalathil EDITOR

Séverine Arsène

David Faris

Sarah Granger

Craig Hayden

James Herlong

Gerald Hyman

Lorelei Kelly

Andrew Puddephat

Joseph Siegle

James Valentine

georgetown university school of foreign service

institute for the study of diplomacy

ABOUT THE INSTITUTE

The richness of Georgetown University and its close relationship to Washington's politics and diplomacy offer boundless opportunities for an institute like ours. ISD's presence at Georgetown reflects the university's dedication to study and action and to social justice and global engagement.

The contours of diplomatic engagement are changing rapidly, as are the environments in which diplomacy is crafted, honed, and practiced. New media have changed the pace and content of political awareness and provided new tools for diplomacy. Porous borders challenge national sovereignty, the conduct of war, and the ways in which peace can be pursued. The capacities of states and multilateral institutions to prevent and fix problems are challenged daily by the enormous agendas that global issues like health and the environment pose for the international community.

Each of these global issues tests the assumptions and practices of traditional diplomacy. Perhaps most important for our work, nonstate actors—whether benign or malign, constructive or disruptive—now play increasingly important roles in the conduct of international politics and finance and are leading us to think differently about global finance and development, conflict and reconciliation.

These new issues, conditions, and actors are helping to refine, and perhaps redefine, what diplomacy means and how it is conducted. They set the context for ISD's work as we identify issues that are global in origin and diplomatic reach, and examine carefully the ways that states and nonstate actors respond to them and to one another.

This agenda infuses our studies, teaching, training, and outreach. Our associates and colleagues join with the many communities that engage the important, hard, enduring, and often unanswered issues that define our global polity. Together, we study the ways that diplomacy can shape global action and serve our complex global societies. And as we have for three decades, we continue to take our cues from the worlds of politics and education and from the university's generous and abiding commitments to the worlds of words and deeds.

Institute for the Study of Diplomacy
Edmund A. Walsh School of Foreign Service
Georgetown University, Washington, DC 20057–1025

CONTENTS

Introduction

Diplomacy in the Information Age

Development in the Information Age

Security in the Information Age

Acknowledgments

This volume began as a series of discussions with Paula Newberg, then the head of the Institute for the Study of Diplomacy (ISD) at Georgetown, who was particularly interested in exploring the complexities of international affairs in the information age. Her encouragement and insight helped shape the themes that have emerged here. I owe her and the Institute a debt of gratitude for providing a welcoming platform to test and argue new ideas.

Additional food for thought was provided through the lively lunch meetings of the Institute's I-Diplomacy group, which met on a quarterly basis to hash over issues ranging from Chinese soft power to the changing role of diplomats.

Special acknowledgement and thanks are due to Katie Seckman and Charlie Dolgas at ISD. Katie skillfully managed the processes leading up to this volume, somehow eliciting order from chaos. Charlie's thoughtful comments, and his patient shepherding of the papers through publication, proved invaluable.

The funding for my work on this project was provided by the Yahoo! Business and Human Rights Program. I am thankful to them for making this possible. The Institute also wants to thank the Joseph J. Schott Foundation for its support of the author working group and the printing of the publication.

Finally, my deep appreciation goes to this volume's stellar lineup of authors, who have together created an invaluable cache of knowledge. Their dedication to this task has helped provide a building block for future research and understanding of a crucially important, yet still emerging, area.

Shanthi Kalathil

Introduction

Transparency and Volatility: International Relations in the Information Age

Shanthi Kalathil

The information revolution is permanently changing the face of international relations. Wired, networked protestors help power and publicize the Arab Spring, leading to the downfall of authoritarian regimes long believed unshakable. Secret cables published by Wikileaks expose the mechanics of U.S. foreign policy decisionmaking to a global public. Chinese Internet users spread photo evidence to expose corrupt local officials. Israelis and Palestinians use video and social media to add another dimension to real-time conflict.

But what do these disparate events really tell us? The popular narrative generally holds that time and distance are collapsing, everything and everyone is scrutinized, filters are nonexistent, and nonstate actors hold disproportionate and ever-increasing power. While powerful, and containing some elements of truth, this narrative is rarely re-examined in the context of policy discourse or the decisions that arise from it.

There is far more to understand about international relations in what is commonly termed the information age. Changes in the speed, volume diversity, nature and accessibility of information, as well as the ways in which it is exchanged, have contributed to a variety of emerging and evolving phenomena. These include the rise of nontraditional security threats (cyber and otherwise), networked forms of organization, asymmetrical conflict, decentralization, recentralization, altered global governance structures, multicentrism, information asymmetry, new development models, contested global norms, and much more. All of these present challenges and opportunities for states and nonstate actors and require a substantial rethink of the lens through which we view international affairs.

Yet fresh thinking on these issues, while taken up by specialized academics, rarely makes it onto the public agenda. Such research tends to get tucked away into the vibrant but often impenetrable (to outsiders) fiefdom of communications research, such that followers of international affairs do not tend to encounter it on a regular basis, if at all. Thus, the initial analysis of events hardens into an accepted truth, and it becomes increasingly difficult to pose alternate narratives or even further explore the dominant one.

This working paper series intends to illuminate this narrative by delving further into the trends in international affairs that have been accelerated or otherwise augmented by the information revolution. Because this task could easily prove unmanageable, the series will examine in particular two separate but linked phenomena enhanced by the information age: heightened *transparency* and increased *volatility*.

As Craig Hayden notes in his paper for this series, both transparency and volatility have come to define the practice of contemporary diplomacy and international relations. While separate, they are increasingly inextricable, he argues—in that transparency is facilitated by the same information and communication technologies (ICT) that also promote instability, risk, and uncertainty in international affairs. Civil society actors—including nongovernmental organizations (NGOs), citizen journalists, and the broad public—have been most visibly adept at taking advantage of volatility to advance their interests as well as using heightened transparency to press for accountability. But states and other large institutional actors must also respond to these trends and in some cases are doing so innovatively.

The examples at the beginning of this paper illustrate transparency and volatility at work in international affairs. But anecdotes cannot usefully convey how transparency and volatility have themselves become globally shared conditions, values, and/or norms. Transparency, argues Hayden, does more than simply put information out there—it inculcates a shared value that information *should* be available. And while volatility as a term does not share the same normative emphasis, it, too, transcends individual instances of technology usage to embody a defining condition of diplomacy, development, and security.

Of course, transparency and volatility are hardly new concepts to observers of international affairs. Yet their salience has grown over the last decade and cannot easily be ignored. Moreover, it is easy for foreign policy practitioners to make misguided assumptions about their impact—assumptions that, if left unexamined, can lead to undesired policy outcomes. With traditional international and regional security concerns dominating the foreign policy agenda, these issues have received less attention than they deserve.

This series thus proposes to unpack the concepts of transparency and volatility across three major arenas of international affairs: security, diplomacy, and development. Each issue-area features two essays, each focusing on different aspects of transparency and/or volatility. Two additional essays (by Gerald Hyman and Joseph Siegle) examine the ramifications of the growing interplay between issue-areas in the information age. Some authors situate their research within the context of academic literature, while others are more focused on policy and/or operational contexts. Taken together, the papers in this series seek to usefully organize the issue under inquiry in order to render it manageable and understandable to a wider scholarly, policy, and practitioner audience.

While this paper series uses transparency and volatility as a framework for examining international relations in the information age, it does not necessarily place information and communication technologies at the forefront of the analysis. While some papers do focus on ICT, the purpose is not to minutely examine new forms of technology and their impact. Rather, the premise for this series is that ubiquitous global communication flows have, over time, created an encompassing information environment that nurtures transparency and volatility as pervasive conditions and/or guiding norms. This larger focus on the changing information environment is intentional; it is hoped that by broadening the focus beyond the narrow application of ICT, we may emerge with nontechnocentric solutions to a variety of complex problems.

In focusing on transparency and volatility, the papers in this series also serve to deconstruct the hype surrounding key concepts of the information age. For instance, entities from the World Bank to the U.S. government to Bono have lauded the virtues of "open data" and transparency. While these hold great promise, there is frequently a gap between rhetoric and reality. Increasingly, governments, corporations, and other large institutions extoll the concept of transparency in public while maintaining opaque practices. Moreover, the promise of transparency may serve as a cover for manipulation, deception, and misdirection. Just as "greenwashing" evolved in response to pressures for environmental responsibility, so might "clearwashing" become a common practice in the information age.

Other terms, such as "information dominance," "decision advantage," and anything beginning with the prefix "cyber," are bandied about frequently in security-focused circles but are not as frequently held up to scrutiny. The security-themed papers in this series offer context and explanation for these terms and, in some cases, propose alternatives to these concepts.

"Digital diplomacy" is also something of a buzzword that has been quickly adopted yet poorly understood. Much current writing on this practice tends to lead with technology, offering techcentric solutions to diplomatic practice while failing to account for the larger trends at work. Several authors in this series go beyond the dominant narrative of tweeting ambassadors to more fully explain the ways in which transparency and volatility have altered the landscape of international diplomacy and to offer tangible recommendations to those engaged in diplomatic practice.

DIPLOMACY

Of the three fields, diplomacy perhaps most visibly demonstrates the effects of heightened transparency and volatility. The authors in this section point out several broad trends affecting the policy and practice of diplomacy.

First, there is now a pervasive notion that diplomacy can and should operate out in the open. If, as David Faris notes in his paper, modern diplomacy has traditionally been defined as the practice of crafting open covenants, secretly arrived at, then the heightened transparency of the information age has perhaps irreversibly damaged this secrecy. Foreign policy is now "made in an environment of radically increased transparency, visibility and contention, which will lead inevitably to struggles over message discipline, engagement and policymaking in a more volatile world," he says.

This has both positive and negative implications. As Gerald Hyman points out, increased transparency can expose discussions of statecraft prematurely, before consensus is reached or while positions are still fluid. It can disrupt sensitive negotiations, exposing the bargaining stances of any or all parties in a conflict. It can also expose information, both classified and not, that can harm various interests (such as parties to a conflict who may have agreed to meet with NGOs or other neutral parties to seek a solution). But it can also help expose hypocrisy or double standards in policymaking, allowing a global audience to hold public officials to account for the gap between their words and their deeds.

Second, nonstate actors (and, more broadly, global public opinion) are not merely just participating but also are exerting a powerful influence on the practice of diplomacy. International NGOs can now bring attention to their agendas through skillful use of media; this has the effect of placing little-known conflicts, for example, on the global public agenda. States must become adept at quickly responding to public outcry over a growing number of issues, many of which may have remained cloaked in obscurity in the past. Ironically, while in the past governments may have had a hard time justifying engagement in such issues to their publics, they may now be faced with the opposite dilemma. "Cooling things down may now be at least as common as revving them up," says Hyman.

Finally, the practical definition of diplomacy is itself changing, blending traditional diplomacy with the subset of public diplomacy as well as aspects of development and governance. If diplomacy is now increasingly conducted out in public, then engaging credibly with multiple audiences is even more important. Yet even with the advent of concepts like the U.S. State Department's "21st Century Statecraft," practitioners of diplomacy are still struggling to understand this fusion, particularly when it comes to interacting with new actors on new platforms. In recent years public diplomacy has, at least on paper, embraced dialogue rather than monologue, emphasizing the "listening" role of diplomatic outposts. This emphasis has now spread to the more traditional side of diplomacy, with embassies attempting to engage with multiple publics through social media. It remains to be seen how effective state bureaucracies are at managing this new, fused form of diplomacy, since few studies have yet systematically reviewed and assessed these undertakings.

Hyman's paper explores these and other trends, focusing in particular on the intersection between diplomacy, development, and new media. The presence of new actors, such as citizen journalists, has helped elevate the agenda-setting role of the public, he says, keeping highly localized conflicts higher on diplomatic and assistance agendas than they may otherwise have been. These new actors have also made it harder for autocratic governments to maintain their monopoly on information, even when they still retain extensive powers to regulate information flows.

For democratic governments, transparency has had complex effects, Hyman notes. It "illuminates without favoritism" and may help reduce overclassification of information. But it also serves to reduce the ground for quiet compromise, a crucial element of traditional diplomacy. "Deviating from hard official lines or initial principles, especially through testing of alternative compromises, is rendered more difficult by fear of exposure," he says. Premature exposure may also spoil useful diplomatic initiatives by opening them to public debate before they are yet ripe. In such fashion, transparency may compromise the effectiveness of long-term diplomatic initiatives.

Yet Craig Hayden argues in his paper that U.S. policymakers should see both transparency and volatility as opportunities to be seized, "in ways that reflect broader transitions in the diffusion of state power and the kinds of strategic arguments that drive diplomatic objectives." While U.S. foreign policy is increasingly geared toward "digital diplomacy" and is shifting its attention, tools, and tactics accordingly, Hayden argues that policymakers must move beyond the hype to understand the new form of ideal diplomatic engagement, which fuses traditional diplomacy, public diplomacy, and strategic communication.

This form of diplomatic engagement hinges on several working concepts for a new "social diplomacy," as he puts it—including persuading and engaging networks; understanding the once separate, now converging diplomatic functions of representation and governance; and the notion of optics, used as a metaphor to describe the capacity of diplomatic organizations to convene resources to solve transnational issues. This last function is particularly important, Hayden says, as the traditional role of the diplomat as information gatherer or source of contextual intelligence is eroding. Rather, network-oriented, relation-focused diplomacy can take advantage of both transparency and volatility to cultivate networks and increase the sensitivity of policymaking to interconnected constituencies.

Hayden says there has long been a sense that conceptions of political authority and influence have changed in ways that undermine traditional foreign affairs institutions. But the descriptions that frequently stem from this analysis must move beyond uncritical, narrow, or overly optimistic assessments of the relationship between technology to foreign affairs, particularly if they are to prove of value in transforming diplomatic structures.

David Faris, in his paper, also explores the interplay of citizen journalism, involuntary transparency, and policymaking in the digital age, narrowing the focus to recent events in the Middle East. Such events perfectly illustrate what he calls the disappearance of the "Age of Secrecy" in favor of the "Age of Sharing," characterized in part by the pervasive use of social media by nonstate actors to collectively read, annotate, and criticize government policies and actions. Policies that were possible in the Age of Secrecy, including U.S. dealings with autocratic and semiauthoritarian states in the Middle East, have become more difficult to execute in the Age of Sharing, he argues.

Faris also notes that another, third, dimension has been added to the classic "two-level games" of foreign policy, which traditionally involve negotiations between states, and again between states and their domestic constituencies. This third level is the networked elite, who serve as an intervening variable between state policies and mass global audiences. Understanding and interacting with the networked elite will be an essential skill set for policy actors in the information age, he concludes.

DEVELOPMENT

In recent years, the linkage between good governance and accountability to positive development outcomes has grown stronger. Bilateral donors, as well as multilateral organizations such as the World Bank and the regional development banks, have placed increasing emphasis on programs that support good governance and democracy. In this environment, the concept of transparency as both a value and a positive development outcome has gained a great deal of currency.

As the thinking goes, transparency is associated with a range of desired development results, including (but not limited to) good governance, empowered civil society, increased accountability, reduced corruption, improved service delivery, and so on. Indeed, "transparency" writ large has become increasingly celebrated, lauded by technocrats and Bono: "Open data and transparency will turbocharge ending poverty," he said during a November 2012 meeting with World Bank President Jim Yong Kim.

But what does transparency actually mean in the development context? Generally speaking, transparency is conceptualized in two separate, if linked, ways. The first treats transparency as, essentially, a normative component of accountability, good governance, and (if relevant) democratization in developing countries. In this sense, transparency is seen to be a desired result of programs that focus on building independent media, improving access to information legislation, promoting open government data, and bringing civil society into the process of governance through participatory budgeting and other measures. A frequently cited World Bank project in Uganda, for example, sought to reduce corruption in the education sector through implementing a public expenditure tracking survey: when it was revealed that centrally allocated funds were not reaching their intended targets, the public outcry and push for accountability led to subsequent funds reaching their intended schools.

Here, transparency is seen as a bottom-up phenomenon that facilitates state accountability in developing countries. It amplifies other good governance goals: enabling government accountability, reducing corruption, improving service delivery, etc. There are several examples of grassroots initiatives that have strongly and successfully advocated for transparency. Many cite the highly successful right to information programs at the state and local level in India as proof that such transparency-related initiatives can indeed demonstrate provable outcomes. That said, there is still a dearth of well-documented evidence regarding the success and failure of project-level transparency efforts.

The second conceptualization treats transparency as both policy matter and evolving global norm at the donor country level. In this sense, transparency is defined as disclosure of information by developed donor countries, particularly regarding the ways donors spend money, the outcomes of that spending, and the effectiveness of their development policies. As Andrew Puddephat notes in his paper, donors can no longer simply give aid; this aid must now be accountable to global civil society. This change, he says, "is driven by the belief that transparency will empower those in receipt of aid and reduce the risks of corruption or misuse of resources, thereby ultimately improving the quality of development." Official donor pronouncements, including the 2008 Accra Agenda for Action, call explicitly for donors to publicly and regularly disclose information on development expenditures to enable audit by the recipients of that aid. In this sense of the word, transparency facilitates a top-down sharing of information that also promotes accountability, but this time among donor countries regarding their development policies.

Puddephat argues that transparency is thought to increase the effectiveness of aid by empowering civil society organizations to monitor aid and to ensure public awareness of aid flows. Conversely, lack of transparency can undermine public confidence in aid, in both donor and recipient countries. Essentially, transparency does not guarantee accountability in the aid process, but the lack of it can make obtaining accountability much harder.

Yet, Puddephat says, despite much enthusiasm and rhetoric about the benefits of this second form of transparency, some donor countries are still unwilling to implement transparency practices, particularly concerning the impact of their aid projects. Studies commissioned by the group Publish What You Fund have found that aid information is often inaccessible, not systematically available, or hard to find. In what is already an unequitable process, Puddephat argues, opacity in aid reinforces a disempowering relationship between donor and recipient and isolates civil society from the aid process.

Why might the most developed countries be unwilling to fully embrace transparency in aid flows, despite rhetoric to the contrary? Puddephat posits that cost could be a deterrent, as well as fear of taxpayer revolt over the revelation of failed programs. "Exposing cases where aid has failed to produce results is a risk many donors aren't willing to take," he notes.

The emergence of new donors, such as China, may also have an effect on the global transparency-in-development agenda. These new players in the development field may be less willing to adhere to this agenda, preferring to set rules that benefit themselves more clearly. As both Puddephat and Séverine Arsène point out, China is emerging as a major player on the development scene, but it is doing so while challenging the consensus-driven, participatory model of development that has emerged over the last few decades. New donors may operate outside the establishment, traditional donor model which—at least on paper—supports transparency and accountability.

In her paper, Arsène examines more closely the role of China, particularly as relates to its involvement in the telecom sector in Africa. This sector is particularly important, she notes, as its development, and related legislation, affects not just social, political, and economic development but state security and sovereignty as well. Thus, even while Africa may not be China's top priority, Chinese aid and investment in Africa's telecommunications sector can have important knock-on effects.

In its own domestic telecom policies, China has famously chosen to leverage ICT for economic development while simultaneously attempting to control their political impact. Arsène points out that China may choose to promote this particular model within Africa and that it has the capacity to do so.

Indeed, she uses examples such as Ethiopia, where deep packet inspection can block proxy services, allegedly with support from China. However, Arsène is careful to point out that not all African countries where China has a presence have adopted such policies. The difference between various country policies seems to depend, she notes, on the level of development of ICT infrastructure and on the type of regime, rather than on the presence of Chinese aid or investment.

At a higher level, China may also influence the incorporation of transparency as a value in global governance norms for the Internet and other technologies. China's position on global Internet governance is one that deemphasizes the role of nonstate actors in governance (the current multistakeholder model) and prioritizes the role of the state. In doing so, it positions itself as a representative of developing countries' interests, says Arsène, arguing that multistakeholder governance gives more influence to developed countries. By pushing back against this model, China is attempting to reject the increased transparency and volatility stemming from the involvement of nonstate actors in favor of a more predictable, statist model.

SECURITY

Whereas the effects of heightened transparency are more readily evident in the development and diplomacy arenas, it is its associated condition, volatility, that surfaces more clearly in the security realm. Whether in the context of cybersecurity or fragile states, volatility affects national security at the level of grand strategy on down.

As Sarah Granger and Lorelei Kelly point out, the guns vs. butter battles of the Cold War era have been replaced by volatile, ongoing crises requiring political and social solutions. While security issues were previously framed as linear and measured, with predictably scalable solutions, they now appear chaotic, random, and unpredictable. Threats are distributed and human centered, requiring innovative and nontraditional solutions. Yet national security policy has not evolved to the point where it can comfortably anticipate and manage, rather than react to, this state of affairs as an ongoing condition.

The new era requires new tools and new policy frameworks, which emphasize, for example, credible influence over coercion, participation over exclusion, networks over borders, and resilience over reaction. They also require viewing security as a larger concept than war-fighting or hardware dominance, Granger and Kelly argue.

In this context, cybersecurity policy could be the catalyst for a much-needed conversation about these necessary shifts. Since addressing cybersecurity requires the integration of such diverse issues as security, offensive capabilities, defensive capabilities, deception, privacy, civil liberties, civic trust, Internet freedom, and global governance, as well as a focus on the inherently rapid rate of change (i.e., in the quality and quantity of attacks and perpetrators), it encompasses much of the complexities and inherent volatility that national security policy today must address. However, the terminology itself—the deliberate use of the throwback term "cyber"—helps place cybersecurity in a box, elevating it to "a dark chaotic threat only fit for military management," say Granger and Kelly. Because the terminology dictates how we respond to the issue, it has led to a situation where many stakeholders prefer no action at all (or simply abrogating civilian oversight of the issue) rather than dealing with the complexity of devising a policy process.

Fragile states also provide a complex testing ground for the heightened effects of volatility on international security, with ICT asymmetrically enabling the capability of small groups of nonstate actors who possess otherwise limited conventional military power, says Joseph Siegle in his paper. These groups are capable of disrupting the global system by using technology to communicate, plan, gather information, transfer funds, organize, and establish command-and-control networks from disparate and isolated locations around the world, he points out. Access to ICT may also allow certain nonstate actors to effectively push certain narratives, thus enabling spoilers' capacity to undermine the legitimacy of fledgling governments or provoke identity-group-based violence. The security implications of these threats are nontrivial, as are the developmental consequences.

Yet the flip side of the coin is also important. While volatility may amplify the reach of violent, antisystem actors in fragile states, transparency in an information-rich environment also provides important opportunities for governments and/or prosystem actors to engage with public opinion, thus shaping their own narratives. Understanding the importance of public opinion is crucial in fragile states; for instance, the greater the degree to which a government is viewed by its citizens as illegitimate, corrupt, or ineffective, the more susceptible it is to instability, Siegle says. While whitewashing such issues is no recipe for success, fledgling governments sometimes fall victim to not being able to successfully speak to their own successes. "Winning the battle for public support, then, is the linchpin for the development-security nexus in fragile states," notes Siegle, "and, for this, information is a vital tool."

Siegle suggests that in the long run, greater access to information can be a force for development and stability. In societies exposed to a diversity of information and ideas, he argues, authorities must respond to alternative proposals and justify their choices, theoretically leading to fewer ideologically driven and/or ineffective policies. Moreoever, spoilers have a harder time maintaining their narratives in an information-rich environment, as their claims can be held up to scrutiny. A vibrant information environment can also facilitate the sharing of development lessons learned, the adoption of best practices, and the introduction of new ideas that can help improve living standards. Watchdog groups can make use of heightened transparency to spotlight corruption, monitor elections, and help improve oversight of government—all of which enhance the efficiency and equity of government, contributing to greater stability. In fragile states and some developing countries, the expansion of the information-rich environment thus presents a tradeoff between greater short-term volatility and the long-term, institutionally based benefits of transparency, he concludes.

Finally, James Valentine and James Herlong discuss the practical aspects of transparency and volatility, particularly as they pertain to U.S. national security strategy. In doing so, they also question the significance of certain terminology used heavily in the context of U.S. military and intelligence documents: "information dominance" and "decision advantage." Both terms are predicated on the idea that information and its associated technology provide strategic advantage in national security. Such terms, they say, misguidedly focus attention on the accumulation of overwhelming amounts of information through technological superiority. "Because of our modern degree of transparency, in the greatest paradox of the 'information age,' information doesn't matter," they argue.

Rather than "information dominance," the United States (and other states) should be focused on what they term "cognitive dominance," a concept that attempts to go beyond information dominance by shifting the emphasis from ICT to human resources and their associated expertise. Cognitive dominance, as Valentine and Herlong define it, includes depth of useful and relevant knowledge, expertise, and experience; the ability to generate more accurate and precise conclusions than one's adversary; the agility to marry the right information with the right expertise; the ability to protect all parts of this network from disruption and exploitation; and the resilience to rebound from major losses or catastrophes. As a test case, Valentine and Herlong examine China's cognitive dominance in the realm of cyberwarfare capabilities. They conclude that, in this instance, China has successfully executed a strategy of cognitive dominance, giving it the tools to manage increased volatility.

FRAMING FOREIGN POLICY IN AN ERA OF TRANSPARENCY AND VOLATILITY

For decades, the fields of diplomacy, development, and security evolved slowly but, at their core, varied little. Now, within the space of the last several years, they have become more complex, less stable, and less predictable. As Gerald Hyman notes in his paper, "It is part of the work of this new era to maximize the advantages of the new information age and to minimize its disadvantages."

To do this, policymakers must acknowledge that surviving in this new era requires more than applying some kind of ICT "patch," the way one might update software. This new era is not about technology per se but rather about applying a new lens for understanding international relations.

Taken as a whole, the papers in this series give rise to several broad suggestions for policymakers and practitioners of foreign policy.

To better understand and devise solutions for the information age, do not lead with technology.

Because transparency and volatility derive from the technologies that power the information age, it is easy to assume that policy prescriptions should be based on ICT and its supposed impacts. But discussions of "digital diplomacy," "ICT for development," or "cyberwar" sometimes miss the point. As Valentine and Herlong argue, amassing ever greater amounts of information, or the technology to acquire it, no longer necessarily confers strategic advantage. "Where information dominance focuses on information, IT [information technology], and security to create a decisional and thus competitive advantage, cognitive dominance focuses on knowledge, people, and active resilience," they point out.

In the same vein, adapting diplomatic institutions to transparency and volatility does not mean opening policymaking to the entire global public; as Hayden puts it, "The United States, for example, should not render its foreign policy from a social media plebiscite." But shaping diplomatic institutions around an ethos of listening (which can use social media and other applications as a platform), several authors argue, demonstrates credibility and provides benefits to the diplomatic process by adding insight and intelligence.

Joseph Siegle notes that true impact requires reform-minded actors to effect meaningful change for ordinary citizens; technological tools must be anchored in organizational structures that can analyze, inform, and mobilize around key reforms and sustain the process over time. These institutional elements go far beyond technology and speak to the resilience of the societies in which they are embedded.

Transparency and volatility are inherently difficult for large bureaucracies but promise opportunities for innovation in statecraft and other areas.

As Craig Hayden points out, transparency and volatility are not just buzzwords for ways in which the field of international relations has changed. Nor are they conditions that diplomats, military planners, and policymakers should innately fear, despite bureaucracy's instinct to keep situations stable and information closely held. These conditions should be "posed in proactive terms, rather than conditions that simply hinder strategic thinking, because they ultimately impact the practical dimension of state power: how diplomats translate foreign policy into workable programs and campaigns," says Hayden.

Of course, translating into workable practices must be done with a considerable degree of finesse. Diplomats in the Middle East will continue to play a key role in policymaking and mediation, says David Faris, but they must do so with newfound appreciation for public opinion as channeled through the networked elite, while maintaining a degree of caution about the representativeness of those elites. Influencing the influencers will require "building horizontal networks of trust and reciprocity between lower-level members of the hierarchy, easing restrictions on the production of content by government employees and diplomatic personnel, and understanding that lifting barriers will lead to the occasional embarrassment when someone says something that was unfiltered and unwelcome."

Diplomats must genuinely engage with, and embed themselves in, local social media networks in order to combat misinformation and maintain the credibility of information. This does not mean using social media technologies as "high-tech soapboxes," as Faris puts it, but to engage in genuine back-and-forth dialogue with followers in their own languages. Moreover, this back-and-forth exchange must take place in real time, at the speed of a typical exchange—that is, not at Washington speed, requiring time for multiple layers of approval.

While transparency and volatility can have positive impacts, they also may be manipulated to suit various actors' aims.

Transparency in international affairs has a primarily positive connotation, particularly as it pertains to the idea of holding the powerful to account. Yet these normative aspects of transparency are not automatic, nor do they flow automatically as a by-product of ubiquitous communication in the information age. Right to information campaigners in India, for instance, did not simply depend on the passive diffusion of technology to gain transparency at the local level; it took years of hard work, paid for sometimes with lives, to institute even basic access to information reforms.

Moreover, the idea of transparency as a positive value can be used as a shield for the powerful to hide behind; recent surveys have critiqued a multitude of countries for taking the positive step of passing freedom of information laws but then failing to effectively comply with them. With open government data now the Next Big Thing on the transparency agenda, it remains to be seen how well both developing and developed country governments live up to its inherent promise. The allure of transparency as a desired value may lead to "clearwashing," or applying a veneer of transparency to business as usual.

Volatility also leaves the door open for manipulation, particularly when parts of the global public are not media literate. Siegle cites the example of spoilers affecting narratives in fragile states, for instance. The information revolution has amplified the reach and potential impact of global public opinion, forcing policymakers to adjust for its potency. But public opinion may be a force for destabilization and chaos if it is *uninformed* public opinion. Public information literacy, thus, is a key aspect of ensuring that publics are not misled or manipulated.

To harness opportunities in the information age, states and nonstate actors alike should focus on a strategy of resilience, credibility, and adaptability.

The themes of resilience, credibility, and adaptability resonate through many of the papers in this series. Taken together, they form the crux of a proactive approach to the challenges and opportunities of transparency and volatility.

Resilient societies, say several authors, are well placed to respond to the volatile shocks of the information age. Resilience is already exemplified by a variety of institutions, say Granger and Kelly, from redundant data storage to distributed power grids to strong community identity. While hierarchical governments and bureaucratic structures have limited flexibility, even they can understand that it is easier, and less costly, to manage risk than it is to manage crisis. Resilience, therefore, is not just an ideal option but also a sensible (and cost-effective) one.

State engagement with nonstate actors is an important part of resiliency: The depth of civil society networks has been shown to be a key predictor of resilience and the success of democratic transitions, Siegle notes. Stiff, hierarchical, nonparticipatory organizations or institutions are likely to find it more difficult to cope with unpredictability or exposure.

The concept of resilience in diplomacy, development, and security is already taking root in various institutions. The U.S. Agency for International Development (USAID), for instance, recently launched a "resilience agenda," defining resilience as "the ability of people, households, communities, countries, and systems to mitigate, adapt to and recover from shocks and stresses in a manner that reduces chronic vulnerability and facilitates inclusive growth."[1]

Credibility, particularly in the realm of diplomacy, has always been the coin of the realm; now, in an era of competing voices, narratives, and loyalties, it is crucial. Heightened transparency, of course, means that credibility is ever more difficult to fake. Credibility does not mean telling various audiences exactly what they want to hear; rather, it may be exemplified by in-depth engagement and a clear explanation of positions as well as adopting the ethos of listening recommended by many of our paper authors. This ethic, says Craig Hayden, does not mean foreign policy practitioners should abandon the self-interested aspect of their strategic calculus or completely disavow the power politics of previous eras. At its crux, credibility reflects the acknowledgement that publics are key to diplomatic success.

Adaptability is the value perhaps most inherently linked to the technologies that characterize the information age, but its adoption in policy structures is not as easy as simply using a new technology. National security and other bureaucracies accustomed to rules and procedures that have existed for time immemorial (and that presumably were created for good reasons) will not easily transform into flexible, easily morphing structures. Yet, as Granger and Kelly point out, in this era "threats will be diverse and dispersed; therefore, the capability to respond must follow suit." Wholesale bureaucratic change is difficult, perhaps impossible; but efforts such as the U.S. State Department's 21st Century Statecraft reflect a willingness to adapt that should be lauded, even if the practice sometimes falls short.

Ultimately, this series seeks to spark better and further understanding of the changing face of international affairs in the information age. This includes ensuring that analysis is not confined to an echo chamber of communications scholars or technology adherents. The papers presented here make the case that transparency and volatility characterize both the present and foreseeable future of international affairs. Understanding the relevance of these conditions should be considered foundational for any scholars, analysts, and policymakers concerned with international affairs today.

[1] USAID, "The Resilience Agenda" (Washington, DC: 2012). http://transition.usaid.gov/resilience/ResilienceAgenda2Pager.pdf.

Diplomacy in the Information Age

Social Diplomacy, Public Diplomacy, and Network Power

Craig Hayden

INTRODUCTION

What are the consequences of a *social* turn in U.S. diplomacy—in terms of policy, practice, and governance? What is the source of this transformation? There is no shortage of sensationalist claims about how *technology* has brought about a "digital diplomacy," claims that are also met with strident skepticism.[1] At the risk of some controversy, however, it is reasonable to argue that the social consequences of new media technologies have indeed resulted in tectonic shifts in the attention, tools, and tactics of U.S. diplomacy.

One way to understand this change is in the anticipated strategic audiences and interlocutors for U.S. diplomacy—and how this transforms the expected scope of impact. For example, according to Anne-Marie Slaughter, the former State Department director for Policy Planning, U.S. foreign policy is building structures that may not be visible for some time. Speaking to the UK (United Kingdom) Parliament in 2012, Slaughter argued that the biggest development in foreign affairs is the rise of *societies* as agents in the international system.[2] U.S. foreign policy, therefore, is increasingly geared toward "seeing" a country as both a government and a public, while at the same time leveraging connections as a "convener" to cultivate domestic and international networks.

Diplomatic practice, driven in part by the cultural and social consequences of ubiquitous communication technology, is transforming as a result of this crucial context. But technology is more than a tool—it carries socially constructed values, procedures, and expectations that are as much an affordance of the technology as they are a reflection of the world they help create. Transparency and volatility are two aspects of technological transformation that impact diplomacy.

The purpose of this paper is to unpack two concepts, *transparency* and *volatility*, as technologically derived conditions that impact the conceptualization and implementation of U.S. diplomatic practice. It presents these concepts as conditions that can be realized as *opportunities* to be seized in ways that reflect broader transitions in the diffusion of state power and the kinds of strategic arguments that drive diplomatic objectives. This paper draws upon speeches, policy statements, and initiatives conducted by the U.S. government to assemble a working understanding about how the United States has recognized the requirements of international influence and is attempting to reconfigure existing institutions to adapt to pressing demands of transparency and volatility. The paper also explores how these efforts reflect more global trends in the shifting burdens of diplomatic practices.

Strategic statements calling on the United States to leverage social media and network-centric platforms to facilitate or convene as an ideal form of diplomatic engagement also begin to illustrate the fusion of diplomacy, public diplomacy, and strategic communication.[3] The objective is to critically assess appeals to terms like "networks" and new forms of "power" in order to move beyond hype while distilling the more durable implications of a technological-charged diplomacy. In other words, this is an attempt to clarify how U.S. diplomatic practitioners "grasp the obvious" at the intersection of technology, culture, and diplomacy.[4]

TRANSPARENCY AND VOLATILITY: FROM CONTEXT TO PRACTICE

Transparency and volatility reflect pressing conditions that define the practice of contemporary diplomacy and international relations.[5] They have become salient given the ubiquity of global communication flows, the empowering potential of new and social media technologies, and the preponderance of nonstate actors that work to both hinder and enable the actions of states.[6] Transparency and volatility are also increasingly *inextricable* concepts tied to technology. Transparency is facilitated by the same technologies that promote instability, risk, and uncertainty in the business of international relations. Transparency as a context works to invite more actors into the fold of international affairs—but not through the well-worn habits and traditions of diplomatic actors.

The pluralization of international relations means that more actors matter and that these actors have *agency* in ways that are not conditioned by the "rules" of international politics.[7] In other words, transparency creates an element of risk and volatility.[8] If transparency engenders volatility, can these two interrelated contexts be *managed* effectively by diplomacy—the nuts-and-bolts infrastructure of international relations?[9]

Neither of these concepts are necessarily *new* to how U.S. policymakers and scholars understand the practice of international statecraft and its relation to information technologies.[10] Foreign policy analysts and political communication scholars have long been aware that *transparency* has at the very least impacted the *conditions* of foreign policymaking.[11]

But transparency has a broader conceptual implication for policymakers and practitioners. *Transparency* as a strategic concern renders state actions as always already available for public consumption: It is not just a problem for policymakers; it is built into the context of doing international politics.[12] Rather than consider transparency as a *hindrance* to information sovereignty—such as in the case of the U.S. response to the Wikileaks controversy—transparency also signals *opportunity* in the practice of statecraft and the formulation of foreign policy.

Understanding how transparency is an opportunity involves understanding how transparency has transformed what international "actors" (from individuals to networks to states), *actually do* with communication tools as much the social and cultural expectations that are now tied to such media technologies.[13] When these technologies begin to accrue meaning—such as the relation between social media and democratic organizing or *sousveillance*, the capacity of transparency becomes freighted with potential and purpose. Transparency becomes an ethic for the practice of international communication. It is not simply an ingredient for legitimacy in democratic politics, but it is a value that is fundamental to the everyday significance of communication technologies around the world.

Opportunity begins with the social role that transparency plays in conditioning credibility and legitimacy.[14] It is not so much that transparency puts information "out there." Transparency inculcates a shared value that information should be available—where communication is a value for its own sake.[15] Transparency can be a kind of *social power*, a norm or value that conditions how other states therefore must act.[16] Transparency as a policy guidance is already embedded in the universalizing ethos of the U.S. "Freedom to Connect" agenda and on display through U.S. ambassadors aggressively utilizing the potential of social media platforms to connect with their constituencies.[17] The currency of transparency as a value forces hard choices for practitioners, especially in the aftermath of U.S. resistance to the Wikileaks distribution of diplomatic cables.

Volatility is commonly understood as a description of the international political climate that implicates the unpredictability of previously stable relations among *and* within states. Yet it is not enough to say that foreign policy practitioners must contend with a context radically changed by new media technology.[18] Certainly, the way in which practitioners do their jobs is impacted by communication technologies that shorten decision-making cycles, increase the range of stakeholders, and heighten visibility. Yet volatility also implies the difficulty of reliable prediction; models and narratives that guide the practice of statecraft are increasingly unreliable. Volatility, likewise, suggests that the "art of the possible" in conducting foreign policy must adapt.

This paper proposes that volatility is more than an assessment of the political landscape. It is also an *institutional* condition that compels planners and policymakers to reconsider the traditional components of international statecraft: diplomacy, development, and the broader constellation of units that execute U.S. foreign policy.

Transparency and volatility are not just buzzwords for ways in which international politics has changed. Rather, we should consider these terms as pivot points in the way the United States recognizes its own institutional resources as useful or applicable to the tumultuous social and political changes witnessed abroad and at home. *Transparency* is a crucial context for global influence and also a means to devise programs and tactics that build off the ethic of transparency through public diplomacy and programs of 21st Century Statecraft. *Volatility* reflects the uncertainty in how traditional instruments and strategies continue to apply to foreign policy. These terms are posed in proactive terms, rather than in conditions that simply hinder strategic thinking, because they ultimately impact the practical dimension of state power—how diplomats translate foreign policy into workable programs and campaigns.

MAKING SENSE OF THE DIFFUSION OF POWER

What does an ambiguous term like "power" have to do with transparency and volatility in international affairs? Much has been said about the way in which "power" is now diffused.[19] Indeed, the *capacity* to get other actors to do something appears transformed in radical ways, especially when ideas like "collaborative power" seem to indicate that power may increasingly be less about "power over" than "power with." Former Undersecretary of State for Public Diplomacy and Public Affairs Judith McHale described power as fundamentally transformed, where the "bottom of the pyramid"—citizens, transnational advocates, and civil society has overturned dictators and fomented rapid political change.[20] Alec Ross, the U.S. special advisor for technology to the secretary of State speaks of a "post-Westphalian" system that is defined by a "massive shift in geo-political power taking place globally."[21] Ross bases his dramatic assessment about system volatility on the prevalence of "hyper-transparency"—a distinctly techcentric view.

From Joseph Nye's pronouncements about power "diffusion" to the compelling narratives of the

Arab Spring there is a palpable sense that conceptions of political authority and influence have irrevocably changed in ways that undermine traditional institutions of foreign affairs. This change is very often described as a direct consequence of information and communication technologies (ICTs).[22] But these depictions need to be unpacked to assess *why* such technologies are so transformative in ways that are available (or not) to policy planners and practitioners in order to move beyond uncritical, narrow, or overtly optimistic assessments of the relationship of technology to foreign affairs.[23] Behind the high-profile stories of transnational nonstate actors and civil society networks lies the uncertainties of those public servants and policyplanners that still represent state actors. Do new, so-called "disruptive" technologies facilitate conversations and organize foreign policy resources in ways that were previously unavailable?[24]

One way to address this question is to argue that the business of statecraft is increasingly carried out through technological platforms. Tools are redefining tasks and perhaps even purpose. As Senator Richard Lugar claimed in 2010, new and social media technologies have the capacity to reach audiences crucial to U.S. foreign policy objectives and provide solutions to pressing problems such as democracy promotion and counterterrorism. These kinds of arguments, however, suggest a strong convergence between the imperatives of public diplomacy and that of "traditional" diplomacy.[25] This is plainly evident in the 2010 Quadrennial Diplomacy and Development Review (QDDR), which situates the objectives of U.S. diplomacy with the mandate for an ambiguously articulated notion of "engagement."[26]

Part of the explanation for this lies in how communication is understood as relevant to politics in these kinds of important strategic statements.[27] If the business of statecraft is merely *representing* a nation-state's interest, then new media technologies are just new tools for old purposes. Especially when so much of the academic literature appears to rehash arguments about the diminished power of nation-states, how might we look to *diplomacy* as a source of innovation in both the strategy of statecraft as much as the tools that define diplomatic action?[28]

It is suggested here that we pause to consider the consequences of the "terministic compulsion" to carry out the implications of talk about new and social media technologies.[29] New social media technologies are used in relation-building, in storytelling, and as modes of alternative political expression, yet what are the *institutional* transformations emerging in the wake of these practices? If credibility and legitimacy are the currency of soft power, then understanding the social dimension of the networks enabled by ICTs is crucial to the practice of statecraft. At the same time, the social dimension of these technologies transforms the institutions of diplomacy that are busily adapting to new contexts. Getting past the hype surrounding new and social media technologies means identifying the connections between technology, volatility, and transparency in ways that can be translated into workable policy and practice solutions that signal real institutional change.

WORKING CONCEPTS FOR A SOCIAL DIPLOMACY

This paper hinges on some conceptual observations in order to make broader arguments about how U.S. diplomatic practice is changing. The following section explains these concepts and how they work to help understand the kinds of big, "structural" changes at work behind U.S. diplomatic institutions. It provides a provisional "vocabulary" in order to make arguments about how diplomatic institutions may have changed under conditions of transparency and volatility.

Transparency requires states to recognize *networks*, the fundamental unit of social organization underneath and above the nation-state, as the "target" of policy-making and partnerships to achieve ends.[30] Why? Because networks are a social structure that most readily carries out the business of politics.[31] This position is hardly new, but it requires reorientation to a *polylateral* view on getting statecraft accomplished.[32] Networks are significant to the workings of transparency, because we can witness the diffusion and propagation associated with transparency as a network effect. A transnational, cascading spread of information or its terminus in enclaves of interest is the property of network relations. But networks are more than just "maps" of relations. They are imbued with qualities that reflect the effect of those relations—shared ideas, norms, and values.

Persuading and Engaging Networks. How states can engage networks to change their actions or attitudes relies on two principal starting positions: influence through credibility (the reality of social power) and the impact of relational structure. Networks—whether they be extremist organizations, domestic political coalitions, or transnational advocacy groups—are defined in part by shared norms, values, and objectives. They are, in network theorist Manuel Castells's term, *programmed* with these concepts that serve to both direct action and to define identity within the network.[33] Understanding how networks police, motivate, and coordinate themselves is a key step toward understanding the contextual requirements of engagement rather than establishing a better message or market segmentation. There are no magic bullets for diplomatic messaging through networks.[34]

It is one thing to suggest that there will be more "networks" than treaties in the future of U.S. diplomacy.[35] It is quite another to suggest the practical implications for what that means. Networks have the *structural* effect of legitimizing shared beliefs and commonsense, and it is important for nation-states to recognize the durability of these properties. David Grewal points to ideas and practices that become "powerful" because they propagate across networks and become difficult to dislodge, like the pervasiveness of the English language as a global lingua franca.[36] When thinking about *influence*, a healthy understanding of networks as a social shape is important.

For example, statecraft may not be about finding the key influencers but about identifying boundary spanners and those on the "fringe" of networks that can propagate change. This means thinking about the relations and communication practices that make publics cohere *as publics*. For example, this might mean paying attention to where certain groups or individuals serve to connect different interest or identity-based groups as opposed to placing overt emphasis on opinion leadership. Anne-Marie Slaughter's argument is to focus on societies—to cultivate publics rather than seek out specific influencers. Slaughter quotes former Secretary of State George Schultz in her 2012 UK speech, to describe the business of diplomacy as "gardening"—to grow "confidence" and "understanding" through relation-building activities, providing means for foreign audiences to communicate among themselves and to build identification with the United States through everyday symbolic connections, such as U.S. Ambassador to New Zealand David Heubner spending 20 percent of his workweek tweeting about matters unrelated to U.S. foreign policy.[37] Yet it is unclear whether adaptation to social media has clearly demonstrated success for diplomats, as the controversial communications of U.S. Ambassador Michael McFaul appear to suggest, or the long-term impacts of the State Department's Digital Outreach Teams on critical arguments about the United States online.[38]

But this kind of *facilitative* turn toward a socially focused diplomacy required institutional adaptation. The change has been anticipated for some time. After the rapid growth of the Internet in the 1990s, emerging implications of the technology to shape social relations and change communication practice provoked speculation among U.S. critics that the institution of diplomacy needed to change. Jamie Metzl, a key public diplomacy advisor during the Clinton administration, argued in 2001 that this emergent context required a fundamental rethinking of diplomatic practice. "Because the conceptual space of a network is global and does not fully respect traditional boundaries, preparing individuals to engage in this space requires both conceptual and organizational change," according to Metzl.[39] For Metzl, diplomacy as a set of rules, practices, and traditions needed to adapt. While adaptation appears evident in recent U.S. practices and programs, it is less obvious that this facilitative turn has yielded favorable policy outcomes.

Representation versus Governance. Diplomatic adaptation is forged both in practice and at the level of *purpose*. Diplomacy is classically understood as a political institution charged with managing relations between peoples who choose to live apart.[40] Traditionally, this is conceived as "representation." Diplomats mediate relations between states. The idea of representation gets more complicated, however, when ambassadors engage in social media-based diplomacy—where the constituency is expanded and transparency is a tool. This is diplomacy in public.

But increasingly, diplomacy scholars have noted that diplomatic practice has expanded beyond the sphere of representation and has come to take on the burdens of governance. For example, around the world ambassadors are now posted to specific *issues* as well as to sovereign nation-states. In the case of the Untied States, they are also embedded in military operations to manage and facilitate state-building operations. As the notion of "21st Century Statecraft" reveals, U.S. diplomacy is increasingly about facilitating relations and providing solutions through the capacity of diplomats to convene a variety of international stakeholders. The point here is not simply to reiterate the relevance of "multilateralism." Rather, it is to suggest that diplomats are actively brokering governance decisions that circumvent traditional sovereign boundaries.

Optics. The notion of "optics" in this case is a metaphor to describe the unique capacity of diplomatic organizations to convene or marshal resources to solve transnational issues. The idea of *optic* turns the traditional concerns of information sovereignty on its head. Instead of states pursuing "markets for loyalty" through management of media spaces, the transparent information environment can be a tool for statecraft and not a liability. Alec Ross describes this convening power as central to the way in which diplomats can add value.[41] For Ross, diplomats can match technology developers with civil society actors or otherwise "local" experts who have intimate knowledge of issues that need attention.

The idea of diplomacy as optic comes at an important time. Sarah Wynn-Williams, an advisor to Facebook, argues that the traditional role of the diplomat as information gatherer or source of contextual intelligence is rapidly eroding.[42] The transparency afforded by information technologies like social media render this historical role as increasingly out of place. Diplomacy has indeed been concerned with identifying key influencers and points of leverage, but the idea of optic is intended to describe prescriptively how a network-oriented, relation-focused diplomacy can seize the prospects of transparency to identify and cultivate networks that can add the sensitivity of policy-making to increasingly interconnected constituencies.

What does this mean in practice? Diplomacy can leverage the resources of foreign ministries to become involved, to cultivate, and to empower international development, advocacy networks, and issue-defined organizations that are more intimately engaged in knowing about these international issues. Diplomacy in a facilitative mode can function as an open source clearinghouse for what Joseph Nye calls "contextual intelligence."[43] The following sections talk more in-depth about what these concepts mean in practice.

WHERE THE CHANGE IS HAPPENING

One of the key assumptions argued here is that diplomatic institutions—the norms, routines, and other kinds of organizational frames that shape how diplomatic practitioners and policymakers engage in their work—require some rethinking. The intention is not to say that "everything is now different," as diplomatic institutions have historically been defined by the inertia of past practice.[44] Yet it is important to recognize that diplomacy is an "infrastructure" of the larger field of international relations and not an *isolated* community of practice.[45] Diplomacy is not divorced from other social and cultural institutions or developments—like globalization. We cannot assume that the historically conservative and insulated practice of diplomacy is otherwise immune to technology-driven changes happening in culture, identity, and politics.[46] This section explores how particular aspects of diplomacy as an institution have changed and what this means in practice.

Actors

One of the problems with trying to parse the language of recent, vivid caricatures of international affairs is that it is not always clear about the impacts of the sweeping abstractions involved. While the Arab Spring has rightly captured attention as an indication of a power shift, the legacies of movement politics empowered by new, network-organizing forms have been around for some time.[47] At the same time, however, it is not necessarily prudent for policymakers to dismiss technology evangelists for naïve optimism.[48] To begin with, it is important to understand the nature of the actors involved.

The term "actors" can mean a lot of things in academic and policy-oriented treatments of international affairs. They are states, but they are also nonstate actors, such as terrorist organizations, civil society groups, nongovernmental organizations (NGOs), transnational advocacy networks, celebrities, and so on. Actors may also be considered communities built on physical or virtual infrastructures—that are oriented as temporary coalitions or collaborations to achieve a particular end. As political communication scholar Lance Bennett observed nearly a decade ago, the technological context for social action removes a variety of barriers to entry to become involved, whether as a dedicated international activist or a casual slactivist demonstrating support through "likes" on Facebook.[49] "Actors" can assemble relatively quickly.

For diplomatic practitioners, the problem is that planning policies and programs around actors is increasingly difficult, because actors are not as rigidly defined by specific kinds of political agency. Political communication scholar Andrew Chadwick demonstrated that there are "network repertoires" shared across social movement participants, political campaigners, and other kinds of online organizers that do not fit neatly into a historical catalog of what these actors do.[50] The dramatic success of Oscar Morales in organizing the "1 Million Voices against the FARC [Fuerzas Armadas Revolucionarias de Colombia–Revolutionary Armed Forces of Colombia]" campaign is one of many illustrations of how the labor of political power gets diffused and distributed. Put another way, we cannot just pay attention to roles assigned to actors, but also to actions and behaviors. International actorhood is no longer a stable category.

Behaviors

Public diplomacy scholar Robert Kelley's discussion of "evolution" in diplomatic affairs settles on this very point. Rather than talking about how the categorical concept of diplomacy or nation-states has changed, we should be focused on how particular practices associated with diplomacy are becoming visible among decidedly nondiplomatic actors, be they citizen diplomats, journalists, human rights workers, or cyber-activists.[51] The diffusion of diplomacy is a symptom of a larger social and technological context. This diffusion, however, need not be a negative development but rather a broader recognition that diplomacy is a practice that encompasses social relations as much as political ones.

As diplomacy scholar Geoff Wiseman argues, diplomacy cannot be discounted in whatever form of "new" diplomacy is devised to deal with the social media revolution and the rise of networked-based, transnational political actors.[52] Scandinavian diplomats seized on the potential of the Second Life virtual worlds platform for public diplomacy well ahead of other larger institutional actors.[53] Moreover, the South Korean government has encouraged an innovative arrangement of public/private partnerships to cultivate foreign policy objectives that are not firewalled within traditional foreign policy institutions.[54] In addition, the United States is working to facilitate collaborative encounters between civil society and technological developers. The diplomatic objectives of agenda setting, representation, and mediation are, in this sense, increasingly diffuse and distributed.

To that end, public diplomacy scholar Ali Fisher has written extensively on how insights from social networking analysis and marketing techniques that aggregate individual experiences can effectively transform the hierarchical nature of power in traditional statecraft. For Fisher, organizations like Amazon and Ebay are examples of how an asymmetrically powerful actor can accrue influence (or power) based on building communities.[55] Fisher draws from the "open source" movement in technology development to suggest a model for statecraft that is at once collaborative and inherently credible.[56] Foreign policy "solutions" in this view are best reached when they are not the product of hierarchical decisionmakers, but rather the provisional consensus of stakeholders invested in the issue at hand. The early involvement of civil society organizations in the World Summit on the Information Society conferences demonstrate this more expansive and inclusive process for global governance, but Fisher extends the argument to suggest that influence among the stakeholders necessitates collaboration from the ground up.

Fisher's take on diplomacy shares some conceptual terrain with the "participatory" trend in international development.[57] The distinction Fisher offers, however, is at the level of influence strategy. To deal with the effective "hyper-transparency" of a networked world, foreign policy should look to the potential of crowdsourcing. This is not to say that time-worn, strategic arguments for foreign policy are no longer relevant. The United States, for example, should not render its foreign policy from a social media plebiscite. Rather, the limited resources of nation-states to manage their interdependent policy obligations to deal with concerns that are increasingly transnational require both tools and strategies that are equally inclusive. Security dilemmas still exist, but their success increasingly involves a wider net of actors committed to shared purposes.

Shaping your diplomatic institutions around an ethic of "listening" symbolically demonstrates credibility to foreign constituencies but also invites perspectives, insight, and intelligence in the crafting of better policy. Fisher describes an "open source" diplomacy as a more viable route to influence given the nature of how publics already communicate and relate around subjects of mutual interest and identity.[58] But this paper also contends that an open source *optic* is just as crucial—a sensory capacity to forge a better, more *informed* policy calculus. This kind of "engagement" can cultivate the power to know and anticipate latent issues and emergent crises.

Conceptual Tools

What does this look like in practice? The United States has piloted this perspective through the so-called "21st Century Statecraft" concept. This concept is based on facilitating linkages between organizations that recognize problems or issues with technology and knowledge providers that can work to address these issues, such as empowering woman, improving democratic practice, and leveraging technological tools for development and conflict prevention.

This orientation toward *facilitation* as an operative term for statecraft (both in public diplomacy and traditional diplomacy) can be seen in the earlier writings of Anne-Marie Slaughter and in the work of British diplomacy scholar Brian Hocking, which emphasize the capacity of networks to accomplish diplomatic objectives and act as stakeholders in their own right.[59] In straightforward terms, networks are the most relevant actors that diplomatic agencies must deal with—as much as they are partners to getting the business of diplomacy accomplished. Hence the shift to a more *social* diplomacy.

But what is the "business" of a new social diplomacy?

A common observation among diplomacy commentators is that transparency is the irrevocable context for practice and that this is a *constraint* on what diplomats can do. What is less obvious is how transparency can be a tool for statecraft. Assuming transparency as an asset, however, suggests there is something different about statecraft than the (often secretive) preservation of agreements and interstate relations that secure state interests. Transparency can be an end in itself—such as the strategy embodied in the so-called "Freedom to Connect" agenda. But an Internet freedom agenda is closely shaped by an *ethic* derived from the technology. The entanglement of technology with policy is most evident in the "Freedom to Connect" agenda advocated by Secretary of State Hillary Rodham Clinton, where a narrative of technological empowerment animates a significant new direction in U.S. foreign policy and programs to facilitate the spread of so-called deliberative technologies.[60]

Communication scholars Shawn Powers and Will Youmans have argued that a public diplomacy based on providing so-called "deliberative technologies" illustrates the potential of leveraging technologies of transparency. Specifically, they propose that international broadcasters can provide technological platforms to encourage the development of democratic institutions within failed states—a key context for U.S. foreign policy objectives. Rather than subsidizing information, this form of public diplomacy would subsidize "deliberative development."[61] The idea extends the domain of diplomacy into the realm of social practice. They hold up the Voice of America pilot project "Middle East Voices" and the Al-Jazeera "Somali Speaks" projects as demonstrative of this concept.

Similarly, Steven Livingston's work on the capacity of new media technologies to sustain a new form of the CNN Effect directly addresses the diffusion of statecraft.[62] Livingston argues that the rise of geospatial social media technologies—like the crisis-mapping Ushahidi mobile phone platform—signals the diffusion of governance. These kinds of surveillance technologies provide both a constraint (publics can be forged around the monitoring of a state's activities) as well an opportunity to empower publics and cultivate long-term relations—the "gardening" that Slaughter implies in her society-focused diplomacy.

But perhaps the clearest statement that implicates the intersection of technology with foreign policy is in official U.S. arguments about strategic communication. Such a direct connection between technology and foreign policy thinking is plainly evident in the following excerpt from the 2012 Update to Congress on [the] National Framework for Strategic Communication:

> Events of the past 2 years have only reinforced the importance of public diplomacy and strategic communications in advancing U.S. interests. The continued rapid evolution of global communications is creating a landscape where our ability to engage and communicate with actors across societies is essential. The development of new media platforms is empowering global populations to reach out and communicate with others in ways they could not just a few years ago, and social and political movements are becoming savvier at mobilizing constituencies.[63]

Social media technologies are increasingly inextricable from strategic formulations about U.S. foreign policy, its methods, and its objectives. This has also sparked innovation and organizational learning at the level of practice—the *diplomatic post*.

In a 2011 conference on best practices in public diplomacy at the George Washington University, U.S. foreign service officers shared their experiences in trying to cope with the potential of new and social media technologies, along with their evolving mandate to conduct diplomacy for the United States. Public diplomacy officer Aaron Snipe described the challenge of trying to use the U.S. embassy Facebook page in Baghdad.[64] After the embassy staff adapted their practices toward speaking in the local language and reorienting content toward what the audience found useful and interesting, they noted a significant change in the attention they received from the Iraqi public as well as the kind of commentary and feedback.

Snipe described this as a fundamental "concept shift" in the way diplomats communicate with publics. Snipe argued that change was necessary in "how we communicate"—rather than having a better means of dissemination and transmission of messages. Snipe's comments highlighted the social context of the technology that ultimately affects the modes and ethics of the communication.

Rachel Graaf Leslie, likewise, noted the struggle to use social media as a means to recognize and counter misinformation in Bahrain during its political uprising in 2011.[65] Her experience highlighted the way in which the technological platform, along with what users "do" with its communication capacities, is not easily controlled, curated, or subject to verification. She noted that the social media sites provided by the United States were appropriated as a tool for conflict by social groups within Bahrain. This illustrates the risks inherent in the long game of Anne-Marie Slaughter's focus on convening and providing fora for communication.

These brief examples, however, describe the way in which *public* diplomacy has adapted to the context of transparency and volatility. The notion of "21st Century Statecraft" provides a policy template that invites analysis of how technology is integrated into translating strategy into practice.

21ST CENTURY STATECRAFT AND [PUBLIC] DIPLOMACY

The idea of 21st Century Statecraft is based on an expansive, polylateral view of diplomacy, where a multitude of nonstate actors are enabled by network technologies. The concept's principal evangelist at the U.S. State Department was Alec Ross, then senior advisor to former Secretary of State Hillary Clinton. Ross describes 21st Century Statecraft as an "agenda" that "complements traditional foreign policy tools with newly innovated and adapted instruments that fully leverage the networks, technologies, and demographics of our networked world."[66]

Such new diplomatic methods are deemed necessary because, as Ross declares, "the very clear evidence of recent years demonstrates that network technologies devolve power away from nation-state and large institutions." While the 21st Century Statecraft idea attempts to capture a range of problems and issues that U.S. diplomacy must confront, the concept is hard to separate from its technological underpinnings. As the QDDR states, "Technologies are the platform for the communications, collaboration, and commerce of the 21st century. More importantly, they are connecting people to people, to knowledge, and to global networks."[67] Twenty-first century statecraft is an inclusive attitude toward technology that sees it both as policy tool and policy itself.

What is the purview of diplomacy under this agenda? The business of U.S. statecraft is increasingly one of orchestrating and facilitating policy solutions made possible through technology. According to Ross, a "growing ecosystem of technology and developers" can be leveraged to achieve policy gains.[68] Social media and the social networks they foster function to direct diplomatic attention and drive the coordination of services and governance. Ross argues that the United States can look to "civil society to identify pressing problems, and then match these actors with technologists to develop solutions."[69]

To justify his claims, Ross paints a sweeping portrait of a world transformed in which U.S. diplomacy must operate. Technology has accelerated movement-making, as evidenced by the use of social media tools for political change. The information environment is also disrupted by such technology to destabilize the centrality of state actors in using information technology to manage the international environment. The United States must contend with the "hyper-transparency" of networked politics that transgresses entrenched political hierarchies and state borders.

Some high profile efforts of 21st Century Statecraft include the recruitment of university students to aid in new media efforts of the State Department known as the Virtual Student Foreign Service, collaborative events such as the Tech@State series of conferences that draw together technology developers and other nonstate actors, the Apps for Africa competition to develop mobile technology solutions for regional development, and other initiatives to promote women and mobile finance solutions in developing countries.[70] Twenty-first Century Statecraft has been manifested as foreign policy through the Freedom to Connect agenda, in which the United States promotes open access to the social, political, and economic benefits of information technology.[71]

Interestingly, Ross has demurred on the subject of *public* diplomacy and its relation to 21st Century Statecraft. During a presentation in 2012, Ross argued that 21st Century Statecraft should not be equated with public diplomacy. Rather, he offered that traditional public diplomacy "doesn't work in the digital age."[72] Ross's perspective on public diplomacy appears grounded in a more traditional and historical view of public diplomacy as propaganda and monological, persuasion-oriented communication.

Instead of public diplomacy, Ross suggests that diplomacy can benefit from creating dialogue with nontraditional interlocutors and should focus on ways to "bring people in." An engagement strategy based solely on public diplomacy cannot work in the wake of the "shocking" and "disappointing" consequences of the Iraq War for the U.S. brand. "We can do all the communications we want," he argues, but "actions speak louder than words."[73] Yet it is clear that the mandate of 21st Century Statecraft to connect and build relationships across a variety of foreign stakeholders shares many aspects with what scholars and practitioners understand as the "new" public diplomacy.[74] This conceptual convergence of diplomacy and public diplomacy shares a good deal with the kind of social diplomacy argued for by Slaughter and is exemplified by how Secretary

Clinton describes the mission of U.S. diplomacy after the QDDR:

> [T]he department is broadening the way it conceives of diplomacy as well as the roles and responsibilities of its practitioners. . . . But increasing global interconnectedness now necessitates reaching beyond governments to citizens directly and broadening the U.S. foreign policy portfolio to include issues once confined to the domestic sphere, such as economic and environmental regulation, drugs and disease, organized crime, and world hunger.[75]

On the surface, this depiction suggests a transformative moment in diplomacy *as an institution*, which transcends the question of whether this is about technology. Indeed, Clinton's broader arguments share similar claims with Condoleezza Rice's "Transformational Diplomacy."[76] Yet spokespeople such as Ross nevertheless frame their pronouncements as inevitably tied to the implications of technology. For some skeptics, this rhetoric is too celebratory of technology as a tool *and* policy objective. Evgeny Morozov argues that "Twitter won't make any of those pesky non-digital issues simply go away."[77] Morozov doubts whether the implications of communication technologies are fully understood when they are translated into the field of foreign policy practice.

Another problem with Ross's pronouncements is that they ignore the contributions of public diplomacy to the business of diplomacy through a narrow interpretation of the term. Public diplomacy has a lengthy history of establishing relations between people in ways that are not simply defined by propagandistic overtures. Indeed, both public diplomacy *and* traditional diplomacy have a long tradition of "engagement" among nonstate actors, citizens, and organizations.

The value of Ross's rhetoric and its reflection in documents like the QDDR is in the way it diagnoses the perceived limits of state power and, likewise, the relations that must be leveraged to accomplish foreign policy objectives. Arguments for a 21st Century Statecraft are mostly a context-driven assessment of what states can no longer do with impunity. The technologists' argument for facilitation and convening power creates the warrant for thinking about diplomacy as engagement, an expanded purview of governance as much as representation. The QDDR, for example, is grounded in an idealized vision of engagement that pushes the boundaries of diplomacy to manage complex transnational concerns and coordinate a diversity of nonstate actors.

While commentators like David Rieff find this strategic template to be overly ambitious, the real unresolved issue may simply be that diplomacy is not always about engagement.[78] Diplomacy is also about secrecy and stability. However, transparency and volatility seem to animate the rhetoric of Ross's arguments and, indeed, provide a basis for the call to arms in the language of the QDDR—to valorize the opportunities, risks, and institutional change in diplomatic practice.

CONCLUSION

The idea of a social diplomacy—driven and perhaps even sustained by transparency and volatility—implies a fair dose of speculative thinking. On the one hand, a social diplomacy of facilitation and relation-building is a necessity in a time of decreased state legitimacy in global politics. So a social diplomacy involves more than the ascendance of public diplomacy, but the integration of technological tools, publics, and state institutions in the formation of policy and successful programs or interventions. Technology offers a revised "art of the possible" for diplomats, but it also impels the conditions that necessitate these practices.

Yet there is an undeniable tension in how states respond to the context of transparency and volatility. On the one hand, notions like "collaborative power" and the kind of strategic templates that follow from this perspective (like 21st Century Statecraft) appear well "adapted" to the social and political consequences of today's networked states and publics. Power resides not in singular actors but emerges as a property of collaborative, coordinated activity that coheres around transnational issues and moments of crisis.

But collaborative power does not mean that the older obligations of diplomacy no longer matter. Nor does it suggest that the stewards of foreign policy must abandon the self-interested aspect of their strategic calculus. Indeed, arguments about more "engagement" could serve to adorn the rhetoric of self-interested foreign policy.[79] It is not as if the strategic norms of U.S. diplomacy reflect a wholesale disavowal of the power politics of previous eras. But it does suggest the need for what U.S. Ambassador to Brazil Thomas Shannon calls "reversing the polarity" of diplomacy toward the "listening" ethic that so animates prescriptions of public diplomacy scholars and critics.[80] The insight that publics matter in ways that fundamentally shape the social conditions for success in diplomacy is not a new insight. Shannon draws inspiration from Elihu Root, who argued, in the inaugural issue of *Foreign Affairs* in 1922, about the enduring purpose of diplomacy that has become more apparent. Shannon is worth quoting at length:

> And he [Root] described the purpose of diplomacy as being to rescue from the field of difference and controversy and transfer to the field of common understanding and agreement one subject after another. And that diplomacy in itself is the history—the long history—of the process of adjustment between different ideas and of the prejudices and passions and hitherto irreconcilable differences which had baffled adjustment.[81]

These differences are not simply ensconced in competing governments but are also a reflection and product of social will. Relations among publics were, in this view, the responsibility of diplomacy. Increasingly, this mandate is inextricable from a technologically charged milieu. The newly appointed ambassador to Zimbabwe, Bruce Wharton, offered that diplomats operating in Africa were required to be "social entrepreneurs" in ways that could leverage technology to meet "social needs."[82]

But there also are inevitable consequences to the way in which states recognize stakeholders *as* publics—publics that are in part shaped by the choices state institutions make in reacting to flows of content within social media. In other words, we need to be aware that relations and interactions are conditioned by the platforms used to reach and "see" publics as publics. At best, this ambiguity obviates the need for a more rigorous understanding of media and communication effects. At worst, it could create dangerous expectations around technology to uncritically carry the burdens of diplomatic relation-building.[83]

Any *power* in contemporary statecraft will result from recognizing the social levers and characteristics of the network form.[84] A social diplomacy focused on the construction of latent communities of goodwill and tolerance toward the United States will derive from understanding the communication ethics that underscore how and why people identify through networks that are transnational, local, and interest focused. Transparency is such an ethic. Volatility is an operational hazard. This requires an analysis of the benefits and limits of collaborative power, and the institution capacity—the organizations, the knowledge, the agency—to put these ideas into practice. If we are operating in a revolutionary moment in diplomatic affairs, then it remains to be seen if the anecdotal evidence, the strategic policy arguments, and the available resources can cohere into a truly adaptable diplomatic institution.

ENDNOTES

1. Jesse Lichtenstein, "Digital Diplomacy," *New York Times Magazine*, July 16, 2010. http://www.nytimes.com/2010/07/18/magazine/18web2-0-t.html; Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (New York: PublicAffairs, 2012).

2. Ben O'Loughlin, "How the US Is Slowly Cultivating the Conditions for a Renewed International Order," *Global Policy Journal* (May 31, 2012), http://www.globalpolicyjournal.com/blog/31/05/2012/how-us-slowly-cultivating-conditions-renewed-international-order.

3. Alec Ross, "Digital Diplomacy and US Foreign Policy," *Hague Journal of Diplomacy* 6: 3–4 (2011): 451–455.

4. Thomas Shannon, "Remarks to the Public Diplomacy Council" (The George Washington University, Washington, DC, November 3, 2011). http://publicdiplomacycouncil.org/keynoter-panelist-information-and-transcripts.

5. Kristin M. Lord, *The Perils And Promise of Global Transparency: Why the Information Revolution May Not Lead to Security, Democracy, or Peace*, annotated ed. (New York: State University of New York Press, SUNY Series in Global Peace, 2007).

6. Elizabeth Hanson, *The Information Revolution and World Politics* (Lanham, MD: Rowman & Littlefield, 2008); David Ronfeldt and John Arquilla, "The Promise of Noopolitik," *First Monday* 12: 8 (August 6, 2007). http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/1971/1846%C2%A0%C2%A0.

7. Arlene B. Tickner and Ole Wæver, *International Relations Scholarship Around the World* (New York, NY: Taylor & Francis, 2009).

8. Ulrich Beck, *World at Risk*, 1st ed. (Polity, 2008); Eric Schmidt and Jared Cohen, "Eric Schmidt and Jared Cohen on the Digital Disruption," *Foreign Affairs* (November 4, 2010). http://www.foreignaffairs.com/discussions/news-and-events/eric-schmidt-and-jared-cohen-on-the-digital-disruption.

9. Ole Jacob Sending, Vincent Pouliot, and Iver B Neumann, "The Future of Diplomacy: Changing Practices, Evolving Relationships," *International Journal* 66: 3 (2011): 527–542.

10. Richard Burt, Olin Robison, and Barry Fulton, *Reinventing Diplomacy in the Information Age* (Washington, DC: Center for Strategic and International Studies, 1998); Ronald Deibert, *Parchment, Printing, and Hypermedia : Communication in World Order Transformation* (New York: Columbia University Press, 1997); Wilson P. Dizard, *Digital Diplomacy: U.S. Foreign Policy in the Information Age* (Westport, CT: Greenwood Publishing Group, 2001); Monroe Edwin Price, *Media and Sovereignty: The Global Information Revolution and Its Challenge to State Power* (Cambridge, MA: MIT Press, 2004).

11. Piers Robinson, "The CNN Effect Reconsidered: Mapping a Research Agenda for the Future," *Media, War & Conflict* 4: 1 (April 1, 2011): 3–11; Sean Aday and Steven Livingston, "Taking the State Out of State—Media Relations Theory: How Transnational Advocacy Networks Are Changing the Press—State Dynamic," *Media, War & Conflict* 1: 1 (April 1, 2008): 99–107.

12. Manuel Castells, "Communication, Power, and Counter-Power in the Network Society," *International Journal of Communication* 1 (2007): 238–266; Hanson, *The Information Revolution;* Price, *Media and Sovereignty*.

13. Philip N. Howard and Muzammil M. Hussain, "The Role of Digital Media," *Journal of Democracy* 22: 3 (2011): 35–48.

14. Ali Fisher, "Looking at the Man in the Mirror: Understanding of Power and Influence in Public Diplomacy," in *Trials of Engagement: The Future of US Public Diplomacy*, ed. Scott Lucas and Ali Fisher (Leiden, The Netherlands: Martinus Nijhoff Publishers, 2010), pp. 271–296; Joseph S. Nye, Jr., *The Future of Power*, 1st ed. (PublicAffairs, 2011).

15. Manuel Castells, "The Theory of the Network Society," in *The Network Society: A Cross-Cultural Perspective* (Northampton, MA: Edward Elgar, 2004).

16. Peter Van Ham, *Social Power in International Politics* (New York, NY: Taylor & Francis, 2010).

17. Michele Kelemen, "Twitter Diplomacy: State Department 2.0," *All Tech Considered*, National Public Radio, February 21, 2012. http://www.npr.org/blogs/alltechconsidered/2012/02/21/147207004/twitter-diplomacy-state-department-2-0; Steve Sternberg, "Japan Crisis Showcases Social Media's Muscle," *USA Today*, April 12, 2011. http://www.usatoday.com/tech/news/2011-04-11-japan-social-media_N.htm.

18. Andrew Hoskins and Ben O'Loughlin, *War and Media: The Emergence of Diffused War* (Polity, 2010).

19. Stefan Geens, "Collaborative Power: The Case for Sweden," *Dliberation*, December 13, 2011, http://dliberation.org/2011/12/13/collaborative-power-the-case-for-sweden/; Nye, Jr., *The Future of Power*; Anne-Marie Slaughter, "A New Theory for the Foreign Policy Frontier: Collaborative Power," *Atlantic*, November 30, 2011. http://www.theatlantic.com/international/archive/2011/11/a-new-theory-for-the-foreign-policy-frontier-collaborative-power/249260/.

20. Judith A. McHale, "Opening Remarks at the Council on Foreign Relations: A Review of U.S. Public Diplomacy" (New York, NY, June 21, 2011).

21. Alec Ross, "Digital Diplomacy and 21st Century Statecraft" (The American University, Washington, DC, March 27, 2012); Alec Ross, "Remarks at Digital Diplomacy: A New Era of Advancing Policy" (presented at the Carnegie Endowment for International Peace, Washington, DC, May 17, 2012). http://carnegieendowment.org/2012/05/17/digital-diplomacy-new-era-of-advancing-policy/apnu.

22. Philip N. Howard et al., *Opening Closed Regimes: What Was the Role of Social Media During the Arab Spring?* (Seattle, WA: University of Washington, Working Paper 2011.1, Project on Information Technology and Political Islam, 2011).

23. Evgeny Morozov, "The Future of 'Public Diplomacy 2.0'," *Foreign Policy, Net Effect*, June 9, 2009. http://neteffect.foreignpolicy.com/posts/2009/06/09/the_future_of_public_diplomacy_20.

24. Schmidt and Cohen, "Eric Schmidt and Jared Cohen on the Digital Disruption."

25. Bruce Gregory, "American Public Diplomacy: Enduring Characteristics, Elusive Transformation," *Hague Journal of Diplomacy* 6: 3–4 (2011): 351–372.

26. Hillary Rodham Clinton, "Leading Through Civilian Power: Redefining American Diplomacy and Development," *Foreign Affairs* (December 2010).

27. Craig Hayden, *The Rhetoric of Soft Power: Public Diplomacy in Global Contexts* (Lexington Books, 2011).

28. Geoff Wiseman, "Polylateralism: Diplomacy's Third Dimension," *Public Diplomacy*, (Summer 2010): 24–39.

29. Kenneth Burke, *Language as Symbolic Action: Essays on Life, Literature, and Method* (Berkeley, CA: University of California Press, 1966); Hayden, *The Rhetoric of Soft Power*.

30. R. S. Zaharna, *Battles to Bridges: U.S. Strategic Communication and Public Diplomacy After 9/11* (Palgrave Macmillan, 2009).

31. Castells, "Communication, Power, and Counter-Power."

32. Brian Hocking, "Rethinking the 'New' Public Diplomacy," in *The New Public Diplomacy: Soft Power in International Relations*, ed. Jan Melissen and Paul Sharp (Palgrave Macmillan, 2005); Wiseman, "Polylateralism: Diplomacy's Third Dimension."

33. Manuel Castells, *Communication Power* (Oxford University Press, 2009).

34. R.S. Zaharna, "The Soft Power Differential: Network Communication and Mass Communication in Public Diplomacy," *Hague Journal of Diplomacy* 2: 3 (2007): 213–228.

35. Roger Cohen, "Positive Disruption," *New York Times* (Opinion), June 23, 2011. http://www.nytimes.com/2011/06/24/opinion/24iht-edcohen24.html?_r=2.

36. David Singh Grewal, *Network Power: The Social Dynamics of Globalization* (New Haven, CT: Yale University Press, 2008).

37. O'Loughlin, "How the US Is Slowly Cultivating the Conditions."

38. Julia Ioffe, "The Undiplomat," *Foreign Policy* (May 30, 2012). http://www.foreignpolicy.com/articles/2012/05/30/michael_mcfaul_undiplomat; Lina Khatib, William H. Dutton, and Michael Thelwall, "Public Diplomacy 2.0: An Exploratory Case Study of the US Digital Outreach Team," *SSRN eLibrary* (n.d.). http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1734850.

39. Jamie F. Metzl, "Network Diplomacy," *Georgetown Journal of International Affairs* 2 (2001): 77.

40. Paul Sharp, *Diplomatic Theory of International Relations* (Cambridge University Press, 2009).

41. Ross, "Remarks at Digital Diplomacy."

42. Sarah Wynn-Williams, "Remarks at Digital Diplomacy: A New Era of Advancing Policy" (presented at the Carnegie Endowment for International Peace, Washington, DC, May 17, 2012). http://carnegieendowment.org/2012/05/17/digital-diplomacy-new-era-of-advancing-policy/apnu.

43. Nye, Jr., *The Future of Power*.

44. Geoffrey Pigman, *Contemporary Diplomacy* (Polity, 2011).

45. Sending, Pouliot, and Neumann, "The Future of Diplomacy."

46. Iver B Neumann, "The English School on Diplomacy: Scholarly Promise Unfulfilled," *International Relations* 17: 3 (September 1, 2003): 341–369.

47. Manuel Castells, *The Power of Identity. The Information Age: Economy, Society, and Culture* (Malden, MA: Blackwell, 1997).

48. Morozov, *The Net Delusion*.

49. W. Lance Bennett, "New Media and Power: The Internet and Global Activism," in *Contesting Media Power: Alternative Media in a Networked World*, ed. Nick Couldry and James Curran (Rowman & Littlefield, 2003), pp. 17–38.

50. Andrew Chadwick, "Digital Network Repertoires and Organizational Hybridity," *Political Communication* 24: 3 (2007): 283–301.

51. John Robert Kelley, "The New Diplomacy: Evolution of a Revolution," *Diplomacy & Statecraft* 21: 2 (2010): 286.

52. Wiseman, "Polylateralism: Diplomacy's Third Dimension."

53. Cory Ondrejka, "Collapsing Geography (Second Life, Innovation, and the Future of National Power)," *Innovations: Technology, Governance, Globalization* 2: 3 (2007): 27–54.

54. Stephen Noerper, "Remarks on Korea at the Public Diplomacy in Northeast Asia: A Comparative Perspective Conference" (presented at the The Brookings Institution, Washington, DC, May 30, 2012). http://www.brookings.edu/events/2012/05/30-asia-diplomacy.

55. Fisher, "Looking at the Man in the Mirror;" Ali Fisher, "Standing on the Shoulders of Giants: Building Blocks for a Collaborative Approach to Public Diplomacy" (presented at the International Studies Association, San Diego, CA, 2012).

56. Ali Fisher, "Music for the Jilted Generation: Open-Source Public Diplomacy," *Hague Journal of Diplomacy* 3: 2 (September 2008): 129–152.

57. Nancy Morris, "A Comparative Analysis of the Diffusion and Participatory Models in Development Communication," *Communication Theory* 13: 2 (2003): 225–248.

58. Fisher, "Music for the Jilted Generation."

59. Hocking, "Rethinking the 'New' Public Diplomacy."

60. Daniel R. McCarthy, "Open Networks and the Open Door: American Foreign Policy and the Narration of the Internet1," *Foreign Policy Analysis* 7: 1 (January 2011): 89–111; Shawn M. Powers and William Youmans, "A New Purpose for International Broadcasting: Subsidizing Deliberative Technologies in Non-transitioning States," *Journal of Public Deliberation* 8: 1 (2012): 13.

61. Peter Evans, "Development as Institutional Change: The Pitfalls of Monocropping and the Potentials of Deliberation," *Studies in Comparative International Development (SCID)* 38: 4 (2004): 30–52.

62. Steven Livingston, "The CNN Effect Reconsidered (again): Problematizing ICT and Global Governance in the CNN Effect Research Agenda," *Media, War & Conflict* 4: 1 (April 1, 2011): 20 –36.

63. United States National Security Council, *National Framework for Strategic Communication* (Washington, DC, 2009).

64. Aaron Snipe, "Remarks on Social Media at The Last Three Feet: New Media, New Approaches, and New Challenges for Public Diplomacy" (presented at The George Washington University, Washington, DC, November 3, 2011). http://www.gwu.edu/~ipdgc/events/2011_11_03_last3feet/index.cfm.

65. Rachel Graaf Leslie, "Remarks on Social Media at The Last Three Feet: New Media, New Approaches, and New Challenges for Public Diplomacy" (presented at The George Washington University, Washington, DC, November 3, 2011). http://www.gwu.edu/~ipdgc/events/2011_11_03_last3feet/index.cfm.

66. Ross, "Digital Diplomacy and 21st Century

Statecraft."

67. "21st Century Statecraft" (Washington, DC: U.S. Department of State). http://www.state.gov/statecraft/overview/index.htm.

68. Ross, "Remarks at Digital Diplomacy."

69. Ibid.

70. Jacob Comenetz, "Innovating Public Diplomacy for a New Digital World," *Washington Diplomat*, July 27, 2011. http://www.washdiplomat.com/index.php?Itemid=428&catid=1476&id=7955:innovating-public-diplomacy-for-a-new-digital-world&option=com_content&view=article; Lichtenstein, "Digital Diplomacy."

71. McCarthy, "Open Networks and the Open Door."

72. Ross, "Digital Diplomacy and 21st Century Statecraft."

73. Ibid.

74. Jan Melissen, *Beyond the New Public Diplomacy*, (Clingendael, The Netherlands: Institute of International Relations, Clingendael Paper, October 2011).

75. Clinton, "Leading Through Civilian Power."

76. Kennon Nakamura and Susan Epstein, *Diplomacy for the 21st Century: Transformational Diplomacy* (Washington, DC: Congressional Research Service, August 23, 2007).

77. Evgeny Morozov, "The 20th Century Roots of 21st Century Statecraft," *Foreign Policy* (September 7, 2010). http://neteffect.foreignpolicy.com/posts/2010/09/07/the_20th_century_roots_of_the_21st_century_statecraft.

78. David Rieff, "Battle Hymn of the Diplomats," *National Interest*, April 2012. http://nationalinterest.org/bookreview/battle-hymn-the-diplomats-4912?page=1.

79. Edward Comor and Hamilton Bean, "America's 'Engagement' Delusion: Critiquing a Public Diplomacy Consensus," *International Communication Gazette* 74: 3 (April 1, 2012): 203–220.

80. Nicholas J. Cull, *Public Diplomacy: Lessons from the Past* (Los Angeles, CA: Figueroa Press, 2009).

81. Shannon, "Remarks to the Public Diplomacy Council."

82. Bruce Wharton, "Remarks at The Last Three Feet: New Media, New Approaches, and New Challenges for Public Diplomacy" (presented at The George Washington University, Washington, DC, November 3, 2011). http://www.gwu.edu/~ipdgc/events/2011_11_03_last3feet/index.cfm.

83. Morozov, "The Future of 'Public Diplomacy 2.0'."

84. Castells, *Communication Power*.

From the Age of Secrecy to the Age of Sharing: Social Media, Diplomacy, and Statecraft in the 21st Century

DAVID M. FARIS

INTRODUCTION

Scholars have debated for years whether social media are a democratizing influence on authoritarian states. Only recently, however, have we begun to ask how the global explosion of social media usage is affecting traditional diplomacy. Unfortunately, thus far, we have many more questions than answers. Can social media transform the traditional practice of diplomacy in the same way it has altered the universe of activism and advocacy? And if so, what would this transformation look like?

What is clear is that the new social media environment poses all manner of problems, challenges, and opportunities for the leaders of sovereign states, whether democratic or autocratic. The best way to conceptualize these changes is to think of ourselves as having departed the Age of Secrecy and entered the very beginning of a new epoch—what I call the "Age of Sharing."

In the Age of Sharing, consumers and subjects have become producers, content-collaboraters, and citizens, and they use the applications of social media to share information with one another. Whether they are posting about the latest episode of *Mad Men* or the most recent policy statement from the secretary of State, individuals in the Age of Sharing are manipulating information flows in ways that really are unique.

The volatility inherent in the Age of Sharing was never more apparent than during the tumultuous and deadly events that occurred on September 11, 2012, when protestors scaled the walls of the American embassy in Cairo and when Libyans mounted a separate attack on the U.S. consulate in Benghazi, leaving four dead including the U.S. ambassador to Libya, J. Christopher Stevens. The Cairo demonstrations were ostensibly a response to a U.S.-produced film called "The Innocence of Muslims," which had been crudely dubbed in Arabic and posted to YouTube during the summer. This YouTube version depicted the Prophet Muhammad in deeply unflattering terms. As it became clear that trouble was brewing, Larry Schwartz, senior public affairs officer at the U.S. embassy in Cairo, sent out a Tweet on the embassy's account, USEmbassyCairo,[1] that sparked a controversy that reverberated all the way to the U.S. presidential election. The Tweet read:

> The Embassy of the United States in Cairo condemns the continuing efforts by misguided individuals to hurt the religious feelings of Muslims—as we condemn efforts to offend believers of all religions. Today, the 11th anniversary of

> the September 11, 2001, terrorist attacks on the United States, Americans are honoring our patriots and those who serve our nation as the fitting response to the enemies of democracy. Respect for religious beliefs is a cornerstone of American democracy. We firmly reject the actions by those who abuse the universal right of free speech to hurt the religious beliefs of others.[2]

The Republican nominee for president, Mitt Romney, immediately seized on this statement as evidence that the Obama administration "sympathized with the attackers." While Romney was criticized for toying with the timeline—he suggested that Schwartz's Tweet was an official Obama administration response to the attacks in Libya, which postdated the Tweet by many hours—the Obama administration quickly distanced itself from the embassy's behavior and told reporters that the Tweet had not been approved by Washington. Whatever its role in the election, the embassy's Twitter account, as well as the general dissemination of the inciting video over YouTube, are both representative of features of the Age of Sharing that are here to stay, whether governments like it or not.

Well prior to the tragic events of September 2012, American diplomacy began featuring an instant "talk-back" feature, in the sense that hundreds of thousands of Arabs will routinely get on Twitter and Facebook and engage in spirited debate, criticism, or deconstruction of U.S. policy pronouncements, speeches, or initiatives. At the same time, many American embassies are now engaged with these publics via the very same social media platforms. Thus the Cairo embassy's Tweet was not an aberration but a continuation of long-standing policy in the State Department. This change is even more important, because the region now features several newly democratic or protodemocratic states in Tunisia, Egypt, and Libya with newly permissive information environments. Citizens in both democratic and authoritarian publics are using these technologies not only to expose the actions of states but also to organize opposition to them. At the same time, individuals use social media to circulate dubious theories, such as the idea that the U.S. government is in bed with the Egyptian Islamist movement, or to disseminate hateful videos like "The Innocence of Muslims." Finally, diplomats are using social media to communicate with one another, which has created a new channel of state-to-state communication that promises to alter interstate relations in ways we have only begun to imagine. In many ways the dilemma faced by U.S. diplomats after the Arab Spring resembles that of state media organizations under authoritarianism. Both must find ways to make deeply unpopular policies palatable to local publics. Because Israel will remain a valuable American ally in the region for the foreseeable future, the United States will be forced to continue engaging in unpopular acts of public support for the Israelis and to defend policies in places like Bahrain and Saudi Arabia that very clearly contradict American values. In addition, the diffusion of social media technologies at a rapid pace throughout the region gives Arab citizens the capability of organizing difficult-to-predict challenges to these policies. For the leaderships of these newly democratic states, they will also find it more difficult to cooperate with American grand strategy, even if leaders are elected who are willing to do so. In other words, American policy is now made in an environment of radically increased transparency, visibility, and contention, which will lead inevitably to struggles over message discipline, engagement, and policymaking in a more volatile world.

This essay will explore the complicated interplay of citizen journalism, involuntary transparency, and policymaking in the digital age and the ways that those relationships unfolded during the Arab Spring of 2010–2011 and beyond. By doing so, it will highlight new challenges to American diplomacy as well as identify ways that the new information environment can be best managed to harmonize American interests and policies. The essay will also outline some commonsense alterations to American public diplomacy and the way that Americans with all kinds of affiliations with the government can work together to advance the general cause of peace and understanding between citizens of different states.

THE AGE OF SECRECY VERSUS THE AGE OF SHARING

Modern diplomacy has been described by Mark Page and J. E. Spence as the process of crafting "open covenants, secretly arrived at."[3] Traditionally, secrecy has served a variety of purposes in relations between states in the international system. Secrecy prevents sensitive negotiations from being blown apart by the revelation of unpopular concessions and allows frank discussion between diplomats whose domestic constituents may disapprove of portions of the agreement. The resulting agreements are of course (usually) made public, but the norm has been for details of the negotiations to remain secret until participants are prepared to defend their choices. The advent of social media has jeopardized the element of secrecy in diplomacy, perhaps irreversibly. Wikileaks is the most explosive and well known of the methods of involuntary disclosure but hardly the only one. Diplomats can no longer be certain that their cables are secure, and even if they assume the temporary security of those cables, they cannot be certain that at some point in the future their thoughts will not be revealed to audiences for which they were never intended. This already happens, of course, when archives are opened, but typically the participants in such releases are dead or sufficiently removed from the public eye as to make the revelations unremarkable. The inevitable result of this paradigm shift is likely to be greater difficulty for the United States in engaging with regimes that are publicly unpopular or whose domestic policies clash with U.S. values. No one wants to get caught making unsavory deals with unpopular foreign leaders. The net effect of this change is probably greater complication and difficulty in U.S. dealings with autocratic and semiauthoritarian states.

In other words, policies that were possible in the Age of Secrecy—the era that ended with the explosion of social media—are more difficult to execute during the Age of Sharing—the new epoch in which ordinary citizens spend hours each day reading, annotating, and creating criticism of government policies and then sharing their thoughts with online social networks ranging from a few hundred to the hundreds of thousands. These "Twitterati," as they are sometimes dismissively referred to, have become among the most important opinion leaders in the region, not because they have their own perches on Al-Jazeera's expensive talk shows but rather because they are funny, biting, and absolutely relentless in their exposure of state hypocrisy and also of the tensions inherent in American regional policymaking. Nothing better encapsulates this trend better than the pictures that circulated constantly, during the Egyptian revolution, of protestors holding tear gas canisters with the phrase "Made in America" printed on them. The United States has been selling weapons and riot control gear to regional authorities since long before even Al-Jazeera became a regional opinion leader—the prominence of American-made weapons has been a constant staple of discourse about Israeli incursions into Lebanon, for instance. But the Age of Sharing has made it more or less impossible to avoid knowing who manufactured the tear gas for Egyptian riot police, and these images did incalculable damage to America's standing in Egypt—even after the Obama administration did a dramatic *volte face* and abandoned Hosni Mubarak at the height of the uprisings.

Secrecy in all its myriad forms was part of the long-term survival strategy of all Middle East dictatorships. The standard information model from the 1950s to the 1990s (which was shattered first by Al-Jazeera) was total state control over all arms of mass media empires, from state television and radio stations to government-run or affiliated newspapers.[4] Secrecy served three purposes. Domestically, secrecy and information control could isolate instances of public discontent and keep them hidden from the broader public. Second, secrecy concealed from Arab publics the exact content and performance of authoritarian policies as well as allowed authoritarian elites to construct vast archipelagos of secret corruption. How else could one explain the bizarre Qaddafi family dwellings found in Libya by astonished citizens and reporters? Would the Qaddafi regime have ever constructed such monstrous monuments to greed and obliviousness if they thought they would be found out? Of course not. But the truth is that authoritarian attitudes have not quite caught up to the paradigm shift wrought by social media, and many tyrants and their hangers-on still apparently believe they can get away with flaunting their opulence while their citizens suffer. This is precisely the miscalculation that the Ben Alis (of Tunisia) made when, for instance, the family and its "entourage" managed to stash away $5 billion in assets. It is much more difficult to keep the existence of a "private jet" secret when citizens can snap pictures of you boarding or deplaning the jet and send them to tens of thousands of people in an instant. It might even make you think about whether you would not be better off flying coach on Tunis Air like everyone else and avoiding the scrutiny.

And finally, throughout this period, secrecy allowed Arab leaders to engage in diplomatic maneuverings that were at odds with expressed public desires. Now, it is important not to oversell this. Egyptians knew that the Mubarak regime was cooperating with the U.S.-led response to Saddam Hussein's 1990 invasion of Kuwait, and they made their displeasure known with massive street protests. Anwar El-Sadat of Egypt was unable to preempt riots in 1977 by telling people that the price of bread was lower than it was. Sadat was certainly not able to keep the Camp David Accords a secret—he was not even able to hang onto his life. But it is certainly true that not every foreign policy decision of the 1990-vintage Mubarak regime was subject to public and instant scrutiny in quite the same way as are those of today's leaders. Today, nearly everything is public. This does not mean that authoritarian regimes are doomed or that they have not devised clever strategies for dealing with social media, but rather that the old days of closed, centralized information control are over.

A telling anecdote involves an Egyptian activist, who remarked to me that during the 1990s, if he was at a demonstration and saw someone with a camera, he assumed it was someone from state media trying to get pictures of faces for surveillance and harassment. Today, someone with a camera phone is almost certainly a citizen or journalist looking to document state abuse (although the balance may be changing again with the advent of facial recognition software that can be exploited by states to identify dissidents).[5] Social media have completely upended or, at the very least, deeply complicated, the dynamic between surveillance regimes and ordinary citizens, by creating in the Middle East a culture of *sousveillance*—the watching of the watchers by the watched. It was sousveillance culture that first brought the issue of torture into the Egyptian public sphere by passing around videos of police abuse, posting them to blogs and YouTube, and generating public outcry against the arbitrary deployment of state power against ordinary citizens. In the Age of Secrecy, authoritarian regimes could do more or less whatever they liked to their own citizens, because the media belonged to the authoritarian elites. But in the Age of Sharing, state media operations are becoming increasingly irrelevant, eclipsed by a participatory Internet and mobile sharing culture that, if it engages with state media at all, does so to mock, undermine, and deconstruct. Opposition media outlets are increasingly merged with elite digital networks of activists, who transition seamlessly between one realm and another, providing an entirely alternate universe of information and thinking, available to enterprising citizens even when the state tries hard to close off all avenues of access, as in Tunisia prior to December 2010.

THE RISE OF THREE-LEVEL GAMES

This dynamic works on the United States as much as it does for local elites. In the 1980s, Ronald Reagan could deliver a speech on regional policy and have it received by no one except its intended audience—dictators and foreign policy elites in the Middle East. The conduct of foreign policy has been famously characterized by the political scientist Robert Putnam as "two-level games"—in other words, negotiations between states, and then again between states and their domestic audiences.[6] Putnam argues that successful diplomacy required not just an agreement between diplomats or states but also the management of public expectations and interests at home. This domestic audience could in some cases scuttle international agreements through opposition to key concessions. One need look no further than the attempt to reach agreement on climate change issues to see how domestic audiences and interest groups can prevent agreements from coming to fruition. With the advent of social media, even policymakers in some authoritarian regimes must now count a third audience in addition to voters and negotiating partners. That audience is the networked elite, who often serve as an intervening variable between policies and mass audiences. In the past, the "interveners" were the foot soldiers of state media outlets, and regimes hardly had to worry about whether they would fall in line or at least keep their criticism to the acceptable minimums. It was the state versus society and, given the arrangement of forces, it was the state that usually won, with quite rare exceptions. Today, however, the blending of social media with traditional journalism (Al-Jazeera harvesting citizen accounts of news events, for instance), means that the distinction between citizens and journalists has become blurry at best. Even large, bureaucratic media organizations are leveraging the capabilities of ordinary citizens, who are often practicing a kind of incidental journalism that has become ubiquitous in an age in which millions of citizens are carrying supercomputers around in their pockets. It is this third-level audience that has proven most difficult for authoritarian regimes to master without resort to draconian filtering and censorship policies.

Bruce Gregory has argued that "public diplomacy is now so central to diplomacy that it is no longer helpful to treat it as a sub-set of diplomatic practice."[7] The blurring of the lines between public diplomacy and traditional diplomacy is what Secretary of State Hillary Rodham Clinton has dubbed "21st Century Statecraft."[8] The essence of the Clinton vision is an increase in horizontal ties, enabled by social media, which increase person-to-person (read: civilian to civilian) and person-to-nongovernmental organization (NGO) contacts. The hope was that these contacts could bypass the lumbering "white guys with white shirts and red ties" (in the now-famous words of Jared Cohen)[9] diplomatic model, not so that citizens could make policy with other citizens but so that the efficacy of American policy would be reliant much less on diplomats and more on relationships between Americans and citizens of other countries, relationships that are not necessarily mediated by bureaucrats. The truth, of course, is that diplomats will continue to play a key role in policymaking and mediation, but they will be forced to do so, especially in the Middle East, with new-found appreciation for public opinion as channeled through the focal points of social media.

Diplomats must also be careful not to impute too much importance to what they see being discussed on social media channels—in poorer countries like Egypt, the networked elite may not be representative of the population as a whole.

Unfortunately, much of the thinking on the Internet remains years behind developments in the social media universe. This thinking is grounded in developments in what was called "the blogosphere," despite the fact that the blogosphere is shrinking in terms of relative influence to other spheres and "verses" like the "Tumblrverse" and Facebook. Citizens are increasingly forgoing creating their own stand-alone web pages, and then trying to attract eyeballs to them, in favor of using the built-in sharing and networking capabilities of social media sites. The essence of these technologies is not the one blogger versus the universe model of the acerbic Egyptian blogger The Sandmonkey; it is sharing. No site was more influential in shaping the Egyptian uprising than Facebook. If Wael Ghonim had gone to Wordpress and started a blog rather than collaborating on a Facebook page, he may never have found the influence he achieved with We Are All Khaled Said. That page built not on Ghonim's fame (he was more or less completely unknown in May 2010) but rather on the ideas and iconography of his Facebook page, which grew through sharing—the sharing of the "like" function, which built its membership into the hundreds of thousands by the time the revolution started, and the sharing of ideas and information on the group's wall.

Now, information that is shared by more prominent members of these communities obviously has an advantage over information shared by nonelites. To influence these influencers does not require duplication of their efforts with government Twitterers or Tumblrs. Given the restrictions still in place on employees of the U.S. government using social media in an uninhibited way, even a highly networked individual like then Senior Advisor for Innovation to former secretary of State Hillary Rodham Clinton Alec Ross is going to have limited effect, since everyone knows who Ross worked for and what his limitations are likely to be, given his affiliation. Influencing the influencers means building horizontal networks of trust and reciprocity between lower-level members of the hierarchy, easing restrictions on the production of content by government employees and diplomatic personnel, and understanding that lifting barriers will lead to the occasional embarrassment when someone says something that was unfiltered and unwelcome. It means understanding that a third level has been added to the diplomatic game.

SECRET CORRUPTION, OPENLY EXPOSED

That third level was something that the Ben Ali clan clearly did not understand. Tunisian activists will argue that the role of Wikileaks in inspiring the revolution is vastly overblown. This is probably true. The general perfidy and extravagance of the Ben Ali clique was not exactly a secret in Tunisia prior to the revolt. But this is not to say that the various revelations contained in Wikileaks did not have an effect or did not contribute to confirmation of open suspicions about the activities of the ruling elite.[10] The Ben Ali family was hardly the first dictatorial clan to abuse their privileges, but they were probably the first whose corruption was so spectacularly revealed by leaked diplomatic cables. If you were on the fence about whether the government was corrupt—in other words if you were engaging in the understandable game of wishful thinking where you give your own government the benefit of the doubt—the Wikileaks revelations probably overcame even the worst case of cognitive dissonance. Therefore one should conceptualize the leaked diplomatic cables as only one digital variable among many—notably the community blog *Nawaat*, run from France by Sami Ben Gharbeia—that contributed to an overall souring of the public mood with respect to the Ben Alis.

These scandals were in many ways reminiscent of corruption scandals that had plagued authoritarian regimes throughout the Age of Secrecy. Again, we need to distinguish firmly between arguing that social media are necessary to expose corruption or whether they merely make it much more likely that corruption will be exposed. Egypt's King Farouk became an international laughingstock in the 1940s, long before a single Egyptian so much as owned a TV. Make enough appearances at casinos and brothels, even in the Age of Secrecy, and your perfidy is likely to make its way into the news. But in the Age of Sharing, "the networked" can withdraw their "consent" (as Rebecca MacKinnon would put it[11]) in a flash. Thus we witnessed the spectacle of French diplomacy during the Tunisian uprising, when Foreign Minister Michȇle Alliot-Marie effectively offered French assistance in putting down the Tunisian revolt. In the Age of Secrecy, her declaration may have been buried in the pages of *Le Monde*, but in the Age of Sharing, scarcely five minutes had passed before both French and Tunisian activists took to their designated social media outlets to denounce the government's perfidy. Whether Alliot-Marie's words actually represented French policy or not was immaterial; the damage was done, and it was done much faster than anyone could have anticipated.

Alliot-Marie's ordeal (she was forced to resign) was representative of a broader shift wrought by the social media age. It is not simply about this one official and her off-the-cuff remarks but rather about a wholesale cultural shift, from authoritarian citizens as passive, recipient subjects, to empowered, networked critics. In the Age of Secrecy, it is entirely plausible that the French foreign policy elite could have quietly engineered a rescue for the embattled Ben Alis, or at least provided some material assistance to give them a fighting chance. But in the Age of Sharing, when any foreign policy shift is going to be blasted through the Twitterverse the moment it is announced (and when lies or hypocrisy are likely to be exposed quickly), the kind of up-is-downism required to execute a policy of support for the Ben Alis while still espousing support for universal freedom and dignity is simply not possible. Or if it is possible, it would have come at a domestic and international price that the Sarkozy government was not willing to pay. The Obama administration learned this lesson the hard way barely a month later and just forty-eight hours after the start of the Egyptian uprising, when Vice President Joe Biden announced that Mubarak was "not a dictator" and should not step down. Certainly, the channels of social media are often clogged with rumor, innuendo, or false information. And some governments, particularly Russia, have become adept at flooding those channels with proregime propaganda. But on certain high-profile issues, it has become much more difficult for authoritarian regimes to propagate—and indefinitely maintain the credibility of—preposterous lies. For a lie to lose its utility and its relevance, it is not necessary for everyone in a country to stop believing it. If even small numbers of people have access to the truth, then the calculus of authoritarian information hegemony is forever altered.

THE PERSONAL ACQUAINTANCE IS POLITICAL

The speed and low cost of passing information through those Facebook feeds is part of why social media have become the default organizing platforms for dissent in many authoritarian countries. Clay Shirky was among the first to foresee how social media would be used to organize dissent in authoritarian environments.[12] Shirky argued that dissidents in nondemocratic countries would gravitate toward the simple group-forming and information-sharing facets of emerging social media and collaborate on common goals for a fraction of the prior cost of collective action. Sharing is central to his vision of influence through Facebook and Twitter, as individuals reveal their ideas and preferences to others in their social networks. The revelation of this "private information," as it was termed by Timur Kuran,[13] prompts changes in individual calculations about revolt and the durability of authoritarian control—leading to what is known as an "informational cascade."[14] Shirky's vision came to its most mature realization with the Arab Spring, as networked publics used two distinct methods for leveraging the capabilities of social media in the face of sustained authoritarian interference. We Are All Khaled Said built a Facebook army that collaborated on choosing the date of the uprising as January 25, a brilliant stroke of tactical jujitsu, seeing as how January 25 had become an Orwellian holiday meant to celebrate Egyptian police forces, who had grown to be loathed in part due to the effort of lone wolf bloggers during the mid-2000s.[15] These bloggers, among them Noha Atef, Wael Abbas, and Hossam El-Hamalawy, used the old model of building a web page, loading it with content, and then hoping the eyeballs would follow. But they have mostly stopped "blogging," whatever that actually means in an era in which content from many different sites and sources is often aggregated in some form on the same platform.

Blogs are limited in their capacity to build community. Even the most leveraged community blogs, like Daily Kos, still require people to join, provide login info to participate, and then proceed over to Daily Kos. The site also presupposes, generally, an interest in left-wing politics. Chances are, if you are more or less ambivalent about politics, you probably have never directed your browser to Daily Kos, or the right's Real Clear Politics, or any of the other political web sites that have exerted their influence on American politics over the past twelve or so years. On Facebook, part of the site's accidental genius is the way it embeds ordinary and possibly nonpolitical individuals in a web of social connections full of people who really do care about politics. These "influencers," can help turn even nonpolitical individuals into sharers of political information. They can also lead nonpolitical people to block or hide the content of political "over-sharers," but it takes an act of volition to block a friend's Facebook feed, and it is more rare than you think for someone to take this step.

These dynamics become particularly important during moments of crisis. Again and again during the Egyptian uprising, the Mubarak regime used state television to broadcast the president's stale and increasingly delusional speeches to the public—each offering a series of concessions whose acceptability had already been eclipsed by events that Mubarak and his staff either were not watching or did not understand. Before he had even finished speaking, he was rejected by two technologies—one older than television and one newer. Listening on Al-Jazeera, particularly during the president's last attempt to salvage his own rule, you could literally hear the howl of rejection tearing through the throngs in Tahrir. This was a message that the regime would, belatedly, receive. Simultaneously, the Twitterati, many of them standing in the middle of the square while they were updating their feeds and profiles and Tumblrs, were broadcasting their rejection to anyone who was paying attention or listening. Their message, broadcast over the many channels of the new social media empire, reached even friends and acquaintances who were not deeply invested in the departure of Mubarak. That kind of cumulative messaging can have an effect, both in terms of boosting initial turnout and of spreading word about ongoing events.

They played perhaps an even more important role when the regime deployed its time-worn strategy of declaring that is up is down during the uprising. On the infamous "Day of the Camel," when mounted hooligans in the service of the regime stormed Tahrir Square and murdered dozens of innocent protestors, the government tried to declare that "foreign hands" were behind the mayhem. Perhaps in another media age this strategy could have been minimally plausible or effective. When Gamal Abdel Nasser declared, shortly after the Six-Day War began, that Egyptian forces were nearing victory, citizens had no reason, or any capability, really, to disbelieve him. Today, the same event would have been witnessed by thousands of citizens, who would have Tweeted under the hashtag #airforcedestroyed. Or perhaps a rogue air force pilot would have posted something on Facebook about what had actually happened. In either case, the deception would have been sniffed out almost immediately, as it was during the uprising of 2011. Declaring the insurrection to be influenced by the United States or Israel was not simply contrary to the common sense of the Egyptian people, who after all were responsible for organizing and executing the protests, but was also belied by every available source of social media, which was full of actual Egyptians Tweeting, Facebooking, blogging, and texting about the events. None of these people was obviously a spy or a foreign agent. Many digital activists in Egypt have told me that part of the reason they have risked life and limb to share their information is so that the government cannot lie any longer. They understood, long before many elites in the West realized this, that government propaganda is endangered by an open Internet. This view has its skeptics, of course, the most prominent being Evgeny Morozov, who has detailed the ways that savvy regimes like Russia and China have manipulated the Internet and flooded it with proregime propaganda.[16] Given the distant kinship of government propaganda and "public diplomacy," this should make us consider the effects of these changes on U.S. policymaking in the Middle East.

ENGAGING HORIZONTAL NETWORKS

How indeed should the United States proceed in the Age of Sharing? First, it is essential to maximize the utility of the massive investments that the government has already made in informal regional assets—the scholars, aid workers, and journalists who have been the recipients of government largesse to go and learn about the Middle East. These people do not have to be employees of the U.S. government, or even contractors. One thing the U.S. government can do much better is to maintain relationships with stakeholders who have benefitted from American support for their research, studies, and work. The U.S. Department of Education has spent untold millions training U.S. students and scholars in acquiring exotic languages, and it desperately needs a better network to keep track of these investments and to better incorporate them into public diplomacy. Fulbright scholars, Foreign Language Area Studies (FLAS) recipients, and ordinary researchers are often in the same country at the same time and have few opportunities to interact with one another. This is typically because the network of U.S. informal ambassadors is conceived too narrowly. Anyone who is in, for instance, Egypt doing work, research, or studies that are financed in any way, shape, or form by the U.S. government should have the opportunity to meet with one another more regularly. This goes doubly for diplomats, who are often perceived as a separate entity by other individuals doing work in these countries.

One of the many reasons this is important is because it is rarely the senior diplomatic staff that will have meaningful contacts with ordinary Egyptians. It is the anthropologists doing field work in poor or rural areas, or the political scientists running around conducting open-ended interviews with members of the elite, or the sociologists studying systems of social support in informal areas. Getting these groups talking to one another through social media should be a major goal of "21st Century Statecraft." But getting the Americans to talk to one another is one thing—how might the United States build influence with the young, networked Arabs who have gained so much influence over the past decade? These are the individuals who are most political and thus most likely to object to one or many aspects of U.S. policymaking in the region. Connecting Americans who are fluent in Arabic, familiar with the important issues of Egyptian politics, and who have recently spent time in the country not only creates an invaluable resource for U.S. policymakers but also familiarizes Egyptians with the best and brightest Americans—those most likely to make an impression that contradicts stereotypes about Americans and who can challenge deeply held beliefs about the country.

Concomitant to this network-building, it would be helpful if employees of the U.S. government could be even freer in their use of social media. This does not mean disguising State Department employees or Central Intelligence Agency (CIA) agents as Berkeley anthropologists or study abroad students, but rather harnessing the truth-sniffing aspects of social media as much as possible in the service of breaking down linguistic, cultural, and economic barriers. Restrictions on the speech, and particularly the social media usage of U.S. government employees abroad, are classic Age of Secrecy anachronisms. They reflect a mentality of accumulating stamps of authority before a piece of writing, thinking, or advocacy can be seen by anyone. Or as Michele Kelemen has written, the State Department seems to be "promoting social media while also trying to control the message and keep tabs on personal blogs of foreign service officers."[17] In the Age of Sharing, deliberately clamping down on the freedom of young diplomats to participate in unfolding events and discussions is tantamount to destroying their credibility and efficacy or, worse, putting anyone who works for the government under suspicion of working for the CIA. To put it another way, to prevent Americans from acting like normal human beings only contributes to their alienation from the very cultures they are ostensibly observing. Their "secret" cables are thus unlikely to be full of much wisdom anyway. Remember the accidental genius of Facebook—incidentally exposing ordinary citizens to the basic decency of State Department employees might help undo some of the damage of America's ongoing refusal to reevaluate its relationship with Israel. This also does not mean using Twitter in "broadcast mode," as James Carafano would put it—sending messages out to tens of thousands of recipients but not engaging in any real conversation.[18] Barack Obama is the most followed "diplomat" in the world, but his Twitter account is not the source of real engagement or conversation. Better to have diplomats using embassy Twitter accounts to engage in back-and-forth with followers in their own languages, rather than using the platform as a high-tech soapbox. This is happening in some countries but not all.

At first glance, the Cairo embassy incident might seem like evidence that the State Department should rein in rather than unleash their diplomats on social media platforms. Certainly, having diplomats free to engage with local publics in native languages opens up the possibility of further political embarrassment. This is especially true for the Obama administration, as the State Department itself has long been a bête noire of critics who believe that it is staffed by anti-American diplomats who have spent too much time falling in love with their areas of expertise.[19] But the Cairo embassy also used Twitter in the days following the attacks to push back against the idea that the U.S. government funded or approved of "The Innocence of Muslims" and pointed out discrepancies between the Muslim

Brotherhood's English and Arabic Twitter accounts, among many other positive things. In fact, the embassy's engagement with the Egyptian public in the wake of the attack was arguably much more important than any Tweet sent at the height of panic about a possible breach of the compound. As long as U.S. diplomats will be forced to work behind blast walls and massive security architectures due to ongoing threats, it is in fact those social media networks that might provide the best path of communication between diplomats and local audiences. This is what it means to be part of a global public sphere. And the truth is that you are either in or out. In the Age of Twitter, you simply cannot wait for permission from Washington to respond to a Tweet. By the time that permission comes through, the original Tweet will be long lost in the never-ending data stream.

CONCLUSION

There is a tendency, after some disruptive technological or epochal shift, for people to want to put the old world back into existence again. For diplomacy, the old world was not just a time, but a manner of being, the whole range of relationships that constituted the Age of Secrecy. Those media monopolies and information chokeholds are as bygone as the corner bookstore, and no amount of wishing and hoping will bring them back. If you could simmer the essence of the Age of Secrecy down to an emulsion, it would be this: States had an overwhelming information advantage over their own citizens, and they used it. This information advantage typically allowed authoritarian regimes to remain several steps ahead of their opponents and allowed democratic states to engage in unpopular deal-making with tyrants. These deals still required managing and public diplomacy, but states possessed an inherent advantage. It should be clear that the Age of Sharing has deeply cut into that information advantage. States are still able to keep information out of the public domain, but the cost has gone up—both the costs of storage and protection, and the costs of failure.

Scholars are only beginning to tackle the questions raised by the intersection of social media and diplomacy. For instance, what are the actual effects of U.S. diplomats using social media? Are their Tweets influential—i.e., are they passed through networks of influencers? Are they simply retweeted? The much-maligned account for the U.S. embassy in Cairo (@USEmbassyCairo) has nearly eighteen thousand followers but appears to have little traction in terms of how often their messages are "retweeted" (i.e., copied and sent out by other users for the purposes of sharing and discussion).[20] Or are they part of complex and important debates about U.S. power, democracy, and the future of governance in the Middle East? These are empirical questions that can only be answered by further, in-depth research. Whatever the results of these inquiries, U.S. diplomats and policymakers will be grappling with the shift from the Age of Secrecy to the Age of Sharing for the foreseeable future.

For U.S. diplomacy, this shift means that debates about U.S. foreign policy in the Middle East will take place publicly, will involve the views of ordinary citizens as mediated through the new networked elite, and will result in the instantaneous exposure of any real or perceived hypocrises in policymaking and rhetoric. It will also result in surprise controversies and the propagation of conspiracy theories or misinformation. Clearly, part of the role of social media in the Age of Sharing is to maintain the credibility of information and to combat misinformation about the United States. The more that diplomats and assets are genuinely embedded in social media networks throughout the Middle East, the better. The Age of Sharing means a permanent complication of efforts to maintain ties with unpopular or morally suspect allies like Bahrain and Saudi Arabia and at the least will mean that a higher price for those alliances will be exacted by networked publics. It means immediate firestorms will be created when representatives of the state like Joe Biden or Michèle Alliot-Marie go off-message and undermine attempts to build alliances and improve the public image of great powers in the region. If something is Made in America—whether it is a policy or a tear gas canister—that information is likely to become public knowledge faster than the diplomatic apparatus is going to be able to respond. This is the real meaning of volatility in the digital age—an increased difficulty in managing messages and the necessity of engaging unpredictable new actors. It also means that dedicated friends of the United States can make inroads into public opinion merely by engaging with the sharers on their own terms and their own platforms. The United States can respond in two ways: either it can try to wish the old world back into existence, or it can try to seize the very real opportunities for networking, engagement, and alliance-building that are built-in features of the new environment.

Whatever choice is made, the only certainty is that it will be shared.

ENDNOTES

1. Josh Rogin, "Inside the Public Relations Disaster at the Cairo Embassy," The Cable, *Foreign Policy* (September 12, 2012). http://thecable.foreignpolicy.com/posts/2012/09/12/inside_the_public_relations_disaster_at_the_cairo_embassy.

2. Glenn Kessler, "The Romney Campaign's Repeated Errors on the Cairo Embassy's Statement," *Washington Post,* September 13, 2012. http://www.washingtonpost.com/blogs/fact-checker/post/the-romney-campaigns-repeated-errors-on-the-cairo-embassy-statement/2012/09/13/978a6be6-fdf0-11e1-b153-218509a954e1_blog.html.

3. Mark Page and J. E. Spence, "Open Secrets, Questionably Arrived At: The Impact of Wikileaks on Diplomacy," *Defence Studies* 11:2 (June 2011): 236.

4. William Rugh, *Arab Mass Media: Newspapers, Radio and Television in Arab Politics,* (New York, NY: Praeger, 2004).

5. Iason Athanasiadis, "Iran Uses Internet As Tool Against Protestors," *Christian Science Monitor,* January 4, 2010. http://www.csmonitor.com/World/2010/0104/Iran-uses-Internet-as-tool-against-protesters.

6. Robert Putnam, "Diplomacy and Domestic Politics: The Logic of Two-Level Games," *International Organization* 42:3 (Summer 1988): 427-460.

7. Bruce Gregory, "American Public Diplomacy: Enduring Characteristics, Elusive Transformation," *Hague Journal of Diplomacy* 6 (2011): 351-372.

8. Hillary Rodham Clinton, "Remarks on Innovation and American Leadership to the Commonwealth Club" (San Francisco, CA, October 15, 2010). http://www.state.gov/secretary/rm/2010/10/149542.htm.

9. Jesse Lichtenstein, "Digital Diplomacy." *New York Times Magazine,* July 16, 2010. http://www.nytimes.com/2010/07/18/magazine/18web2-0-t.html/?pagewanted=all.

10. Tom Malinowski, "Whispering at Autocrats: In one fell swoop, the candor of the cables released by WikiLeaks did more for Arab democracy than decades of backstage U.S. diplomacy," *Foreign Policy,* January 25, 2011. http://www.foreignpolicy.com/articles/2011/01/25/whispering_at_autocrats?hidecomments=yes**.**

11. Rebecca MacKinnon, *Consent of the Networked: The Worldwide Struggle for Internet Freedom* (New York, NY: Basic Books, 2012).

12. Clay Shirky, *Here Comes Everybody: The Power of Organizing Without Organizations* (New York, NY: Penguin Press, 2008).

13. Timur Kuran, "Now Out of Never: The Element of Surprise in the East European Revolution of 1989," *World Politics* 44: 1 (October 1991): 7-48.

14. Sushil Bikhchandani, David Hirshleifer, and Ivo Welch, "A Theory of Fads, Fashion, Custom, and Cultural Change as Informational Cascades," *Journal of Political Economy*, 100: 5 (October 1992): 992-1026.

15. David Faris, *Dissent and Revolution in a Digital Age: Social Media, Blogging and Activism in Egypt* (London: I.B. Tauris and Co., 2012).

16. Evgeny Morozov, *The Net Delusion: The Dark*

Side of Internet Freedom (PublicAffairs, 2011).

17. Michele Kelemen, "Twitter Diplomacy: State Department 2.0," *All Things Considered,* National Public Radio, February 21, 2012.

18. James Carafano, *Wiki at War: Conflict in a Socially Networked World* (2012).

19. See for instance Robert D. Kaplan's *The Arabists: The Romance of an American Elite* (New York, NY: The Free Press, 1995).

20. www.retweetrank.com. Data as of September 4, 2012. The Cairo embassy's retweet rank is 109,184. For some perspective, the Egyptian volunteer news organization Rasad News Network (RNN) is ranked 684.

Development in the Information Age

The Chinese ICT Development Strategy in Africa: Transparency, Sovereignty, and Soft Power

Séverine Arsène

THE RISE OF ICT IN DEVELOPMENT POLICIES AND THE ADVENT OF NEW PLAYERS

Increasingly, transparency is identified as one of the key challenges in the field of development aid. Transparency was mentioned as a condition to improve accountability and aid effectiveness in the 2005 *Paris Declaration on Aid Effectiveness*, completed in 2008 by the *Accra Agenda for Action*.[1] In 2011, the *Busan Partnership for Effective Development Cooperation*[2] reaffirmed this principle.

Information and communication technologies (ICTs) are considered as an important tool to achieve this goal. An entire field of research and practice has emerged under the title "ICT for development" (ICT4D).[3] It underlines the potential of ICTs for development in general (it could provide more economic opportunities, especially in remote places) and for transparency in particular.[4]

This promise of ICTs for transparency is twofold. On the one side, it could empower civil society, increase participation, or help fight corruption,[5] all of which considerably improve local governance and have a positive impact on development. From that perspective, reducing the "digital divide" between countries and within countries has become one of the top priorities of development agencies around the world.

On the other side, ICTs could be used to improve the management of development projects themselves. By sharing and publicizing information on their development aid initiatives, donors improve aid coordination, control, and efficiency. Major donors, such as the World Bank,[6, 7] the U.S. Agency for International Development (USAID),[8] and other international actors like the Organization for Economic Cooperation and Development (OECD),[9] are, therefore, rethinking and prioritizing the role that ICTs can play in achieving favorable development outcomes and good governance. As an example, the OECD Development Centre has developed two wikis aimed at sharing data on development and on women—Wikiprogress[10] and Wikigender.[11]

In this context, new players are gaining an increasingly important role in building the ICT infrastructure of developing countries. This is particularly true in Africa, where most ICT infrastructure—from telecommunications backbones to customer services—is just starting to be developed, at a very rapid pace. Chinese companies are particularly under scrutiny as they gain new markets in Africa and win public bids to implement telecommunications technologies.

Several studies focus on the impact of this increasing Chinese presence within the international aid architecture. For example, they assess whether Chinese practices could undermine previous efforts by the international donor community to establish norms in terms of international debt, supported export credits, social and environmental standards, or governance and transparency, among others,[12] or, on the contrary, whether such practices would give African countries an alternative to the neocolonialism that is embedded in some traditional donors' practices.[13]

It is not my intention to discuss the impact of China on development norms in general. Instead, I would like to outline a number of issues that are specific to ICTs and transparency.

Indeed, these technologies have important stakes in terms of fundamental rights, from freedom of expression to privacy to the rule of law.[14] The very rapid development of telecommunications infrastructures in countries where they were not available so far—and the subsequent adoption of legislation to control them—is a crucial moment in these countries, affecting not just the social, political, and economic development but also their state security and sovereignty. It has an impact on global Internet governance as well. In this paper, I intend to explore the logical tension between these sensitive stakes and the transparency promises that are both embedded in ICTs.

The arrival of new actors like China, which plays a central role in this development process and may be a game changer, is an excellent lens through which to explore this issue.

CHINA HAS BECOME A CENTRAL PLAYER IN AFRICAN ICT DEVELOPMENT

China has been involved in development aid for decades as part of its diplomatic strategy. Its influence in African countries' development has increased considerably in recent years, not only through aid but also through a range of financial tools that enable Chinese companies to invest in infrastructure development projects.

Chinese development aid policy is now coordinated by the Chinese Ministry of Commerce (MOFCOM) and executed through the two Chinese "policy banks"—China Exim Bank and China Development Bank. Some of the financing tools used by China fall under the category of "official development assistance" (ODA) as defined by the OECD Development Assistance Committee. They generally consist of concessional (subsidized) loans by Exim Bank. According to the *China White Paper on Foreign Aid* issued by the Chinese State Council, Africa was the recipient of 45.7 percent of Chinese foreign aid in 2009.[15] The *White Paper on China-Africa Economic Trade and Cooperation*, published by the Information Office of China's State Council in 2010, states that "from 2007 to 2009, China provided US$5 billion of preferential loans and preferential export buyer's credit to Africa. It has also promised to provide US$10 billion in preferential loans to Africa from 2010 to 2012."[16, 17]

In fact, the main tools of the Chinese development policy in Africa do not count as "aid," according to the OECD standard (they fall into the category of "Other Official Flows"), although they do contribute to infrastructure development. That essentially includes export buyers' credits (loans with or without a preferential rate) and other financial tools that facilitate Chinese corporations' exports in Africa. Deborah Brautigam quotes Li Ruogu, president of China Exim Bank, who announced in 2007 $20 billion of export buyers' credits over three years. She also mentions that by 2010, China Development Bank had committed more than $10 billion to projects in Africa in loans at commercial rates.

Besides, Chinese policy banks can use "strategic lines of credit" to help key Chinese corporations invest in Africa through a combination of sellers' credit, export buyers' credits, import credits, and preferential loans.

The Chinese commitment to increase trade and cooperation with African countries was confirmed by the creation of the Forum on China-Africa Cooperation,[18] which has held summits every three years since 2000. In a report for the OECD, Martyn Davies underlines that this is part of a Chinese "state-capitalist" approach, with state-owned companies in key sectors and policy banks through which China can make strategic commitments to Africa. This enabled China to increase the outbound foreign direct investment (FDI) in a "countercyclical" manner.[19] Although Africa may not be China's top priority, Chinese aid and, even more important, Chinese investments in Africa have increased considerably, making China one of the key actors in development in Africa, at a time when contributions from other donors and investors (mainly western countries) may stagnate or decrease as a consequence of the global economic crisis.

While these investments mostly go to such sectors as mining, resource extraction, energy, or financial services, they also fund a certain number of important infrastructure projects in the field of telecommunications. For example, the *White Paper on China's African Policy* states that "the Chinese Government will step up China-Africa cooperation in transportation, *telecommunications*, water conservancy, electricity and other types of infrastructure."[20]

As a result, such companies as the Chinese manufacturers Huawei and ZTE are becoming major players, winning huge contracts to implement telecommunication networks that are still underdeveloped in many countries. One of the most striking examples is the case of Ethiopia, where, according to Brautigam, "ZTE was able to offer finance for the Ethiopian Government's Millennium Telecoms Project, securing a US$1.5 billion deal."[21] In 2008, ZTE was chosen as the exclusive partner to build the Ethiopian telecommunications backbone network.[22]

I. CITIZENS' RIGHTS

One key feature of the discourse about telecommunications in terms of development is that ICTs are supposed to enable more transparent and, therefore, more efficient governance. ICTs are conceived as tools for better planning and resource allocation. The digitization of administrations is supposed to reduce bureaucratic burdens and increase the efficiency of public policies. E-government and open data are supposed to improve accountability and transparency. In general, the development of telecommunications may be a source of empowerment for civil society. In other words, ICTs not only may be a leverage tool for economic development but also may carry the potential to improve the functioning of democracy itself.

In that perspective, the increasing success of China in developing countries is puzzling, because China is one of the earliest and most efficient censors of telecommunications and particularly of the Internet in its own territory. The organization Reporters Without Borders qualifies China as an "enemy of the Internet"[23] because of its censorship practices and its repression of cyberdissidents. China was also one of the main targets of Hillary Rodham Clinton's speech on "Internet Freedom" in 2010.[24]

In fact, beyond the question of freedom of speech per se, the specificity of China is to have bet on ICTs as leverage for economic development without really introducing democracy, which questions the assumption of a link between ICTs, transparency, and democratization. The Internet is part of the strategy of the Chinese government to modernize the country and provide business opportunities throughout the territory. Administrations are also supposed to modernize and become more efficient and accountable through the use of ICTs. At the same time, Chinese citizens' expression online is tightly controlled and subtly channeled so that they can let off steam, but they can never seriously question the regime.[25] Rebecca MacKinnon calls this "networked authoritarianism."[26]

Therefore, one of the main concerns when it comes to Africa is that China may promote its own conception of telecommunication, as both an accelerator of economic development and a tool of social control. Indeed, China has the capacity to provide African countries with technologies as well as legal and practical expertise to censor public opinion and spy on dissidents.

There are examples of African countries that censor telecommunications. Ethiopia strengthened its control of telecommunications substantially in the last few years, while engaging in efforts to develop infrastructure (only 1.1 percent of the Ethiopian population has access to the Internet so far).[27] The country now uses deep packet inspection to block proxy services such as Tor, allegedly thanks to technologies provided by China with a $1.5 billion loan.[28] Ethiopia is considering legislation that would make voice over Internet protocol (VoIP) illegal and that would give "the ministry of communications and information technology the power to supervise and issue licenses to all privately-owned companies that import equipment used for the communication of information," according to Reporters Without Borders.[29] The latter measure, which would introduce a kind of intermediary liability, is one of the key characteristics of the Chinese domestic Internet control architecture (although holding intermediaries liable for content is now prevalent throughout the world).

However, not all the African countries where Chinese companies operate have adopted such policies and censorship technologies. There are great differences throughout the continent. For example, apart from the Ethiopian case, the Open Network Initiative has found no evidence of Internet filtering in Sub-Saharan Africa,[30] while most countries in the Middle East and North Africa region use various methods of Internet filtering and control.[31] The differences between countries seem to depend on such factors as the level of development of ICT infrastructures (the Internet access rate is on average much higher in the Middle East and North Africa region than in Sub-Saharan Africa, and so are the corresponding censorship technologies) and, of course, on the type of regime, rather than on the presence of Chinese providers.

What may have changed, though, is that if required by an African government, censorship technologies cannot anymore be purchased exclusively from western companies[32] but may be purchased from Chinese companies, which have acquired a more competitive position in this market. In fact, Chinese corporations seem to have similar reputation problems as western companies when it comes to providing censorship technologies to authoritarian countries. Both Huawei and ZTE have had to promise to reduce their partnership with Iran after the fact that they had provided censorship technologies was revealed, and also out of concerns about the Iranian nuclear projects.[33]

As their business is growing, Chinese companies are now putting much work into improving their image globally, including through transparency efforts. This happens in a context where the ICT sector is perceived as extremely sensitive, notably because of the cybersecurity and sovereignty issues that it raises.

II. TRANSPARENCY, CYBERSECURITY, AND SOVEREIGNTY

Precisely because ICTs bear important democratic promises, they are particularly sensitive in terms of state sovereignty and public order. For example, the vice president of Huawei, Guo Tianmin, announced that his company was able to provide the Congolese authorities with adequate infrastructure for conducting a population census, identity card fabrication, and electoral filing for future elections.[34] Although the promises brought by such technologies are extremely appealing, there are risks such as data theft (for foreign intelligence) or manipulation (to destabilize the country). One may wonder whether it is safe for a country to put such data and power in the hands of foreign companies, be they Chinese or other.

This concern is emerging at a time when cybersecurity is becoming an important issue in global affairs, China and the United States being among the key players of a sort of "cyber war."[35] In this context, the United States and Australia have barred Huawei and ZTE from participating in bids to build network construction projects on their territories.[36] Meanwhile, the U.S. Congress investigated whether the "networking equipment sold could secretly contain Chinese military technology to spy and interfere with U.S. telecommunications"[37] and concluded that Chinese telecom equipment makers should be kept from the U.S. market.[38] It is notable that the Chinese government also claims that China is the victim of many cyber attacks.[39] In general, every country in the world is paying more attention to cybersecurity and to the impact of ICTs in terms of state sovereignty.

True, there is not enough transparency among Chinese corporations to be able to dispel concerns about cybersecurity. First, there are intricate links between the Chinese Communist Party and the leadership of the Chinese corporations. This is a very common feature in China, due to the frequent conversion of political positions into economic responsibilities since the beginning of the 1980's economic reforms, but it is considered with particular suspicion in this sensitive sector. For example, Huawei's founder, Ren Zhengfei, is known for having held the position of deputy director in the Chinese People's Liberation Army's engineering corps. Sun Yafang, the chairwoman, used to work for China's Ministry of State Security.[40] Although Huawei is formally a privately owned company, the personal and informal ties that link its leadership to the Chinese authorities may be binding (which the Chinese firmly deny).

Besides, there is a relative lack of transparency in Chinese development projects in Africa (and elsewhere) and the amounts invested.[41] China does not report aid to the Development Assistance Committee—whereas other nonmember countries do. It is also very difficult to find figures broken down by country or by sector. This lack of accurate and up-to-date data about Chinese aid and investments in Africa is a source of concern for the donor community, which is trying to increase coordination efforts in order to improve aid efficiency.[42] This is particularly paradoxical, since ICTs are usually associated with greater transparency. However, this is also a very sensitive and strategic area, that is, in the eyes of the Chinese, not so much about aid but essentially about exports and investment.

Indeed, the dynamism of the Chinese banks and manufacturers in this region is primarily an element of the Chinese "going-out strategy." This strategy, launched by the Chinese leaders in 2000, is an encouragement for Chinese companies to invest abroad in order to reduce the volatility of Chinese financial assets and expand their markets. The handling of the issue by MOFCOM instead of the Ministry of Foreign Affairs also suggests that the Chinese perspective is now more economic than diplomatic. In other words, these projects are considered as a strategic element of the Chinese economic and industrial expansion, which explains a certain level of secrecy.

The Chinese telecommunications companies have made some efforts, however, to increase their level of transparency in order to reassure potential commercial partners.[43] In December 2010, Huawei opened a "Cyber Security Evaluation Centre" in Great Britain[44] where they let potential buyers test their products for potential threats. In spring 2011, the annual report of the company, audited by KPMG, released for the first time the names of Huawei's board members (but only to receive more criticism when Sun Yafang's past at the Ministry of State Security was revealed, as well as the presence of several members of the Ren family in the list).[45] Huawei is said to be considering a potential listing in the U.S. stock market, which would force Huawei to disclose even more information.[46]

These transparency efforts highlight the uncomfortable position of the Chinese telecommunications companies. ICTs are considered to be an extremely sensitive area in China, monitored closely by the authorities. As such, the lack of transparency and the links between the party and the company are not surprising, just like in any leading economic sector in China. At the same time, as industrial giants, Huawei and ZTE are supposed to take part in the Chinese "going-out strategy" and conquer new markets. Although it may be technically possible to implement devices or software enabling some forms of spying or manipulation, any discovery of such technologies on Chinese installations could ruin the companies' decade-long efforts to gain global trust and could seriously hamper profits. In that sense, there is no evidence to support the hypothesis that Chinese companies would be different from any of their western counterparts that are competing for the same markets and that could also raise cybersecurity issues.

Actually, from an African point of view, cybersecurity is only one among various sovereignty concerns. As there are relatively few local resources in terms of technology and know-how, most African countries rely on foreign development projects to develop their ICT infrastructures. Moreover, development aid in Africa by western organizations and companies is sometimes considered to be a new form of "imperialism" or "colonialism" to the benefit of western countries.[47] Indeed, foreign aid is most often conditional upon or designed so that contracts are signed with multinational corporations from the donor countries. Financial support from international organizations (the International Monetary Fund, the World Bank) is also conditional upon governance reforms that are often considered locally as infringements of sovereignty (privatizations, deregulation, suppression of trade tariffs, etc.).

In that regard, the relative opacity in which Chinese contracts are signed may be considered as an advantage for African countries that want to keep an upper hand on their own development policies and on the negotiations with international investors. Chinese investments are often considered locally as more politically neutral, since they are not tied to political conditions and governance reforms.

But are they really?

III. THE OPAQUE POWER OF NORMS

True, the Chinese actors in this field do not seem interested in changing political regimes or government practices in Africa. However, investing in Africa as part of the "going-out strategy" is clearly aimed at raising China's position as a global power. As such, it is one element of the Chinese government's recently enhanced "soft power" strategy. Based on Joseph Nye's theory,[48] this strategy aims at improving China's global influence and image not only through economic and industrial development but also by promoting Chinese language and culture, products, trademarks, standards, and technological know-how.[49] The global expansion of the Chinese media is a central element of this strategy, particularly in Africa.[50] The expansion of Chinese expertise, technologies, and norms in the ICT field is also a crucial element of this strategy.

Indeed, investing in African markets is part of a strategy to climb the ladder of innovation. China is investing a lot to develop its own technical standards in order to reduce its dependency on foreign technologies and actually start earning royalties. Moreover, implementing networks based on Chinese technologies in Africa may weigh in favor of China in the global negotiations over technical norms. As China is very active in pushing for the adoption of norms that are favorable to the Chinese interests in such fora as the Internet Engineering Task Force (IETF) or the International Telecommunication Union (ITU),[51] the fact that China is equipping an important part of the world may result in a kind of fait accompli. Therefore, it would be interesting to look more closely at the technological choices involved in these contracts, to assess how they may shape these countries' future relationships with China and with the international community.

Another related issue that will be crucial to look at in the near future is whether China will influence its African partners' positions in telecommunications governance. For example, Huawei's Guo Tianmin recently announced the opening of a new training center in Kinshasa (one of five in Africa).[52] Could this have any influence on the opinion of future African ICT experts on these issues?

As the treaty known as International Telecommunications Regulations, which dates back in 1988, is being renegotiated in 2012, China is taking very conservative positions that include the defense of digital sovereignty and the transfer of key competencies to the United Nations through the ITU.[53] The "multistakeholder" governance scheme that currently prevails in this field and that allows nonstate actors to take part in negotiations certainly does not have the support of China, as it is much too "volatile," so to speak, compared to the very codified, exclusive standards of intergovernmental negotiation.[54]

In this context, China is positioning itself as a representative of developing countries' interests, arguing (with relatively good reason) that multistakeholder governance gives more influence to developed countries (particularly to the United States). These governments and for-profit and not-for-profit organizations all have better resources for lobbying than do those of developing countries. This argument seems to resonate with a number of developing countries. This year's negotiations at the ITU will be an excellent occasion to assess whether some African countries take positions that are close to the Chinese and what they are.

CONCLUSION

The fact that new actors like China are acquiring an increasingly important role in the development of new infrastructures in Africa certainly has the potential to deal the cards. In the field of information and communication technologies, there are important stakes beyond the field of development aid, from freedom of speech to cybersecurity and to global telecommunications governance.

Not all Chinese practices are different from western countries' practices. Chinese companies, too, are selling technologies that are supposed to increase transparency and accountability in African countries. Chinese companies, too, are selling technologies that help governments monitor, filter, or censor their citizens' expression. But the well-known expertise of China in using ICTs to control its own population has shed a new light on the fact that there is no direct link between ICTs, transparency, and democratization. This all depends on various factors and particularly on the recipient country's political agenda as well as on the people's appropriation of the technologies.

As a consequence, the very attempt to study the Chinese role in "Africa" is very limited. It symbolically implies that African countries would be passive objects of other entities' actions, which is not the case. Africa is a very diverse continent, with all sorts of political regimes, levels of development, and local dynamics. At this stage, it seems important to advocate for more specific case studies in a series of African countries.

Chinese and western companies are also not that different in that they raise cybersecurity and sovereignty issues for African countries that put their most sensitive data and government processes into these companies' hands. All of them are now competing to develop, implement, and normalize new technological standards and therefore exercise power on the people and countries that will use them. The very sensitive character of these technologies and the geopolitical stakes paradoxically lead to a certain level of secrecy around the technologies that are supposed to bring more transparency.

However, China is different from other countries in that its development projects are most often not considered as aid but as investment, for the conquest of new markets in the framework of the "going-out strategy." More generally, this is part of the Chinese "soft power" strategy, which aims at increasing China's global power through economic, technological, and cultural domination. Both Africa and ICTs are clearly identified as strategic goals in that regard. The initiatives to increase transparency undertaken by such companies as Huawei and ZTE are, in fact, only the result of an effort to gain trust in the international markets, not that of a will to increase coordination with other donor countries. The flip side of this coin is that it gives recipient countries more autonomy in their own political and economic choices, whereas governance requirements by other donor countries (including transparency) are perceived as a new form of western hegemony.

What the Chinese rise underlines is in fact the hard competition that the world's biggest technological powers are involved in and the importance of developing countries as an enormous stake in this battle. Western calls for more transparency seem not only motivated by the need to improve aid coordination (though this seems justified) but also by a perceived potential threat to their own interests in Africa.[55]

This puts at the forefront the issue of the political importance of "code" and technical standards.[56] These stakes have remained relatively opaque to the public so far, perhaps partly because of their highly technical character. Opacity may also be inherently linked to the development of ICTs as it is shaped now, based on a race to impose proprietary technologies. Therefore, one might suggest the idea that open source technologies, together with technological training, could be an interesting solution to efficiently improve transparency, better guarantee developing countries' sovereignty, and avoid getting trapped in a technological race at the expense of users and citizens.

ENDNOTES

[1] *Paris Declaration on Aid Effectiveness* (2005) and *Accra Agenda for Action* (2008). www.oecd.org/dataoecd/11/41/34428351.pdf.

[2] http://www.aideffectiveness.org/busanhlf4/images/stories/hlf4/OUTCOME_DOCUMENT_-_FINAL_EN.pdf.

[3] Tim Unwin, *ICT4D: Information and Communication Technology for Development* (Cambridge University Press, 2009). Several journals are entirely dedicated to this field: *Information Technology for Development*; *Information Technologies and International Development*; *Electronic Journal of Information Systems in Developing Countries*, etc.

[4] At the same time, more and more studies warn against techno-determinism and underline that this increasing role of ICTs is coming along with a new set of technological, economic, political, and anthropological issues. See a good bibliography on the blog of Ismael Peña-Lopez, *ICTlogy*. http://ictlogy.net/bibliography.

[5] John C. Bertot, Paul T. Jaeger, and Justin M. Grimes, "Using ICTs to create a culture of transparency: E-government and social media as openness and anti-

corruption tools for societies," *Government Information Quarterly* 27: 3 (July 2010): 264-271.

6. World Bank, *Information and communication for development 2012—Maximizing mobile* (Washington, DC: 2012). http://siteresources.worldbank.org/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/Resources/IC4D-2012-Report.pdf.

7. World Bank, *Information and communications for development 2009: extending reach and increasing impact* (Washington, DC, 2009). http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/EXTIC4D/0,,contentMDK:22229759~menuPK:5870649~pagePK:64168445~piPK:64168309~theSitePK:5870636,00.html.

8. See their policies at http://www.usaid.gov/our_work/economic_growth_and_trade/info_technology.

9. Richard Heeks, "The ICT4D manifesto" (Manchester, UK: OECD Development informatics working paper series, Institute for Development Policy and Management, 2009).

10. http://www.wikiprogress.org/index.php/OECD_Development_Centre.

11. http://wikigender.org/index.php/New_Home.

12. For example, Algeria banned Huawei and ZTE from bidding in public markets for two years last June because employees of both companies were convicted of bribery. Juha Saarinen, "Huawei, ZTE banned from Algeria," *IT News* (June 14, 2012). http://www.itnews.com.au/News/304858,huawei-zte-banned-from-algeria.aspx.

13. Deborah Brautigam, *China, Africa, and the global aid architecture* (Abidjan, Ivory Coast: Africa Development Bank, 2010). http://www.american.edu/sis/faculty/upload/Rev-working-paper-china-africa-aid-architecture-August-2010.pdf; Martyn Davies, *How China is influencing Africa's development* (Paris, France: OECD Development Centre, 2010); Johan Lagerkvist, "Foreign aid, trade and development," *Occasional UI papers* 5 (2011).

14. See, for example, Rebecca MacKinnon, *Consent of the Networked: The Worldwide Struggle for Internet Freedom* (New York: Basic Books, 2012).

15. China State Council, *China White Paper on Foreign Aid* (Beijing, China: March 21, 2011). http://english.gov.cn/official/2011-04/21/content_1849913.htm.

16. Information Office of the State Council, *White Paper on China-Africa Economic Trade and Cooperation* (Beijing, China: December 2010). http://english.gov.cn/official/2010-12/23/content_1771603.htm.

17. Brautigam estimates that Chinese aid (ODA) to Africa was about $1.2 billion in 2008 and probably $1.4 billion in 2009. Deborah Brautigam, "Chinese Aid: What, Where, Why and How much?" in *Rising China. Global challenges and opportunities*, ed. Jane Golley and Ligang Song (Canberra, Australia: ANU E Press, 2011), pp. 203–222. http://epress.anu.edu.au/wp-content/uploads/2011/08/ch131.pdf.

18. Forum on China-Africa Cooperation (Beijing, China). http://www.focac.org/eng/.

19. Davies, *How China is influencing Africa's development.*

20. Information Office of the State Council, *White Paper on China's African Policy* (Beijing, China: January 2006). http://english.peopledaily.com.cn/200601/12/eng20060112_234894.html. Emphasis added.

21. Deborah Brautigam, "Chinese Aid," pp. 203–222.

22. ZTE Corporation, "ZTE to Help Ethiopia Telecommunications Corporation Build National Network," *ZTE* (Beijing, China: July 2, 2008). http://wwwen.zte.com.cn/en/press_center/news/200807/t20080703_156835.html.

23. Reporters Without Borders, "World Day Against Cyber Censorship" (March 12, 2011) (Paris, France). http://march12.rsf.org/en/#ccenemies.

24. Hillary Rodham Clinton, "Internet Freedom," *Foreign Policy* (January 21, 2010). http://www.foreignpolicy.com/articles/2010/01/21/internet_freedom?page=full.

25. Séverine Arsène, *Internet et politique en Chine* (Paris, France: Karthala, 2011); Séverine Arsène, "Chine : Internet, levier de puissance nationale," *Politique étrangère* 2 (2012): 291–303.

26. Rebecca MacKinnon, "China's Networked Authoritarianism," *Journal of Democracy* 22: 2 (2011): 32–46.

27. ITU (Geneva, Switzerland, 2011). http://www.

itu.int/ITU-D/ict/statistics/explorer/index.html.

28. Andrew Jacobs, "China's News Media Are Making Inroads in Africa," NYTimes.com, August 16, 2012. http://www.nytimes.com/2012/08/17/world/africa/chinas-news-media-make-inroads-in-africa.html?pagewanted=all.

29. Reporters Without Borders, "Government steps up control of news and information" (Paris, France: June 7, 2012). http://en.rsf.org/ethiopia-government-steps-up-control-of-07-06-2012,42735.html.

30. OpenNet Initiative, "Sub-Saharan Africa." http://opennet.net/research/regions/ssafrica.

31. OpenNet Initiative, "Middle East and North Africa." http://opennet.net/research/regions/mena.

32. It is useful to note that western corporations like Cisco, McAfee, or Websense sell most censorship technologies in the world. Helmi Noman and Jilian York, *West Censoring East: The Use of Western Technologies by Middle East Censors, 2010–2011*, OpenNet Initiative, March 2011, http://opennet.net/west-censoring-east-the-use-western-technologies-middle-east-censors-2010-2011.

33. Steve Stecklow, Farnaz Fassihi and Loretta Chao, "Huawei, Chinese Tech Giant, Aids Iran," WSJ.com, October 27, 2011. http://online.wsj.com/article/SB10001424052970204644504576651503577823210.html; Bryan Bishop, "ZTE follows Huawei's lead, promises to curb Iran business after surveillance system sale," *The Verge* (March 24, 2012). http://www.theverge.com/2012/3/24/2898835/zte-follows-huaweis-lead-promises-to-curb-iran-business-surveillance-system.

34. Angelo Mobateli, "Congo-Kinshasa: Kabila inaugure le centre régional Huawei de formation des experts," *Allafrica*, May 26, 2012. http://fr.allafrica.com/stories/201205260006.html.

35. Nick Hopkins, "US and China engage in cyber war games," guardian.co.uk, April 16, 2012. http://www.guardian.co.uk/technology/2012/apr/16/us-china-cyber-war-games.

36. Yueyang (Maggie) Lu, "Australia Bars Huawei From Broadband Project," NYTimes.com, March 26, 2012. http://www.nytimes.com/2012/03/27/technology/australia-bars-huawei-from-broadband-project.html.

37. Michael Kan, "US Committee to Investigate China's Huawei, ZTE," *PCWorld*, November 18, 2011. http://www.pcworld.com/businesscenter/article/244210/us_committee_to_investigate_chinas_huawei_zte.html.

38. Jim Wolf and Lee Chyen Yee, "China's Huawei, ZTE should be kept from U.S.—draft Congress report," Reuters, October 8, 2012. http://uk.reuters.com/article/2012/10/08/uk-usa-china-huawei-zte-idUKBRE89702A20121008.

39. Information Office of the State Council, *White Paper on the Internet in China* (Beijing, China: June 15, 2010). http://china.org.cn/government/whitepaper/node_7093508.htm.

40. Kevin Brown, "Huawei's opacity a colourful issue for US," *Financial Times*, April 19, 2011. http://www.ft.com/cms/s/0/65e93b90-6a84-11e0-a464-00144feab49a.html#axzz1uafyc2XQ.

41. Sven Grimm, "Transparency of Chinese Aid: an analysis of the published information on Chinese external financial flows," University of Stellenbosch (Cape Town, South Africa: Centre for Chinese Studies, August 2011). http://www.aidtransparency.net/wp-content/uploads/2011/08/Transparency-of-Chinese-Aid_final.pdf.

42. Deborah Brautigam, *China, Africa, and the global aid architecture* (Abidjan, Ivory Coast: Africa Development Bank, 2010). http://www.american.edu/sis/faculty/upload/Rev-working-paper-china-africa-aid-architecture-August-2010.pdf.

43. In fact, these transparency efforts seem to be aimed at European and U.S. decisionmakers rather than at developing countries.

44. Huawei, "Huawei Opens Cyber Security Evaluation Centre in the UK" (Beijing, China: December 6, 2010). http://www.huawei.com/en/about-huawei/newsroom/press-release/hw-093468-ukcenter-security.htm.

45. *Economist*, "Huawei, The long march of the invisible Mr. Ren," June 2, 2011. http://www.economist.com/node/18771640.

46. Spencer E. Ante, Telis Demos and Anupreeta Das, "China's Huawei Considers an IPO [initial public offering]," *Wall Street Journal*, October 4, 2012. http://online.wsj.com/article/SB10000872396390443493304

578036860213855012.html.

47. Y. Z. Ya'u, "The new imperialism & Africa in the global electronic village," *Review of African Political Economy* 31: 99 (2004): 11–29 ; Olivier Sagna, "De la domination politique à la domination économique: une histoire des télécommunications au Sénégal," *tic&société* 5: 2–3 (2012). http://ticetsociete.revues.org/1030 ; Jørn Støvring, "'The Washington Consensus' in relation to the telecommunication sector in African developing countries," *Telematics and Informatics* 21: 1 (2004): 11–24.

48. Joseph S. Nye, *Soft power: the means to success in world politics* (New York: Public Affairs, 2004).

49. Bates Gill and Yanzhong Huang, "Sources and limits of Chinese 'soft power'," *Survival* 48: 2 (2006): 17–36.

50. Jacobs, "China's News Media"; Iginio Gagliardone, Maria Repnikova and Nicole Stremlau, *China in Africa: a new approach to media development?* (University of Oxford, 2010). http://stanhopecentre.org/china-africa/mod/file/download.php?file_guid=1926.

51. See the examples of the WLAN Authentication and Privacy Infrastructure (WAPI) standard or the Multiprotocol Label Switching (MPLS). Christopher Gibson, "Technology Standards—New Technical Barriers to Trade?" *The standards edge: golden mean,* ed. Sherrie Bolin (Ann Arbor, MI: The Bolin Group, 2007). http://papers.ssrn.com/sol3/papers.cfm?abstract_id=960059; Iljitsch van Beijnum, "ITU bellheads and IETF netheads clash over transport networks," *ars technica* (March 03, 2011). http://arstechnica.com/tech-policy/news/2011/03/itu-bellheads-and-ietf-netheads-clash-over-mpls-tp.ars.

52. Mobateli, "Congo-Kinshasa: Kabila inaugure le centre régional Huawei."

53. Robert McDowell, "The U.N. Threat to Internet Freedom," WSJ.com, February 21, 2012. http://online.wsj.com/article/SB10001424052970204792404577229074023195322.html; Ben Woods, "Schmidt: UN treaty a 'disaster' for the internet," *ZDNet UK* (February 29, 2012). http://www.zdnet.co.uk/news/regulation/2012/02/29/schmidt-un-treaty-a-disaster-for-the-internet-40095155/.

54. For more details, see Milton Mueller, "China and Global Internet Governance," in *Access contested*, ed. Ronald Deibert, Rafal Rohozinski, and Jonathan Zittrain (Cambridge, MA: MIT Press, 2012): 177–194. http://access.opennet.net/wp-content/uploads/2011/12/accesscontested-chapter-09.pdf.

55. Joanne Wagner, "'Going Out': Is China's Skillful Use of Soft Power in Sub-Saharan Africa a Threat to U.S. Interests?" *Joint Force Quarterly* 64 (July 2012). http://www.ndu.edu/press/chinas-use-of-soft-power.html.

56. Lawrence Lessig, *Code and other laws of cyberspace* (New York, Basic Books, 1999).

Complicating the Already Complicated: Diplomacy, Development, and the New Media

Gerald F. Hyman

The core of diplomacy has varied little for close to a millennium. It involved exchanges of emissaries between sovereigns: kings, queens, emperors, sultans, and chiefs. The eighteenth century brought elected sovereigns. The nineteenth and certainly the twentieth century brought the nation-state and much more immediate methods of communication between capitols and their emissaries—telegraph and telephone, for example—so instructions could be more specifically tailored and diplomatic discretion reduced, but the basic pattern remained.

Similarly, the first few decades of development assistance after the end of World War II created a fairly consistent pattern among donors and between donors and recipients. The donors' objective was to contribute to creating consistent improvement in the countries in which they were engaged. Indeed, the mission of the U.S. Agency for International Development (USAID) was "sustainable development' in "sustainable development countries," the vocabulary most articulately employed during the Clinton administration but that also characterizes previous administrations and is characteristic as well of the other bilateral donors and the multilateral donors, like the World Bank and its sister regional banks.

It would be hyperbolic to say that the past decade has brought dramatic change to those two paradigms (diplomacy and development), but it has brought nontrivial change. For one, the object of, and conduit for, diplomacy and development is no longer always the state or the sovereign, the result most obviously of the attacks of September 2001 on New York and Washington and the resulting but new fixation on terrorism and conflict within states and internationally through opaque networks for which state boundaries are irrelevant. For another, the modes of communication inside and, more importantly, outside government, have changed markedly. Governments are only one kind of actor, and generally their domestic and international control has diminished, partly as a result of globalization, partly as a result of internal and external conflict, partly because governments in many states have lost the monopoly of force and also of communications, partly for a myriad of other reasons. Perhaps more important, the formerly secondary "public diplomacy" has become more central. Public perceptions are now more pivotal to diplomacy. Secret agreements and personal relations are less binding than they once were. Still important, they no longer suffice to define interstate relations, if they ever did. Similarly, development projects can no longer be simply the result of quiet agreements between diplomatic or assistance emissaries and prime ministers, presidents, or kings. The result is some, again, nontrivial change in both diplomacy and development and in their interconnection.

Two features, in particular, help define the new landscape of diplomacy and development, at least for the United States. First, the new media have created a much more transparent environment in which everything is now public, or at least should be assumed to be public, because soon enough it will be. As a minor corollary, the connection between diplomacy and development is now also more visible. The consequences are mixed. The public is now far more exposed, and therefore engaged, in the intricacies of diplomacy that were once undertaken in quiet discussions and paneled offices. That engagement "democratizes" the relations between countries, including their assistance relations. But it can also expose the discussions of statecraft "prematurely," while they are still being fashioned and molded. It can also expose classified information that harms a variety of legitimate interests including the bargaining position of any or all of the parties in a relation. Second, relations between coherent states is only one dimension of diplomacy, albeit still perhaps the dominant one. Fragile, failing, fragmented, and conflict-ridden societies (not just states) are also part of the diplomatic and developmental environment, and they create very different kinds of problems: How does a state relate to an entity with formal legal character but unable really to speak for its citizens let alone to claim the old sine qua non for a state: monopoly of legitimate force and authority?

In effect, the world has become more transparent, mostly for the better but with complications for diplomacy, development, and their connections. Publics know better what their governments, corporations, and other centers of power are doing. Autocrats cannot hide but neither can democrats. Groups can organize better, more cheaply, and more anonymously to oppose torture, abuse, and tyranny but also to inflict terror, exacerbate communal tensions, and stoke hatred and violence. It is part of the work of this new era to maximize the advantages of the new information age and to minimize its disadvantages.

DIPLOMACY AND DEVELOPMENT: THE HISTORICAL RELATIONS

Notwithstanding the mistaken nostalgia of much of the foreign assistance community, development was never truly independent of foreign policy and diplomacy in the United States, or, for that matter (again notwithstanding widespread views to the contrary), among the other donors either. In fact, Congress has for decades divided the omnibus International Affairs Budget, the so-called 150 account, into ten or twelve subaccounts of which only one, for Development Assistance (DA), is the budget normally associated with broad, sustainable development goals.[1]

One such other account is, probably misleadingly, called Economic Support Funds (ESF). If the Development Assistance account supports primarily long-term sustainable development allocated to countries whose policies and performance justify confidence that U.S. assistance will contribute to their developmental progress, ESF is allocated primarily for foreign policy reasons and covers a wide range of projects, only a fraction of which deal directly with economic issues. While DA has in the past been programmed almost entirely by USAID, the official development agency, ESF has always been under the *policy* direction of the Department of State. The State Department decides, in some degree of partnership with USAID, the countries to which ESF should go, the amounts for each country, and (more recently) what should be done with it. State's regional bureaus make their requests through the secretary of State to the Office of Management and Budget, and the State regional bureaus are at least the senior partners in the country budget determinations. The degree of their partnership with USAID has varied from region to region, time to time, and sometimes from person to person. But until recently, State has not normally directly implemented assistance programs. It has relied on USAID to make the actual grants or contracts. So State has traditionally laid out the policies, while USAID has designed the specific programs and managed the funds.[2]

But if foreign policy has determined assistance levels and policies, assistance has also been a part of foreign policy. It has been one of the tools available to diplomacy for influencing the policies of other states. State has used it as one incentive among several to gain allies and affect behavior.[3] In that respect, it has both shaped and mirrored the relations between the United States and other counties countries at least since the Marshall Plan and (during the Cold War) the policy of containment, in both cases over a decade prior to the creation of USAID. For example, Turkey received ESF in part because of its geostrategic position astride the Bosphorus and the Dardanelles, in part because of support by the Turkish military, and in part because of Incirlik Air Base. Similarly, the Philippines got substantial amounts of ESF primarily because of U.S. access to Clark Air Force Base and Subic Bay Naval Base, not as much because of its development record. Egypt is the classic case, with a $750 million assistance package because it signed the Camp David agreements and made its peace with Israel.

Even after the collapse of the Warsaw Pact and then the Soviet Union—so after the Cold War—Congress created two totally new ESF-like assistance accounts. One was for Central and Eastern Europe, and later another was for the countries of the former Soviet Union itself both with special assistance coordinators, in both cases housed at State. Deputy Secretary of State Lawrence Eagleburger was the first coordinator for the counties of Central and Eastern Europe. Substantial food aid has been provided to North Korea beyond the amounts of the past, not only because the chronic famine has worsened but also as part of the Six-Party Talks aimed at the disclosure and reduction of its nuclear resources, research, and potential for weapons. Moreover, South Sudan received millions of dollars in assistance, initially primarily humanitarian relief in the "rebel-held" part of Sudan, now to help it succeed as an independent country. Most thematic (as opposed to geographic) bureaus at State now have assistance programs. The amount of ESF was not reduced after the Cold War nor were its purposes systematically reconsidered once the lens of Soviet containment was removed. Instead, the door was opened for a florescence of creativity at Foggy Bottom, as almost any project in almost any bureau was fair game. So for a while at least, ESF was a potential source of funding for a lot of different projects in a lot of different countries, some large and important to core foreign policy and security considerations, others definitely not. If anything, it might be argued that greater conceptual and policy discipline should be reasserted over the many foreign policy principles that drive ESF funding.

TERRORISM, INSURGENCY, AND CONFLICT

That discipline and purpose have to some extent been supplied not by some positive conception of national interest or development but, unfortunately, by the tragedy of September 11. The first direct attack on the United States came, ironically, not from the military strength of the industrialized Soviet empire for which the West had developed such extensive doctrine and defense. It came instead from a few dozen, at most a few hundred, barely armed religious zealots who developed their plans in the caves and villages of a barely agricultural collection of violent internecine rivalries between ethnic groups, tribes, and clans.

Two effects for the relation between diplomacy and development resulted. The first and most obvious were the wars in Afghanistan and Iraq together with the subsequent doctrine of counterinsurgency, revised from that of Vietnam. Shock and awe may have been enough to dislodge both the Taliban and Saddam Hussein, but they were insufficient to secure the peace, stability, and comity necessary to stabilize these countries. Instead, the United States was engaged in two unconventional, "asymmetric" wars: nine years in Iraq, eleven years (and still counting) in Afghanistan. As in Vietnam, these were more than just military encounters and required more than just a military engagement. The latest iteration of counterinsurgency doctrine, developed under General David Petraeus and encoded in Army Field Manual 3-24, has been abbreviated 'shape, clear, hold, and build' and is centered not on pure military targets but on the populations that support the insurgency. The "shape and clear" part is almost entirely military. The "hold" part is both military and civilian. The "build" part is, at least conceptually, primarily civilian and framed in developmental terms. Hundreds of billions of dollars have been programmed to "build" (Afghanistan) or "rebuild" (Iraq), and that counts only the portion provided by the United States, never mind the billions provided by other countries.

However, no matter what their term, they were provided not through the development or even the direct foreign policy procedures of State and USAID applicable to the other, nearly one hundred countries in which the United States provides assistance, but in the case of counterinsurgency under the disciplines and procedures of an active war. As in Vietnam, the assistance programs became instruments of the counterinsurgency effort. Moreover, the military itself had enormous amounts of funding available quite apart from the civilian assistance budgets. For example, the Commander's Emergency Response Program (CERP) provided local commanders with sometimes large amounts of actual cash to distribute to local individuals, groups, or "governmental" structures. In theory, CERP was for projects, but "projects" sometimes as individual as rebuilding a family home, opening or stocking a small store, or repairing an irrigation sluice. Sometimes these very funds were retaxed by the insurgents so, in effect, the United States was funding the insurgency with its own counterinsurgency funds. Of course, there were no committees or formal procedures attaching to the CERP funds. They were immediate, tactical tools.

Moreover, even the hundreds of millions, in fact the billions, of dollars available through what purported to be normal channels of assistance were also in fact at the immediate service of the counterinsurgency effort, under the very strong influence of the military and under the very direct authority and instruction of the ambassador. So, if the ambassador and the commanding general or their immediate subordinates (themselves sometimes ambassadors and generals) thought that improving irrigation systems or education systems or court systems was important to the counterinsurgency, they were funded, often without the design or monitoring efforts that accompanied normal assistance programs. Indeed the State and USAID civilians attached to the military, for example in provisional reconstruction teams (PRTs), were often overwhelmed with the immediate security imperatives to move money and implement projects and were so confined physically for their own security that they could not have undertaken anything like regular design and monitoring efforts even had they been allowed the latitude to do so.

As between diplomacy and development, the counterinsurgency and counterterrorism efforts also forged different relations of State and USAID, diplomacy and development, in Washington and, after the Quadrennial Diplomacy and Development Review (QDDR), in most "normal" countries.[4]

For example, in the PRTs in Iraq and Afghanistan, which were the most local unit for military but also for "diplomatic" and "development" or reconstruction efforts, the military have far outnumbered the civilians—in no small part because the civilian side often could not provide the needed personnel or their duration—and, at least as important, were under the direct command of the senior military officer. Development projects were almost totally at the immediate service of the military's security and pacification objectives although, to be fair, those objectives contained "build" and "hold" dimensions, not just "kinetic" efforts to "clear." Still, especially in the context of an exposed forward base, the military calls the shots, and the civilian programs, diplomacy as well as development, serve the security dimension. This is perhaps the right order, since security is the sine qua non for everything else, including the safety of the diplomacy and development staff. The State and USAID officers there are under the authority of the military commander (not surprising, since the PRTs are primarily military units) and, as between the two, the USAID officer often reports directly to the State officer, not the commander.[5] So the pecking order is: military; State; USAID. Diplomacy, in these environments, had little to do with geostrategic alliances and high foreign policy. Development had little to do with long-term economic or social improvement. Both had to do with pacifying the area and "turning" the loyalties of the local population to the (usually central) government, and all of the U.S. government officers used their respective tools for those purposes.[6]

To the extent that conflict in general and insurgency more particularly have become more central to U.S. foreign and development policy globally, the peculiar paradigms of counterinsurgency in Iraq and Afghanistan have also leaked into the more usual goals, relations, and procedures of State and USAID, of diplomacy and development more generally. Preventing, mitigating, or resolving domestic, internal conflicts is not the same as normal state-state diplomacy or sustainable development. And to the extent that Secretary of State Hillary Rodham Clinton's QDDR retains much salience, conflict prevention is now "a core mission" of State and USAID.[7] And Conflict and Stabilization Operations is now the name of a new bureau (and an attendant assistant secretary) at State. The attempt to intervene in domestic conflicts may well be a fool's errand, not the proper state-to-state work of diplomacy or even development, but for the moment it has taken a central place in both State and USAID. No doubt the cancer of conflict, especially if it crosses borders and creates regional instability, even global terrorism, creates the need for unusual engagements. Certainly it requires a change in roles, procedures, and paradigms.

Those constitute the second effect of counterterrorism on the relation between diplomacy, development, and security. In addition to its involvement in actual battleground states, the Department of Defense is now engaged in both diplomacy and development in a qualitatively different way, geographically and substantively. The diversion of its attention from states that directly threaten the security of the United States to those that threaten regional stability anywhere in the world has broadened its scope dramatically. And with that broader scope has come the use of Defense funding and Defense engagement in entirely different settings, including diplomacy and development.

The creation of an entirely new command—Africom—is only the most obvious example. No *state* in Africa has the intention, let alone the capacity, to threaten U.S. security except in the most derivative sense that they always did: their natural resources; bases that could be built by and made available to states potentially posing real threats; votes in international bodies; and the like—all of which have become less important since the end of the Cold War. However, if regional stability in Africa is a

U.S. *security* interest, and if guarding the security of every African state from the possibility of insurrection and instability and therefore the possibility of providing a haven for operatives of Al Qaeda or some other terrorist group is also a national security interest, and if virtually every African state has significant potential for instability, then the entire continent and all its fragile states warrant national security attention and therefore participation by the Department of Defense and the National *Security* Council. Regional stability in Africa, a secondary national security issue for diplomacy and defense during the Cold War, is now front and center. Indeed, the dispersal of national security threats so broadly defined as "instability" changes the purposes, the participants, and the calculations of both diplomacy and development.

So every country review now necessarily includes a serious consideration of conflict and instability, part of the core missions of State and USAID under the QDDR. Under the National Security Strategy of 2010, they also become part of the "whole-of-government approach" to that country, including the direct involvement of Defense resources and interests, which has had many multiples of the resources available to State or USAID. Those resources are now potentially available to the diplomacy and development programs in areas of conflict. And not just potentially. In fact, transfers have been made from the Defense budget to State and USAID for programs that would otherwise have been less well funded or funded not at all.[8] Indeed, somewhat unseemly appeals have been made by State and USAID to consummate such transfers and thereby to incorporate Defense into what had been purely State or USAID interests. So the actors, procedures, and paradigms of traditional diplomacy and development have shifted markedly to the extent that stability and conflict prevention have become central security purposes. Diplomacy and development in a country like Sri Lanka or Congo, never mind Somalia or Pakistan, are now qualitatively different.

THE INFORMATION AGE

The new age of widespread and immediate information more than complicates these changes in purposes, roles, resources, procedures, and paradigms. The wide availability of new media, especially social media, has changed both the domestic and the international dynamics themselves. And it has done so in the new context of fragility and conflict as well as in the older, more traditional context of formal state-to-state diplomacy and development. That availability has affected relations with every kind of country and almost every kind of context, from autocratic regimes to civil wars to humanitarian disasters to classified materials and to what were once state secrets.

The most obvious effect of the new information environment is on the relation between the United States and other governments. The old control by central authorities over capital-intensive, nondigital media with large plants and equipment—newspapers, television, and radio—has now been eroded. Where the previous first targets of many coup attempts were the capital garrisons, the airports, the rail links, and the television and radio stations, those traditional media outlets (the objects of skirmish precisely because they had virtual monopolies on communication with the public) are now far less relevant both to the dissemination of information and to the ability to mobilize and organize supporters and opponents.[9] Ordinary information, not just about crises like coups, is now also widely available, quite apart from official sources and whatever the wishes of the current government.

No doubt, governments still retain extensive powers to regulate information flows even with the new, more mobile, and more individualized sources of transmission, but their powers are much diminished, and they carry greater costs. Even if a government can in theory close down the Internet or capture cellphone towers and perhaps block satellite dishes, doing so in practice is not so easy, especially given the ability to send signals from neighboring countries.[10] Moreover, doing so would also shut down much commerce, make the country much less attractive to foreign investors, make domestic information harder to receive for the government's intended audiences, and carry other domestic and international consequences. In that sense, governments are much more vulnerable to public opinion and, in theory, commensurately more accountable irrespective of their governmental form and purely as a result of the new media. More important, the ability to organize antigovernment coalitions and activities has increased through the new media, so even authoritarian governments are more vulnerable, perhaps in some senses more accountable, through these new channels of information and opinion.[11]

Naturally, the reality is more complicated. First, authoritarian governments still control a preponderance of assets, so accountability is more complicated. Second, true accountability requires ordinary mechanisms to which governments are answerable, not protest demonstrations, insurgencies, and coups. Absent fair elections, the rule of law, and institutional checks and balances, institutional accountability would seem to rely on extraconstitutional procedures (rather than embedded structures and procedures), and that kind of accountability is crude, hard to direct, very difficult to organize, and with uncertain results. Protests and insurgencies do sometimes arise spontaneously, as the events in Tunisia demonstrate. But publics are much more likely to endure years of privation and control than to revolt, especially when security services use force and intimidation. Nevertheless, the new media have made anonymity, hence some measure of protection, more feasible and have therefore reduced the risks of and exposure to reprisals notwithstanding the new countermeasures governments can take to discover users' identities.

Perhaps more important as a practical matter, the secrecy on which autocratic governments have relied in order to avoid violence and retain control has clearly eroded. Much more is known by their publics and at much lower costs. The old *samizdat* dependence on ragged mimeographed, photocopied, or even printed sheets of soon-tattered papers surreptitiously passed from person to person has been replaced by cellphones, instant messages, twitters, and the Internet. More people know what fewer once suspected no matter how great the control of the government. And as the "color revolutions" in Eastern Europe pioneered and the recent revolutions in Northern Africa have advanced, social networking has introduced much enhanced tools for organization in all settings, but with especially important effects in autocratic regimes. There, while social media certainly do not equalize organizational strength, they reduce the dramatic disparity between the government and its critics. With a Google executive in the spotlight on Facebook, the Internet, and short message service (texting) (SMS), Egypt last January is the most obvious illustration but hardly the only one, especially in the Arab world. Dissident Shiites are using social networking sites to organize protests in Bahrain (and, in the process, challenging their traditional spokesmen in the more compromising and participating Al Wefaq). The new media have been instrumental as well in arousing Sunnis in Lebanon, anti-Khadaffi forces in Libya, and apparently almost everyone in Tunisia.

But the authoritarian or semiauthoritarian context is only the most obvious case. Relations between the United States and nonautocratic states, indeed traditional diplomacy and assistance, have also been affected by the 24/7, instantaneous new information environment. Sometimes it has improved relations. Humanitarian disasters, for example, like the earthquakes and tsunamis in Indonesia or Japan (then compounded by the meltdown of the Fukushima reactors) or the floods in Pakistan were instantaneously on personal computer and cellphone screens as well as television. No presidential or prime ministerial explanations of what had happened, of the widespread devastation and death, or of the continuing disasters were necessary to galvanize public support for relief efforts. The scramble at State and USAID is now more frequently to keep ahead of reports about disease, corruption, and coups, and their implications for the United States. The clamor for action, often generated by nongovernmental organizations (NGOs) backed by news reports or documentaries, prompts spokespersons to discuss the complexity of relations and "the need for balance and patience" as against justifications for engagement as in the past. Cooling things down may now be at least as common as revving them up.

Similarly, conflicts and civil wars in what earlier were exotic, even unknown, places have become common subjects in the media, often first in the new media and then in the more traditional ones. How much attention would an isolated place like Darfur have received two decades ago; how sustained would the isolated story have been; and who would have cared? In that respect, Darfur is the story of the social media and celebrity advocacy driving traditional diplomacy or at the least keeping the diplomatic cauldron hot and far more central than it would otherwise have been. The story is similar, though less central (perhaps precisely because less prominent) in Chechnya, the Kivus, Tibet, Xinjiang, and Rohingya (How many people ever knew or ever heard of the Rohingya, let alone about their treatment within Burma?). These are otherwise perhaps unnoticed (and *therefore* inconsequential) conflicts now at center-stage as a direct result of exposure through the efforts of blogs and instant messages. Iraq and Afghanistan have been covered in multiple and more complex ways for the same reasons: blogs, amateur journalists, and messages from the combatants themselves.

Beyond just raising awareness of these various conflicts, the new media and the new information environment have provided sustained, if sometimes sporadic, coverage and analysis of the conflict dynamics, the successes and failures of their various adversaries, the attempts to reach some accommodations, and the possible shape of resolutions. Unlike conflicts involving the major powers (like Iraq, Afghanistan, and even Colombia), the major media cannot sustain coverage of the (unfortunately) dozens of "minor" conflicts. But because the actual production costs of the new media are so marginal and the costs of entry are so low, a small but committed cadre of "citizen journalists"—itself a new development within the media—and a devoted readership can sustain some coverage of even highly localized conflicts, like Chechnya, the Kivus, and the Rohingya. Moreover, that coverage spills over into the major media channels from time to time and, partly for that reason, keeps these conflicts on the diplomatic and assistance agendas where they otherwise probably would not have been.

Still, multiple, complicated, and interwoven factors and interests do not fit neatly into tweets of 140 characters. But the globalization of interests, relations, contexts, information, opinion, and advocacy has created a much more sophisticated public of quasi-Metternichians, even at bars, picnics, and school meetings. High school students in Iowa or Nevada have "friended" their equivalents in Paraguay, Malawi, and Bangladesh. A campaign debate on the better course as between confrontation and force on the one side and diplomacy and sanctions on the other to entice nuclear reductions in Iran would probably not have had much staying power half a century ago when President Kennedy and President Nixon squared off in the first televised presidential debate, nor would the intricate dynamics within the present Israeli cabinet about a first strike on Iran. The complexities exposed by the new information and opinion environment have definitely complicated but also enriched and exposed the work of diplomacy and development, especially for a democracy in which both ultimately depend on public support.

Beyond merely creating the context and beyond the potential transformation of governments, the new media affect the normal course and conduct of traditional diplomacy. They have the power to expose facts to which diplomacy is obligated to respond. The Wikileaks cables are the most obvious example. Albeit the result of a theft of clearly classified materials by an army private with security clearance and unaccountably broad access to material he had no need to know, it did more to embarrass the United States and its officials than actually to expose serious secrets. The publishers of the leaks were immune from prosecution under the first amendments, but the actions of those who stole the material and who made it available were not. Still, at least in this case, the leaks exposed nothing not already known or well suspected. They did expose candid assessments and gossip better left private, at least from the perspective of good relations, decent etiquette, and (most important) future access. Even in common parlance, diplomacy carries the connotation of tact and discretion, hence the idea of "being diplomatic" even in everyday social settings. Not everything that is known, believed, or suspected needs to be said out loud and certainly not publicly. Ordinary human intercourse, and certainly official diplomacy, depends on the opposite: not being public about it is better left private, that so-and-so has deteriorated physically or mentally, or has had an affair, or has made unfavorable or embarrassing comments. As Molière's Alceste came to understand, always telling the truth may be what parents initially instruct their children, but as those children grow, they also learn what "white lies" to tell and what to keep to themselves: "My goodness, you're ugly."

Similar but more graphic than the Wikileaks cables were the various photos from Iraq and Afghanistan that were initially sent to specific recipients but then "went viral," and with striking consequences: The photos of naked Iraqi prisoners, especially the pyramid, from Abu Ghraib; the four marines urinating on the bodies of dead Taliban; and the photos of Korans (admittedly desecrated by the Taliban with secret messages) incinerated with garbage rather than turned over to the Afghans or destroyed in a religiously appropriate way. The photos and reports from Afghanistan, which in previous times would have been confiscated before they were published or which some discreet editor or publisher might have embargoed for a period, at the very least disturbed negotiations between the coalition forces, the government of Afghanistan, and the Taliban. The Abu Ghraib photos ignited global revulsion and were instrumental in the closure of Abu Ghraib and, however independent, were cited to support allegations of torture at the Guantanamo Naval Base camp for "enemy combatants." The reaction by Afghans to the Koran burnings far exceeded their reactions to various reports about deaths of civilians during coalition night raids, affecting development projects as well as the no-longer-secret diplomatic negotiations in the Gulf. At the very least, these exposures increased the volatility of the negotiations and the immediate tactical postures of the parties.

Moreover, quite apart from legal liability (which was clearly unlikely), the Wikileaks cables and the viral photos created for the *mainstream* media dilemmas similar to but much less consequential than the publication of the Pentagon Papers during the Vietnam War controversies. What should be published? What should be withheld? What should be delayed? What material should be redacted? Who would be hurt? Who would be "victimized"? How engaged were they? How "innocent"? And so forth.

But those dilemmas were clearly absent from the social media precisely because of their anonymity and individuality and the inability to control them. Cellphones with cameras are everywhere, capturing everything, profound and prosaic alike. Anyone with a cellphone is a photojournalist; anyone with Twitter is a commentator. No editor or publisher second-guesses the wisdom of exposure. Everyone with access has the ability to publish. As a result, everything that can be broadcast almost certainly will be. There is no filter. Everything is transparent. There is therefore only downside for a mainstream publisher to exercise discretion and withhold information that will surely be viral anyway.

For governments, particularly democratic governments, such transparency has dual effects. It illuminates without favoritism. It clarifies those aspects of diplomacy and development that most evidence positive intentions. But it also clarifies those aspects that are not so positive, for example the so-called "dark arts" of intelligence and covert operations. More commonly, though, it merely exposes analyses, information, policies, contacts, and compromises that are sensitive or embarrassing. If diplomacy is the art of advancing national interests, in part through representation and agreements with counterparts (adversaries as well as partners), those agreements are likely to encode common ground and reduce differences, which often means some kind of compromise. Reaching those agreements and compromises most often requires quiet, private conversations and negotiations in which policies and possible options are surveyed and hypothetical positions are explored, all without commitments. When complete commonality cannot be reached, they sometimes intentionally include what Henry Kissenger has called "constructive ambiguity." No matter the result, the difference between a going-in and a coming-out position often gives rise to accusations of hypocrisy, especially when core principles, not just minor details, are seen to be compromised. Deviating from hard official lines or initial principles, especially through testing alternative compromises, is rendered more difficult by fear of exposure. Transparency and exposure, and the fear of both, make all of that more difficult. So, the negotiation process, with its inherent give-and-take and its ultimate requirement for some degree of compromise, can be impeded, not aided, by transparency.

Apart from the difficulty of negotiations themselves, the increased transparency and volatility created by the new media have rendered planning and long-term strategy for even ordinary diplomatic relations more risky than before, precisely because the uncertainties have grown. No one knows where or when the next shoe will drop or what it will be. In addition to the origin of change, the new media have also increased the volatility of change.

So what are the consequences? Not all are deleterious. Perhaps the propensity of governments to overclassify will be reconsidered. The smaller the amount of material that truly needs to be kept secret, the greater the ability to protect it. First, it is simply not possible to protect the enormous amount of material classified by the U.S. government, and quite a bit is classified primarily because it would be inconvenient if it were public. Much of the material carries no real national security stake. Second, too many indiscretions are passed through cables, indiscretions that are not really fundamental, some not even germane, to foreign policy. The temptation by embassies to display their access and (presumably) value back to the capitol is matched by the temptation of recipients there to relish knowing the hidden intricacies and intimacies (personal and political) of their foreign counterparts. The mainstream press makes public much of what is really important for policy and, as noted, very little of what passes for secret will not be well-known in the near future. But precisely because of its value as gossip or, on occasion, because of its real, useful insight, cables passing on rumor and fact not (yet) public about counterparts (especially adversaries), their motives, their weaknesses, and the like will surely continue. Their exposure will embarrass the protagonists and sometimes neuter potential allies.

Unfortunately, some disclosures will also spoil useful diplomatic initiatives that might have contributed to solutions by exposing them before they are ripe or by exposing the quiet willingness to negotiate, even to make important concessions, of a protagonist who has taken a hard public line to the contrary. Certainly, some revelations scuttle the possibility of compromise and conciliation. All of that is more likely with the increased transparency of the new media. These media are more individual, less institutional—one or a few people with a camera and a computer—in which there are no real standards of probity or ethics and in which there are, therefore, few peer or organizational pressures or mature supervision over content.

Take perhaps the most transformative diplomatic initiative of the last half century: the establishment of diplomatic relations between the People's Republic of China and the United States. The clandestine negotiations in furtive trips abroad by then-National Security Advisor Henry Kissinger were necessarily cloaked in secrecy. Surely the discussions would have been aborted once they became public and long before they ripened into agreement. The arch-champion of anticommunism, President Nixon, would have been unmasked by some blog, text message, or Twitter exposing the trips, their purpose, and their facades. Whether for better or worse, once public, the exposure and their effects on U.S. commitments to Taiwan, in fact on the international legal standing of Taiwan, could well have scuttled the diplomatic effort in its fragile infancy, as those opposed to normalization of relations would almost surely have organized a blocking constituency. The chances of such an unmasking would have been much higher and the risks much greater in the age of the new media, when any worker with a cellphone and some "friends" could have had global, viral access.

The most recent illustration of the extent to which increased transparency and accompanying volatility poses problems for diplomacy is the Chen Guangchen incident in China. Briefly, a little over a week before the annual China-U.S. Strategic and Economic Dialogue meeting in Beijing between the two respective foreign and finance ministers, blind human rights activist Chen Guangchen managed to elude the security guards enforcing his house arrest in Shandong Province, then (inexplicably) managed through a chain of human rights activists to be driven to Beijing and (even more incredibly) to scale the wall of the U.S. embassy to ask for protection, notwithstanding a foot injury sustained when he climbed over his house fence. U.S. diplomats, including of course the secretary of State herself, were clearly caught between the impulse to protect Chen; find a solution to his presence in the embassy; and continue with the issues, apart from human rights and democracy, the dialogue was designed to address. Two decades ago, news of the incident would have been carried on television and in the newspapers, but certainly hours, probably even a day, later. The new media created instantaneous and global coverage without any time for diplomatic exchanges to fashion a diplomatic strategy by either side, let alone quiet consultations between the two countries. After a set of missteps, embarrassing to all sides, in which Chen left the embassy; was admitted to a hospital for his injured foot; was kept apart from his wife and family; changed his mind about forgoing his asylum request; and heard about Chinese government harassment, even reputed torture, of his friends and family, the final face-saving solution emerged. He would be allowed by the government to apply for a visa to study abroad "the same as any Chinese citizen" since, he said, he was only asking for the rights of any Chinese citizen all along. The solution was fashioned in the full and constant glare of instant messages, photojournalists, blogs, Twitter, Facebook, and YouTube. There was neither the normal time nor political space for the sensitivity of crafting a solution that would satisfy the needs of all the parties. As important, the key State officials were distracted from the issues and agenda of the dialogue by the need to negotiate a solution for Chen.

For development, the consequences of transparency and volatility are in general lower than for diplomacy but still evident. True, there is less to hide, less need for secrecy. Development activities have long been overt. Indeed, development agencies are perhaps overanxious to publicize their efforts and unfortunately probably too anxious to claim undue credit for their impacts. Certainly in the United States, the tendency is to "brand" too much so that the foreign recipients will be appropriately appreciative for everything that has been (to use USAID's version of branding) "brought by the American people" under the USAID logo.

Still, there are elements of every assistance program that both host governments and donors would prefer to remain nonpublic. Perhaps most obvious is the extent of corruption, particularly the participation of host-country public officials in it, and its effects even on assistance funds. To take some obvious examples, corruption by high-ranking host government officials in the chain of pharmaceuticals and medical devices is well-known, but donors prefer to keep the information quiet and absorb the losses in deference to serving the health needs of the large number of poor recipients. More outrageous is the provision of budget or other financial support by bilateral and multilateral donors to countries whose officials are engaged in illicit financial transactions, drug trafficking, corruption in the sale of natural resources, and other similar transgressions. In effect, the taxpayers of the donor counties are subsidizing those crimes and doing so in countries that would not be quite so poor if their national assets were not being stolen. When called to account for their complicity, many donors retreat behind the insipid slogan: "Let's not hurt the poor twice, first by the corruption and second by a consequent withdrawal of aid."

To take another example, probably most assistance is not—as advertised—politically neutral. Incumbents are generally aided. They can point to goods, services, and projects that made life better for their constituents. To the extent that every government benefits from the provision of a better life for its constituents, it can point to the benefits it has brought (admittedly through donors, but not usually publicly acknowledged by the local authorities). While the government makes or encourages daily news clips documenting specific (often donor-funded) development projects—a new school, water purification facility, electric power plant—its formal political opposition is left with mostly theoretical critiques. Moreover, domestic providers (often clients of government officials) are aided concretely, and too many make their appreciation known to their patrons in inappropriate ways.

Perhaps more pointed are some of the economic growth and democracy projects. Privatization is often seen by local residents as the transfer of public goods to politically connected cronies at prices well below what a market sale would produce. Insider privatizations reinforce, sometimes create, crony capitalism with a small, politically created, very wealthy economic elite. And some privatizations are indeed exactly that. Yet the underlying economics are often more complicated. Most publics believe that public capital goods (factories, equipment, transportation networks) are far more valuable than investors are prepared to pay even in a public and completely honest bidding process. Investor valuations depend on market returns; public valuations are often based on costs already incurred rather than future profits and therefore market value. Social media, inherently shorthand and idiosyncratic, are much more likely to emphasize simplistic rather than complex accounts and conclusions. Naturally, they pay disproportionate attention to the successful as against the unsuccessful investors.

Likewise, donor-provided political party building programs, even when officially available to all parties committed to the democratic process, disproportionately benefit the smaller parties and the opposition parties. The lager parties, especially those that have formed the government, do not need them, indeed prefer to keep their party strategies quiet and internal. In many countries, the participants in social media are likely to be oppositionists, so perhaps they are less likely to dwell on the disparities of benefits. But democracy proponents and their donor benefactors also prefer quiet discretion to public transparency. Assistance to democracy advocates has long been tolerated so long as it has been minor compared to the larger amounts for food, health, education, the environment, and even economic reform . . . and so long as it has been relatively quiet. Without publicity, each government in the bilateral relation could maintain its position: on the U.S. side that it was supporting democracy and reform and on the recipient side that the support was insignificant, not worth a rupture in relations. Greater transparency emboldens reformers, but the higher profile also increases the risk of disputes.

Embassies are called upon to defend these programs, indeed not just the programs themselves but also their U.S. and domestic implementers. For example, when the Supreme Command of the Armed Forces government in Egypt detained and charged the U.S. and Egyptian staffs of six U.S. NGOs (including the National Democratic Institute, the International Republican Institute, and Freedom House) that were fielding programs in Egypt while waiting for ministerial approval of their registrations—which they had done for years under the Hosni Mubarak government—the embassy, the Department of State, and the secretary of State were required to intervene. The U.S. government posted the $5 million bond required for their release pending trial. The U.S. citizens all returned to the United States. All of this, including the (in previous times, discrete) negotiations, were carried day-by-day on TV, blogs, and instant messages.

Unlike in real diplomacy, the main donors and recipients have adopted a set of principles, the *Paris Declaration on Aid Effectiveness*, in which they pledged not merely transparency but partnership in providing assistance. The donors have committed to harmonize their respective programs and, going further, align them with the development plans of the recipient countries that presumably developed and "owned" them; both donors and recipients agreed to mutual accountability and to manage for results. The underlying paradigm is partnership and participation. Much of the Paris Declaration is ill advised or unworkable in countries that suffer from authoritarianism; major conflict; poor policies; or high levels of corruption, nepotism, and cronyism. But in countries benefitting from good development policies and implementation, the Paris principles can produce country ownership, reduction of redundancy, and true partnerships. In those countries, transparency is already high, since the donor and recipient partners are supposedly already in alignment. The mantra of participation, ownership, and alignment means broader accountability to the host country, both to government officials and to the public. At least in theory, every project, grant, contract, and expenditure is known mutually, can or should be publicly posted, and ought to be monitored by both donor and recipient governments and their respective publics. In an environment of transparency, the new media have little to expose, although perhaps much on which to comment, and they provide additional mechanisms of transparency. Still, there are sensitivities: Who got the funds, and how much did they get? For what purposes? How was the money really spent? and the like. Of course, that is precisely the level of transparency that is anathema to authoritarian regimes with high levels of corruption, nepotism, and cronyism.

SUMMARY

The social media are now an inherent part of the diplomatic and developmental landscape. For better or worse, there is no going back, no returning to the status quo ante. The transparency that both reflects and creates volatility is also embedded in our current environment. What is gained, and what is lost? And, more important, how will statesmen deal with them?

No doubt the pace of change has quickened, and in part because of the new media environment. The recent events in Tunisia, Egypt, and Libya transformed a region long requiring an explanation for its stability and stagnation into one that makes the transformative events in parts of Central Europe two decades ago seem almost slow by comparison. Their conclusion is another matter, perhaps not as felicitous, but it would be hard to imagine them in the absence of blogs, Twitters, email, and cellphone text messaging. For similar reasons, it would be hard to imagine Al Qaeda and its many imitators, including web-based instructions for constructing and delivering weapons of terrorism, without the new media. The new media offer anonymity; the ability to create virtual organizations and communities but with real consequences; and the capacity to organize activity even among colleagues who have never met and cannot know one another's identity for fear of reprisals. The new media and, to some extent, the new forms of traditional media (for example, cable and satellite television sometimes originating beyond the borders of a country) can create virtual communities, but they can also fracture real, existing, but fragile ones, as in Pakistan, for example.

Meanwhile, the authorities in some countries search for countertechnologies that will pierce the anonymity, send false instructions, confuse the adversaries, foil (even subvert) their plans, expose their members, and capture them.

At a more prosaic level, the new media have made it harder for the United States and its allies to support problematic governments discreetly in order to gain favors, pursue common goals, or at least to find limited common ground. They have made it harder precisely because they create transparency even when and where fog can sometimes be useful, perhaps necessary, to practical achievements. The tension between public statements and practical realities, which have traditionally lent diplomacy an aura of stealthy deals and shady hypocrisy, will grow. So too will the dissonance between diplomacy and certain parts of development. The new media can complicate work in conflict environments, especially when diplomats are forced to negotiate with and perhaps even provide compensatory assistance incentives to distasteful combatants who kill, maim, and rape while they also hold some part of the keys to peace. It will be harder as well for diplomats to work with autocratic or even authoritarian governments while their developmental partners have programs designed to weaken the hold those government officials have on state-owned enterprises, rents from corruption and nepotism, or political and economic monopolies. Diplomats will be asked to defend precisely the developmental programs designed to undermine their counterparts' political and economic power. That tension may not be new. But its exposure by individuals or groups, sometimes anonymously, has expanded dramatically.

ENDNOTES

1. Among the others are accounts for the Andean Counterdrug Program (ACP); Child Survival (CSH); Foreign Military Financing (FMF); Global HIV/AIDS Initiative (GHAI); International Military Education and Training (IMET); International Narcotics Control and

Law Enforcement (INCLE); Migration and Refugee Assistance (MRA); Nonproliferation, Anti-Terrorism, Demining and Related Programs (NADR); Peacekeeping Operations (PKO); and P.L. 480 (food aid). No doubt, the assistance provided from these accounts contributes in some way to development, but only for the special purposes clearly identified by the titles of the accounts.

2. In recent years, State has become much more active in determining the details of the assistance programs in the countries it identifies, not just the policies and overall budget levels. Post–Cold War, more latitude for policy beyond gaining and assembling allies, punishing adversaries, and containing the Soviet Union increased State's bargaining leverage in discussions with recipient countries and, without the fixation on the Soviet Union—who was gaining and who was losing—perhaps consequently increased the engagement by State in the details of their programs.

3. Without gainsaying a basic interest by State and its Foreign Service officers in development, diplomats consider assistance a resource available to achieve diplomatic objectives. These are concrete incentives accessible to add heft and tangibility to its diplomacy. For that reason, the diplomatic part of the embassy will always try to influence assistance flows to individuals and institutions it would like to bring along to the U.S. side. And for exactly that reason, the favorite assistance element, albeit usually by far the smallest amount, is the flexible "ambassador's fund," which allows the ambassador to provide small but very public assistance to projects of high visibility (ribbon cutting) or to domestic actors the ambassador wants to influence. These funds may even have a developmental impact and may be put forward as "developmental," but development is often not really their primary purpose.

4. Of course, the wars in Iraq and Afghanistan led to the even broader integration of the "three D's" (defense, diplomacy, and development) in the National Security Strategy of 2002; the National Security Strategy of 2006; and, in a slightly more diluted way, in the National Security Strategy of 2010.

5. That assumes the military and State officers make good decisions about the development or "build" dimension or at least that their decisions are as good as the development officers. There are ample examples that suggest the assumption is questionable, especially when the PRT commander has more money than good projects, spends the funds in ways that enhance corruption, and inevitably strengthens certain factions at the relative expense of others and that achieve at best short-term gains, and also when the lessons of one company or brigade are not passed along to the successors. Of course, the record of "development experts," especially in areas of conflict, is itself questionable. However, counterinsurgency is the exception to the normal Defense, State, and USAID relations as contemplated in the various national security strategies and in the QDDR, and too much should not be made of the many anomalies in a counterinsurgency environment.

6. For some period in Afghanistan, the entire military and civilian effort was designed explicitly "to enhance the legitimacy and reach of the Government of Afghanistan," although it became increasingly clear, as it should have been initially, that no international effort could possibly establish the legitimacy of the government of Afghanistan, especially given the levels of corruption and ineffectiveness of the cliques of Kabul.

7. Department of State, "Preventing and Responding to Crisis and Conflict", in *Leading Through Civilian Power: the First Quadrennial Diplomacy and Development Review, 2010* (Washington, DC: 2010). http://www.state.gov/documents/organization/153635.pdf

8. Section 1207 of the National Defense Authorization Act for Fiscal Year 2006 (P.L. 109-163) provided authority for the Department of Defense to "transfer to the State Department up to $100 million in defense articles, services, training or other support for reconstruction, stabilization, and security activities in foreign countries." http://fpc.state.gov/documents/organization/104687.pdf. That authority was renewed in subsequent years albeit with some concern in Congress that such funds should properly be appropriated directly, if at all, not routinely through the Department of Defense.

9. Times may not to have changed so radically after all: "BAMAKO, Mali—Gunfire rang out over this West African capital Monday night as soldiers loyal to the president [Amadou Toumani Touré] who was deposed in a coup in March, appeared to be attempting a countercoup against the ruling military junta. But by early Tuesday morning the junta aired a message on state television saying that it controlled the positions that had been under attack, including the state broadcaster, the city's international airport and a military base in Kati, the garrison village at the edge of Bamako where the military junta and its troops are based, Reuters reported." *New York Times*, "Loyalists of Mali's Overthrown Leader Appear to Be Attempting Countercoup," May 1, 2012. http://www.nytimes.com/2012/05/01/world/africa/mali-soldiers-appear-to-have-countercoup-as-goal.html?_r=1&ref=world.

10. Indeed, the proliferation of television broadcast via cable and by satellite—perhaps not new media per se but rather an old medium provided in a new way—has also transformed the monopoly of news, information, and analysis. Even when a government forbids satellite dishes, they are smuggled in and erected inside people's homes rather than on rooftops where the security forces can easily see them. One consequence of the proliferation of programming and stations originating from abroad is the splintering of the audience, for example by language, religion, or ethnicity. Rather than a few stations broadcasting a fairly common narrative in a common "national" language, each "community" has access to, and can in a sense create, its own media environment, including its own vernacular.

In many ways accommodating to diverse tastes and interests, such stations can also feed isolation and distortion. The viewers are more likely to share common attitudes and be impervious to alternative views and facts, reinforced by like-minded broadcasters who derive their audience and revenues precisely by appealing to their viewers' predispositions and preconceptions. In the extreme, these media can easily stoke division, conflict, and violence, as did some of the registered, in-country radio stations in Rwanda. The difference is that, unlike Rwanda, the external stations do not need government complicity, at least not from the government of the country into which they broadcast.

11. Recent cases exemplify the acceleration of information and the commensurate ability to organize. Beyond the Middle East, the "Red Shirt" opposition in Thailand brought down the government and nearly caused a constitutional crisis. China experiences hundreds of demonstrations almost daily. Awareness of the disparities of income between regions and classes, the spread of knowledge and analysis, and the much wider dissemination of information, all accelerated by the new media, have increased protests around the world. Ironically, improved standards of living, which are responsible for the improved access to the media, have often resulted in more, not less, social protest.

Transparency in Aid Programs

Andrew Puddephatt

1. AID TRANSPARENCY: INTRODUCTION

The policy focus upon transparency has become widespread in recent years and is far from limited to the realm of aid. Indeed, it has become a centerpiece of debates about governance. The growth of ubiquitous digital communications has enabled both the supply of and demand for information.[1] Developments in technology have led to easier access to information and, as a consequence, have raised public expectations about the transparency and accountability of government activities. While expectations about the impact of digital communications are high, the evidence of their impact is still sketchy and unproven. Whether digital technologies make aid more effective is a proposition yet to be tested.

The effectiveness of aid has long been the center of debate. Advocates such as Jeffrey Sachs continue to promote the benefits of aid giving, while sceptics such as William Easterly and Dambisa Moyo scrutinize its ability to truly affect developing countries. Yet an emerging concern for both advocates and sceptics alike is the manner in which aid programs are delivered. It is no longer acceptable for donors simply to give aid; there is now a call for delivery of aid to be accountable and, above all, transparent. This is driven by the belief that transparency will empower those in receipt of aid and reduce the risks of corruption or misuse of resources, thereby ultimately improving the quality of development.

This paper explores these existing initiatives designed to promote transparency with a particular interest in civil society involvement. The normative assumptions that lie behind these initiatives assume that transparency itself will increase the effectiveness of aid by empowering civil society organizations (CSOs) to monitor aid, by acting as a disincentive to corruption, and by ensuring broader public awareness of aid flows. The relative success of country-level, CSO-led initiatives as compared to initiatives on the international level will be examined. The vast range in the nature of initiatives and their relatively recent genesis does mean, however, that an assessment of their impact is difficult.

A counterthesis will also be examined, one that points to an unwillingness among donors and implementers to be transparent about the impact of their work through fear of a taxpayers' revolt and an undermining of the multilateral aid industry if the programs are perceived to have failed. The paper will offer an analysis of possible future strategies toward aid delivery that would embrace a risk-taking approach founded on the notion of aid as an "investment."

During the Cold War, aid was shaped by the geopolitical rivalry between the United States and its allies and the Soviet Union and in its latter stages saw the emergence of structural adjustment programs. The end of this confrontation changed the focus of aid more toward the alleviation of poverty, which led, in time, to increasing concern about the impact of aid on recipient countries. During the 1990s, the international aid effectiveness movement began to take shape. There was a growing realization among donor governments and aid agencies that the diverging and frequently conflicting approaches toward aid giving were imposing huge costs on developing countries and making aid less effective. This led to a desire to coordinate development.

However, only in the past decade has there been any significant effort to make aid effective. There has been increasing concern that aid has not been producing the development results expected. There was a need to understand why this was the case and to increase efforts to meet the ambitious targets set by the Millennium Development Goals.[2] The international development community has become preoccupied with the need to make aid more effective, and efforts to coordinate a new approach have been focused on four major international events: the High Level Fora on Aid Effectiveness in Rome, Paris, Accra, and Busan in 2003, 2005, 2008, and 2011, respectively.[3] Through these events, the demand for greater transparency has become more marked.

The *Accra Agenda for Action* (prepared in 2008) claimed that greater transparency and accountability for aid—domestic as well as external—was a concrete step toward more effective aid. In Accra, the signatories made the following significant commitment: "We will make aid more transparent. Developing countries will facilitate parliamentary oversight by implementing greater transparency in public financial management, including public disclosure of revenues, budgets, expenditures, procurements and audits. Donors will publicly disclose regular, detailed and timely information on volume, allocation and, when available, results of development expenditure to enable more accurate budget, accounting and audit by developing countries."[4] This commitment was cemented in Busan in 2011 with the preparation of the Busan Partnership for Effective Development Cooperation which outlines important developments for aid transparency.[5]

However, the most recent critical factor in pressing for transparency in aid programs has been the global financial crisis, particularly that facing the United States and Europe. The need for tighter budgets has led to a resurgence of commitment to financial aid transparency in all areas and a greater focus on the effectiveness of spending.[6]

This push for transparency in aid programs has spawned a range of initiatives such as the International Aid Transparency Initiative (IATI), established in 2008 following the Third High Level-Forum on Aid Effectiveness in Accra. IATI is a voluntary, multistakeholder initiative that includes donors, partner countries, and civil society organizations and that sets a standard for guidelines for publishing information about aid spending. IATI builds on the work already achieved by intergovernmental initiatives like the Organization for Economic Cooperation and Development (OECD) Development Assistance Committee, which produces statistics about past aid flows and aid activities to encourage greater transparency. Further initiatives include civil society coalitions like Make Aid Transparent or the global campaigners for aid transparency, Publish What You Fund.

Transparency in aid programs is a relatively recent development and, as such, measuring the impact of transparency on aid effectiveness is still very much in its early stages, and evidence is sparse. The general hypothesis is that improving budget transparency is not only an important goal in itself but also that it would achieve better development outcomes for people, or human development.

However, it is too early to assess whether, or indeed *when*, this hypothesis will come to fruition.[7] Chains of causality between aid transparency, accountability, and development outcomes are long—so it may be a few years before the real impact of transparency can be assessed.

The case for transparency as a deterrent against the mismanagement of aid is strong. Poor coordination between donor governments and aid agencies, competing interests and priorities, and a lack of communication with partner countries leads to an ineffective delivery of aid. Clare Lockhart writes in *Prospect* magazine of $150 million in aid that should have gone toward reconstructing a village in Afghanistan and that ended up being squandered in administrative costs in various agencies in the United States and Switzerland.[8] Sadly, this is not an exceptional case. Just in the process of writing this paper, the author read a breaking news story of millions of dollars wasted in Afghan reconstruction projects.[9] Poor coordination between the U.S. Defense Department, the U.S. State Department, and the U.S. Agency for International Development (USAID) led to unrealistic cost estimates and inadequate planning.

Campaigners such as those from IATI have responded to revelations such as these with the claim that increased transparency in the aid process would help prevent such blatant misuse of aid. Publish What You Fund claims that the benefits of transparency include more effective allocation and management of aid by donors, better planning by recipient governments, increased accountability of donors and governments in the North and South, a reduced risk of corruption, and enhanced public participation.[10] Campaigners argue that the publication of relevant and accessible information, which is also timely and accurate, is the crucial element in ensuring aid effectiveness. The innumerable examples of malpractice in aid delivery point to the need for a more effective system where it is clear both to the donors and recipients exactly what purpose the aid is serving and to what it is being directed.

2. CIVIL SOCIETY INVOLVEMENT

Transparency in aid programs is crucial for maintaining public support for aid. Worldwide, celebrity-endorsed campaigns such as Make Poverty History and Live 8 saw public support for aid and development reach an all-time high. However, this support, as noted in a Publish What You Fund briefing paper, is unreliable while in aid recipient countries public faith in foreign aid remains low.[11] In the current, unstable economic climate, it is even more essential for citizens to have access to clear, accurate, and timely information about public expenditures on aid in order to maintain public support.

It is obvious that the lack of transparency in aid programs makes it much harder for civil society, both in donor and recipient countries, to hold governments accountable. For donors, transparency is necessary to allow citizens and taxpayers to understand how aid is being used and to see the vital role that aid plays in supporting progress on poverty alleviation in many developing countries. In order for implementation of aid to be carried out effectively on the ground, citizens of recipient governments must have access to greater levels of aid information to allow them to hold their governments to account over inconsistencies between aid received and aid spent on behalf of beneficiaries.[12]

There is much interest in whether digital technologies help foster greater accountability in aid—or even more demand for transparency and accountability. The empowering potential of digital communications—making access to interactive technologies widely available—would seem to offer the possibility that individuals can use technology to hold governments to account. One study[13] found that while there was some evidence that these tools could be deployed effectively, much depended upon whether technology platforms were tailored to local skills and capacities and whether technology reinforced the strategies of potential users. In fact, such studies as exist[14] show that it is not "mass" users such as citizens or consumers who make the most effective use of technology; rather, it is "organizational" interests such as journalists, nongovernmental organizations (NGOs), governments, and corporations.

This seems to result from the motives and incentives of potential users of the technology platform. For issues concerning public accountability, organizations have the incentives to acquire and act on information about corruption or budget misallocations and have the specific capabilities to use technology effectively.

Of particular relevance in the development context are systems that combine voice and data, allowing people to both file and access citizen journalism reports via mobile phones. Examples include CG-Net Swara in India and the FreedomFone system developed and used by the civil society organization Kubatana in Zimbabwe. People can contribute stories through dialling into a system to record their message in their mother tongue, and they also can listen to items posted by other people. News items and stories are stored and administered on a fixed line computer server, which is also used to send short message service (SMS) (texting) alerts to subscribers about new material. In addition to being available via the voice-operated system, stories are also available via the web and are distributed by email, from which they have been picked up by the mainstream media. With this system, even the poorest communities have some form of access to the information.

Digital technologies also permit crowdsourcing to harness the value of combined knowledge and ideas from geographically dispersed people. The mobile phone platform Ushahidi[15] is one of the most famous examples of how this can enhance the power and impact of crowdsourcing. This is a software platform that allows people to report incidents and events that they have seen or experienced relating to a specific issue. The software processes reports that it receives and logs them in a database. The database is linked to a map of the area in which incidents are occurring, allowing users to see how events are unfolding and to analyze geographical and temporal trends. The system allows people to log reports via a website, email, Twitter, SMS, or multimedia message service (MMS). It has been used extensively for a range of purposes, from tracking harassment of women in Egypt, to monitoring election violence in Kenya, to tracking water supplies in India. While the system has tremendous potential to monitor aid, there is, as yet, little development in this field. The most innovative uses of technology are focused upon domestic political or accountability issues. This underlines the fact that it is not the availability of technology that is crucial but the incentives to use technology to monitor aid, the appropriateness of the technology, and the skills and capacities of the users.

It is sometimes assumed that transparency fosters antagonism between the state and citizens, but a key enabler of CSO-driven aid transparency initiatives is active cooperation between the state and its citizens. The mutual benefits from such a collaboration are obvious. CSOs cannot access detailed information on aid spending without cooperation from the state, while state actors cannot justify aid transparency efforts in isolation from citizens and civil society accountability seekers.[16]

Civil society has been shown to play a crucial role in pressuring governments for increased accountability through greater transparency and access to information (ATI). The positive correlation between CSO involvement and improved ATI frameworks is discussed in the paper "Citizens and Service Delivery" by Dena Ringold. Countries with strong civil society institutions, such as India, Mexico, and Romania, appear to have more extensive ATI legislation because of the ability of civil society to "influence policy makers to draft effective laws" and to "create awareness among citizens about how to use ATI legislation."[17]

The involvement of civil society is shown to be equally effective in pressuring for transparency of aid policy and programs. A report by Sakiko Fukuda-Parr found that open budgeting, especially with citizen participation to help set budget priorities, can lead to resource allocations for development that result in positive human development and human rights outcomes. Participatory budget processes in Rio Grande do Sul, Brazil, for example, have lead to the consistent prioritization of key sectors such as urban infrastructure (roadways and water and sanitation), housing, and education and to rural needs such as transport and agriculture in state budgeting.[18] In the current financial climate, citizen *participation* in the processes of *public budgeting* and financial management is increasingly essential for promoting transparency and accountability.

In recent years, there has been a notable shift toward grassroots participation instead of a "trickle-down" process of social change. The demand for civil society participation can be traced back to the 1970s, but it has only more recently been picked up by the big, bilateral institutions. The inclusion of civil society participants at the Third High-Level Forum in Accra in 2008 was considered by many to be the hallmark of the event. Significant gains were made in recognizing the importance of CSOs as independent development actors and in the agreement to work together to address CSO effectiveness as a responsibility shared among CSOs, donors, and developing country governments (though civil society groups argued that power remained with the donors).[19] Only through civil society putting pressure on donors can effective aid transparency come about. In Canada, for example, it was only through pressure from Canadian NGO Engineers without Borders that the Canadian government agreed to join IATI.[20]

Various civil society initiatives now operate at the international level in order to coordinate their efforts to hold donors to account. Civil society coalitions like Make Aid Transparent have been established in order to pressure donors into providing transparent information regarding their aid delivery. The Reality of Aid network is noted for being a southern-led North/South group that includes more than forty civil society regional and global networks and works to reform the practice of aid. Similarly, Better Aid brings together more than seven hundred development organizations from civil society in order to challenge the aid effectiveness agenda.

This is just a sample of CSO-led initiatives that have been established in recent years to pressure donors for increased transparency and accountability. They have amassed wide support (Make Aid Transparent, for example, has over seventy signatories and sixty-four thousand public signatures). However, it is difficult at this stage to assess the extent to which these initiatives have genuinely affected aid policy and practice. Although the organizations go into great detail on their websites about their various arguments and claims for transparency and accountability, there is little to indicate exactly how they aim to ensure donors' commit to transparency.

Furthermore, the sample above is taken from a wide range of civil society schemes that look to hold *donors* accountable; however, there are relatively fewer CSOs that focus exclusively on the transparency and accountability of aid in the *recipient* countries. This disparity between "supply" and "demand" initiatives is noted by Sarah Mulley, who describes initiatives on the "demand side" of accountability and transparency as "fragmented and patchy."[21]

That said, there are examples of country-level civil society initiatives that have been successful in holding their governments to account, some, one may argue, demonstrating more concrete effect than their international initiative equivalents.

India and RTI

India has had a degree of success with its country-level initiatives that push for in-country transparency in public governance and aid expenditure. For example, Mazdoor Kisan Shakti Sangathan (MKSS) is a people's organization and part of the growing, nonparty political process in India:[22]

> The MKSS spearheaded the right to information movement in Rajasthan which eventually extended to the rest of India. MKSS used the RTI [Right to Information] as [a] tool to draw attention to the underpayment of daily wage earners and farmers on government projects, and more generally, to expose corruption in government expenditure. Initially, MKSS lobbied government to obtain information such as employment and payment records, and bills and vouchers relating to purchase and transportation of materials. This information was then crosschecked at Jan Sunwais (public hearings) against testimonies of workers. The public hearings were very successful in drawing attention to corruption in the system. They were particularly significant because of their use of hard documentary evidence to support the claims of villagers.[23]

The MKSS website shows a very effective video documentary of the MKSS's campaign for RTI, which portrays how the poor of India are deprived of their social benefits due to corrupt government officials.

The particular success of this local campaign as opposed to international CSO initiatives could be attributed to the following factors. The organization of MKSS is entirely local, of genesis in Rajasthan, and focused exclusively on the rights of the Indian people. Even more crucially, MKSS is an organization that has built widespread mass support rather than relying upon a small number of professionals. It is a grassroots movement that includes local peasants and workers who directly benefit from the work of the organization. There is a somewhat "Maoist" ideological commitment in the MKSS to try to "match the lifestyle and work ethics with the community to which it belongs."[24]

Since its formation, MKSS has thus spurred community mobilization not only across the state of Rajasthan but also nationwide. This mass support, alongside the regular public hearings, has led to increasing pressure on government officials to clean up their act. Through the perseverance of the MKSS campaign, the Rajasthan Right to Information Act was eventually passed in 2000, followed by the nationwide Right to Information Act in 2005.

A further RTI campaign in India that has had considerable success is the National Campaign for People's Right to Information (NCPRI), which works in conjunction with MKSS. NCPRI activities include organizing National RTI conventions and establishing public campaigns for a more transparent prelegislative process.[25] Shekhar Singh, founder of NCPRI, has outlined the size of the Freedom of Information movement, with around eight million applications each year. A freedom of information system helps improve the quality of government by committing to the release of information that should be provided anyway. It also increases the efficiency of bureaucracy and acts as a deterrent against corruption.

Attesting to the positive impact of the freedom of information movement in India, a Yale University study found that it was almost as effective as bribes, with the particularly interesting finding that the movement works for poor as well as rich (unlike bribes).[26] The study involved slumdwellers in Delhi who wanted to apply for ration cards. They were randomly assigned to one of four experimental groups: One of the groups paid a bribe after putting in the application, while the other group made an RTI request in order to inquire about the status of their ration card. Although the group that applied with the bribe received their ration card in the quickest time, the group that put in an RTI request was almost as successful. Leonid Peisakhin conducted an extension of this study and found that RTI requests helped underprivileged applicants get results almost as fast as did the middle class. He concluded that access to information appears to empower the poor to the point where they receive almost the same treatment as middle-class individuals at the hands of civil servants.[27]

Needless to say, despite the incontestable achievements of MKSS and NCPRI and the findings of the Yale study, there are still many unresolved issues regarding India and RTI. Indeed, RTI activists in India have been exposed to brutal attacks and even murdered for seeking information to "promote transparency and accountability in the working of every public authority" in India.[28] The RTI Act of 2005 holds no protection for the activists. Since 2010 alone, twelve activists have been murdered. The assaults on activists point to the continuing, deep-seated problems with corruption and the refusal of officials to be held accountable.

There are other examples of improvements in domestic service delivery through applying transparency. The Huduma project aims to improve service delivery in Kenya using a crowdsourcing model. The project—developed by the Social Development Network and the Kenya African Treatment Access Movement and launched in February 2011—is a platform that allows citizens to report specific problems they encounter related to service delivery (for example, a lack of access to a certain medicine) through their phone. Each report is verified and sent to the relevant authorities in the private or public sector who in theory should solve the problem and inform Huduma.[29]

In Uganda, corruption in the education sector was reduced significantly through a combination of transparency initiatives and governance reforms in the education sector. In the early 1990s, there were substantial "leakages" of funds from the system of capitation grants—grants of money allocated to schools based on the number of eligible pupils. Between 1990 and 1995, a public expenditure tracking survey was done by the World Bank. Calculations from this revealed that only 12.6 percent of centrally allocated capitation funds for schools were actually reaching the schools. And many schools did not receive their capitation entitlements at all, with parents and teachers in many cases unaware of the existence of the capitation grant. A follow-up public expenditure tracking survey for 2001, however, revealed a dramatic increase in the proportion of capitation grants reaching the intended schools of close to 80 percent.[30]

Lessons can no doubt be taken from these national initiatives that are local, country-level initiatives with mass support and that have fought to prove the value of transparency and accountability through their RTI campaigning. Successful country-level initiatives such as these indicate that civil society *can* have a positive effect in pushing for in-country transparency and that this increased transparency can empower citizens, allowing for more efficient aid delivery. What remains to be seen is whether these lessons can be translated into the monitoring of international aid programs.

3. DONOR BEHAVIOR

For all the work of CSO-led initiatives such as IATI and Make Aid Transparent, there remains a struggle to implement transparency and openness in aid programs unless donors are willing to adapt their behavior accordingly. The benefits of aid transparency for donors are set out clearly by IATI.[31] Incentives for joining IATI and for implementing the IATI standard include

- improving the organization's external profile,
- improving organizational processes and systems,
- publishing better data to improve planning processes, and
- Applying political pressures.

A research paper on the relationship between aid transparency and aid recipient corruption levels talks of "nearly universal enthusiasm for aid transparency."[32] But is this really the case? Numerous studies indicate unwillingness on behalf of certain donors, despite their verbal and policy commitments, to be transparent about the impact of their work. Findings from a Pilot Aid Transparency Index in 2011 from Publish What You Fund indicate that the vast majority of aid information is still not published, with only a few organizations publishing more than 50 percent of the surveyed information types. The performance of some of the organizations included in the assessment is "particularly problematic given the amount of aid they give and therefore the relative impact of their lack of transparency."[33] This notably includes the United States (with U.S. Department of the Treasury (scoring 10 percent) and U.S. Department of Defense (14 percent)); Germany Gesellschaft fur Internationale Zusammenarbeit (GIZ–or Agency for International Cooperation) (25 percent); France (31 percent); and Japan (36 percent).

The index revealed that aid information was often inaccessible, not available systematically, and hard to find. Nonetheless, it is apparent from the index that aid transparency *is* possible, as evident from the high scores achieved by organizations such as the World Bank, the UK Department for International Development (DFID), the Netherlands, and the Millennium Challenge Corporation. Interestingly, while some patterns do emerge, one of the key findings from the index is that "an organisation's size, how established they are, or whether they are a multi- or bilateral organisation does not predict or determine the level of their transparency."[34] The nature of an organization should thus not impede its potential for transparency or, equally, excuse its lack of transparency.

Opaque and unaccountable aid reinforces disempowering relationships between donors and aid recipients.[35] It also isolates civil society from the aid process, an involvement that is crucial for effective aid delivery (see section 2). A report by Access Info, "Not Available! Not Accessible!" examining aid transparency in Canada, France, Norway, Spain, and the United Kingdom, found there often to be a widespread failure on behalf of donors to make an explicit connection between budgets and activities in the reports available on the websites of their aid agencies. This also meant it was impossible for the public to make a link between donors' budgets and ongoing activities, effectively blocking them from the aid process.[36]

How donors operate often militates against transparency. A budget brief by the International Budget Partnership carried out in 2008 made interesting findings regarding donor behavior related to transparency. According to the brief, much of the rationale behind transparency failure lies in the fact that donors often direct their aid through mechanisms that are outside an aid recipient government's formal budget system and that follow "separate and parallel budget formulation, implementation, and reporting procedures."[37] Off-budget funding is justified by donor concerns that existing government budget management institutions and practices may be inclined toward mismanagement.

While donors should be concerned about the proper use of their aid, they also need to assess the long-term impact of off-budget funding.[38] According to the authors of the budget brief, off-budget financing often places strains on aid recipient governments. In Ghana, for example, a study found that senior government officials in the country spent approximately forty-four weeks in a year fulfilling the requirements of donor agencies.[39] The brief offers sound advice about how donors should avoid inflicting unnecessary bureaucratic work on partner countries:

> Whenever possible, donors should channel aid flows through government budget systems, for example, by using budget support mechanisms of different kinds. When this is not possible, donors should ensure that the systems and procedures utilized for their projects and programs are as compatible as possible with those of recipient government budget systems. For example, donors should ensure that planned aid-financed activities are captured in the relevant sector's medium-term plan and expenditure framework, and that information on commitments and disbursements is provided to government in formats and at times that facilitate their inclusion in budget documents.[40]

The budget brief indicates that off-budget aid-giving does not facilitate effective delivery or allow for transparency and openness in aid policy and budgeting. Working directly with the aid recipient government allows for improved long-term planning, which is a key area that many aid programs should work on. The current short-term nature of funding cycles, where distribution of funds is assisted by framework agreements, complex designs, and assessment processes that are mostly paper exercises, means that a realistic impact evaluation of aid is difficult.

What assessments such as the Pilot Aid Transparency Index do not explain is exactly *why* some donors might be unwilling to implement transparency. An initial deterrent could be cost: Implementing the IATI standard is costly for donor agencies. The publication of more detailed information in a standardized form requires changes to information technology systems, training, and change management within donor agencies. Donor agencies will need to budget for these additional costs in order to enable them to implement IATI effectively.[41]

Furthermore, fear of inciting a taxpayers' revolt and of undermining the multilateral aid industry if the programs are perceived to have failed may explain donors' reluctance to be transparent and open about their aid processes. In a climate where the effectiveness of aid is already under question, exposing cases where aid has failed to produce results is a risk many donors are not willing to take.

Even when projects have clearly fallen short of their objectives, donors are still reluctant to admit failure. For example, from 1988 to 2003, the Swedish government was involved in a lengthy project in Mozambique, enlisted to help improve the quality of budget management in the country. Over $17 million was invested in the project and, although positive changes were implemented, for example creating a system to prepare state accounts for the first time since 1975, the government of Mozambique eventually rejected the Swedish financial model. The Mozambique government chose instead the Brazilian cash accounting package, which did not even include double-entry bookkeeping—a derivative of old Portuguese systems—most likely because it was a more suitable model given the country's history or more cynically because it does not produce accountable and transparent finances.[42] The project ended in 2003 and, although it is difficult to accurately judge the effectiveness of such a long-running and changing project, it is fair to say the objectives of the Swedish government (namely to reform and build capacity in budget preparation and budget execution/accounting) were not met. Yet the project was never publicly acknowledged to have been a failure, most likely because such an acknowledgement would have generated a backlash from Swedish taxpayers.

The desire on the part of donors and grantees to avoid transparency about outcomes thus stems from fear that it will expose the failure of aid to produce results. The structuring of the aid process often means transparency is not easily facilitated, and often donor practices can mitigate efforts for transparency.

4. THE CHANGING FACE OF DEVELOPMENT

It has become even more crucial in recent years for donors to adapt their behavior in order to keep up with the radically evolving global development landscape. In the last few years alone, transformations have been tangible with the emergence of new donors from the South and East, increased austerity in the North, and a push toward transparency and accountability in aid delivery. This section looks at the development context, how it continues to shape political debate, and the implications for future aid strategies.

The efficacy of aid as a tool to help developing countries has long been under fire. Dambisa Moyo wrote a damning report of aid programs in 2009, entitled *Dead Aid*, which fired an attack on the "patronising" West.[43] In the past fifty years, an estimated $1 trillion in aid has been invested in Africa alone, and Moyo questions what there is to show for it: Sub-Saharan Africa continues to be one of the poorest regions in the world. In June 2012, Moyo continued her attack by outlining in the UK magazine *New Statesman* why, in her opinion, aid does not work, and why "until African governments come to regard aid as temporary support, as opposed to a right in perpetuity, they will continue to fail to implement the necessary measures for self-sufficiency, including food production."[44] Critics of aid note how aid supply has been driven in the past by diplomatic and political pressure and that aid often serves the needs of donors and donor countries before recipients.

In the current economic climate, where seemingly every dollar spent has to be accounted for, it is no surprise that critiques such as Moyo's are becoming ever more prevalent. The state-versus-market debate continues, yet economic history shows that neither the state nor the market on its own is adequate and that economic development is about finding a balance between the two that works but also adapting that synergistic solution as conditions change. East Asian countries seem to have done this more efficiently than African countries; this is one of the keys to their success and why they are emerging as key players in the development field.[45]

Indeed, this emergence of new donors from the East and South is a major shake-up in the development scene. Future prospects for aid programs will also be shaped by domestic austerity in western countries. Indeed, the OECD has linked falls in development aid to the financial crisis, which has affected governments' budgets. In 2011, the amount of aid richer nations give to developing nations fell by nearly 3 percent for the first time since 1997.[46] Increasingly tight budgets in OECD countries are inevitably going to put pressure on aid levels in coming years. Notable cuts in official development assistance in 2011 were registered in sixteen Development Assistance Committee countries, with the largest cuts recorded in Austria, Belgium, Greece, Japan, and Spain.

The shift toward the South and East as emerging Asian donors, including China, India, South Korea, Thailand, Malaysia, Singapore, and Thailand, grow and improve their aid programs will also have a significant impact on the way development currently works. The Lowy Institute for International Policy outlines some of the consequences from this shift:

> Strategy, tighter commodities markets and a glut of donors means foreign aid is increasingly acquiring a geostrategic edge. For aid recipients, emerging-country donors will be attractive for reasons other than strategy

> and self-interest; the emerging economies' own stunning economic successes offer an alternative model for developing countries.
>
> In delivering aid, Asian donors often have different motivations and expectations to those of traditional donors. A combination of local and regional stabilisation, humanitarian concerns, commercial interests and geo-strategic factors tend to be the primary forces motivating emerging donors in Asia. Of course, each donor is developing and polishing their own unique characteristics.[47]

As became apparent in the Fourth High-Level Forum on Aid Effectiveness in Busan, new, emerging donors such as China are less willing to comply with the Eurocentric aid effectiveness agenda. One of the stipulations for China signing the Busan Declaration was that commitment to the declaration for South-South partners is to be on a voluntary basis. China is set to become a key player on the development scene, yet the rise of China (and other Asian countries) poses a threat to the aid process. It "challenges the consensus model of aid and development built up over recent decades by other donors" and "weakens the grip of key international institutions such as the OECD Development Assistance Committee (DAC) which have been at the center of aid reform efforts."[48]

Busan therefore saw the beginning of a new global partnership. "South-South" cooperation will certainly shape the future of development and could challenge efforts for transparency and accountability. New donors currently operate outside traditional donor fora that have provided the focus of many existing transparency and accountability initiatives; it will therefore be necessary to analyze aid from new donors at the country level first, as so little is known about their aid delivery, programming, and effectiveness.[49] One of the main objectives for IATI should be to try and engage new donors with IATI standards.[50] For the moment, there is no formal cooperation between traditional and emerging donors, though this is likely to change as the influence of emerging powers in global governance continues to increase through fora such as the Group of Twenty (G-20). Many of these new donors are a threat to aid transparency, as it is difficult with donors such as Brazil or China to extrapolate what is aid and what is investment. Furthermore, much of this aid comes without conditionality for the recipient countries.

5. RISK-TAKING AND INCENTIVIZING AID

Current aid practices are heavily influenced by the need to meet targets and produce tangible successes, even if this means concealing the reality of donor aid effectiveness and obscuring the transparency of certain aid programs. Original development planners were influenced by the failure of capitalism and by the apparent successes of Soviet industrialization.[51] This led to a mindset of state planning that is still evident in the current practice among donor programs, where a lot of donor aid fails but the pretense is upheld that targets are achieved. This paper believes that these current practices toward aid are essentially a modern variant on the Soviet approach to planning and that a new, risk-taking approach is needed.

As was discussed in section 3, with an increasing demand for donors to be accountable to their taxpayers and demonstrate results, donors are seemingly becoming more risk averse. A particular pattern in donor practice concerns the choice of funding channels. With the call for increasing transparency and accountability, donors are demonstrating a particular aversion to fiduciary risk. While there is donor support for government-led, sectorwide approaches and technical assistance, even in the more unstable contexts there continue to be many donors who prefer to fund projects and programs carried out by trusted UN, NGO, or commercial partners.[52] The benefits of funding projects in this way are manifest: In channelling funds through a UN agency, donors simply shift the risk (and the blame) onto them.

Limiting or avoiding risk can lead to perverse results: The more risk averse the approach, the narrower may be the range of attainable goals.[53] The OECD Aid Risks report gives the example of the Multi Donor Trust Fund for South Sudan, whose success has been limited by unrealistic donor expectations and fiduciary regulations that are too strict.[54] The World Bank was appointed the fund's trustee; however, the fund is restricted in terms of fiduciary risk-taking because of the bank's board and their policy on fiduciary rules and regulations.

In high-risk environments such as Afghanistan and Iraq, donors continue to be risk averse, often to the detriment of effective aid implementation. As the OECD report suggests, "Traditional approaches and standard operating procedures today are often ill-adapted to the contexts of fragility and transition. For more effective aid in situations of transition, donors need to change their individual and collective behaviour, allowing their implementing partners greater flexibility."[55]

It is important, therefore, that a new approach to aid be adopted, one that would embrace rather than avoid risk and where incentives for donors would consequently be put in place for appropriate risk-taking.

This new approach to aid should be based on incentivizing behaviors on the *recipient* level as well, whereby aid is seen as an investment, rather than a gift or contract. The notion of aid as an investment is significant; it implies that the approach should be longer term and should be implemented with certain stipulations on the part of both donors and recipients that encourage maximum effectiveness.

Incentivizing aid has already had success on the recipient level. PROGRESA in Mexico, for example, is an antipoverty program that provides monetary transfers to families; such aid is contingent upon their children's regular attendance at school. The findings demonstrate that the program, based on incentivizing behavior, successfully reduces dropout rates and facilitates academic progression.[56] Similarly, in Indonesia, an experiment in over three thousand Indonesian villages was designed to test the role of performance incentives in improving the efficacy of aid programs. The implementers of the experiment found that "incentives led to what appear to be more efficient spending of block grants, and led to an increase in labour from health providers, who are partially paid fee-for-service, but not teachers. On net, between 50–75% of the total impact of the block grant program on health indicators can be attributed to the performance incentives."[57]

Incentives can equally contribute to greater transparency. More transparent regimes create greater incentives for politicians and aid agencies to undertake better scrutiny of projects funded by their organizations.[58] Perhaps the greatest incentive for donor programs to implement transparency is the proven lower recipient corruption that occurs as a result.[59] Greater transparency in itself is a risk to donors; however, it would nonetheless be better to carry out an honest appraisal of donor programs, rather than continue to uphold the pretense that targets are achieved, when actually a lot of donor aid fails.

"Failure" is a loaded term that is feared and misused in the development context. Failure can actually lead to positive outcomes; for example, if a project is deemed to have fallen short of its objectives, it can still be seen as a positive venture if there was an element of risk-taking involved. Most importantly, lessons can be learned for the future. Donors should therefore admit when projects have not been an un-qualified success and have failed to meet targets. This could lead to a more open and honest debate about why the project fell short of its targets and how it can be implemented more effectively in the future.

6. CONCLUSION

In recent years, an ambitious vision of aid has emerged, spurred on by initiatives such as IATI. Aid is envisaged as being implemented by transparent and accountable programs, programs that will reduce the potential for corruption and that allow for long-term success.

A crucial development, as this paper has discussed, in aid programs is the empowering role of civil society. Citizens and beneficiaries should be empowered to participate in the development process and should hold donors, recipient governments, and institutions to account. Initiatives such as Make Aid Transparent are seeking to do just this; however, these initiatives are still in their early stages, and their focus seems to be mainly on the donor side rather than the recipient side. There would be merit in establishing similar multistakeholder initiatives in recipient countries—initiatives that can work to bring together various stakeholders in order to discuss aid delivery, programming, and effectiveness.[60]

The involvement of civil society in the aid process is thus imperative in ensuring that a donor government, aid agency, or recipient government can be held to account. Citizen participation can lead to more responsive budgets and outcomes, particularly at the local level, as demonstrated by MKSS. MKSS is surely an example to be followed as a successful grassroots uprising with mass local support. It will be important for future research to examine the types of civil society institutions that facilitate transparency most effectively.

It will also be useful to focus on the potential impact of communication technologies, particularly those that use mobile phones and combine voice and data (to deal with problems of literacy and limited connectivity). There are currently six billion mobile phones in the world, and penetration has reached 53 percent in Africa, the least well-served region. By 2020, it is estimated that everyone will own or have direct access to a mobile phone, so applications that empower people, through crowdsourcing platforms, to track aid delivery will become an essential tool in the movement from transparency and accountability. This will require the development of user-friendly mobile interfaces and aligning technology with incentives, so that aid recipients are involved in designing the applications they use for ends that they determine. But the potential is huge.

There is still a long way to go. The move toward transparency is a relatively new focus and, as such, there is very little existing assessment of its impact on the efficacy of aid. This, no doubt, is an area that will be focused on in future years. Current donor behavior does not easily facilitate transparency, with only about 50 percent of aid information being published. A fear of failure means that many donors and grantees continue to implement aid without any accountability. This is often detrimental to effective aid delivery, as it renders coordination among donors, and between donors and recipients, very difficult.

The development context continues to change; the current financial climate is not one in which aid can easily flourish, so it will be increasingly crucial for aid programs to adapt suitably. Aid should no longer be viewed as a gift or contract but as a long-term investment and, as part of this investment, it will be critical to have civil society support. An element of risk-taking should, furthermore, be encouraged; ambitious and risk-taking aid projects should be commended, even if they fall short of their objectives. Lessons can be learned that could lead to even more effective aid implementation in the future.

Only time will tell whether transparency and accountability are likely to empower the potential of aid programs; however, the claims made by campaigners such as Publish What You Fund and IATI in favor of transparency are strong. IATI could be just the tool needed to convert the rhetoric from Accra and Busan into practice.[61] But this will only be possible through citizen participation and the work of country-level, CSO-led initiatives such as MKSS. With pressure from these kinds of initiatives, and willingness on behalf of donors and recipients to coordinate and commit to accountable and transparent aid, we can move toward a new era of aid delivery where aid and development effectiveness continue to improve through honest and open appraisal.

ENDNOTES

1. Sarah Mulley, "Donor aid: New Frontiers in transparency and accountability," *Transparency and Accountability Initiative* (2010). http://www.transparency-initiative.org/wp-content/uploads/2011/05/donor_aid_final1.pdf.

2. Organization for Economic Cooperation and Development (OECD), "The High-Level Fora on Aid Effectiveness: a History" (Paris, France: 2011). http://www.oecd.org/document/63/0,3746,en_2649_3236398_46310975_1_1_1_1,00.html.

3. Ibid.

4. Aid Info, "Aid Transparency Movement" (Bristol, Somerset, United Kingdom: 2010). http://www.aid-info.org./about-us/aid-transparency-movement.

5. Publish What You Fund, "Aid transparency in the Busan Outcome Document" (London, United Kingdom: December 14, 2011). http://www.publishwhatyoufund.org/news/2011/12/aid-transparency-busan-outcome-document/.

6. Publish What You Fund, "Why Aid Transparency Matters, and the Global Movement for Aid Transparency" (London, United Kingdom: May 10, 2010). http://www.un.org/en/ecosoc/newfunct/pdf/luxembourg_bp1_why_aid_transparency_matters.pdf.

7. S. Fukuda-Parr, P. Guyer, and T. Lawson-Remer, "Does Budget Transparency Lead to Stronger Human Development Outcomes and Commitments to Economic and Social Rights?" *International Budget Partnership* 4 (December 2011). http://econpapers.repec.org/paper/esswpaper/id_3a4707.htm.

8. Claire Lockhart, "The Failed State We're In," *Prospect*, 2008. http://www.prospectmagazine.co.uk/magazine/thefailedstatewerein/.

9. BBC News, "Millions wasted in Afghan reconstruction projects, finds report," July 2012. http://www.bbc.co.uk/news/world-us-canada-19052539.

10. Publish What You Fund, "Why Aid Transparency Matters."

11. Ibid.

12. Publish What You Fund, "Why Aid Transparency Matters."

13. Archon Fung, Hollie Russo Gilman, and Jennifer Shkabatur, *Technologies of Transparency for Accountability: An Examination of Several Experiences from Middle Income and Developing Countries* (October 1, 2010). http://right2info.org/resources/publications/technology-for-transparency.

14. Ibid.

15. http://ushahidi.com/.

16. R. McGee, "Annex 5: Aid transparency," *Institute of Development Studies* (2010), p. 16. http://www.ids.ac.uk/files/dmfile/IETAAnnex5AidTransparencyMcGeeFinal28Oct2010.pdf.

17. Dena Ringold, et al., "Citizens and Service Delivery," *Overseas Development Institute* (2012). http://www.odi.org.uk/events/docs/4871.pdf.

18. Fukuda-Parr, Guyer, and Lawson-Remer, "Does Budget Transparency Lead to Stronger Human Development Outcomes."

19. Task Team 2011*, CSO Development Effectiveness and the Enabling Environment: A Review of the Evidence"* (Härnösand, Sweden, March 2011), p. 6. http://www.cso-effectiveness.org/IMG/pdf/final_task_team_on_cso_development_effectiveness_and_enabling_environment_evidence_of_progress_on_aaa__en__.pdf.

20. Engineers Without Borders, “10,000 Canadians Ask for IATI” (Canada: October 2011). http://legacy.ewb.ca/en/whatsnew/story/102/10-000-canadians-ask-for-iati.html.

21. Mulley, “Donor aid.”

22. Mazdoor Kisan Shakti Sangathan (MKSS), “About Us.” http://www.mkssindia.org/about-us/.

23. Commonwealth Human Rights Initiative, “State Level RTI: Rajasthan.” http://www.humanrightsinitiative.org/programs/ai/rti/india/states/rajasthan.htm.

24. MKSS, “Story of MKSS,” http://www.mkssindia.org/about-us/story-of-mkss/.

25. National Campaign for People’s Right to Information (NCPRI), “Activities of the NCPRI.” http://righttoinformation.info/about-us/activities-of-the-ncpri/.

26. L. Peisakhin and P. Pinto, “Is transparency an effective anti-corruption strategy? Evidence from a field experiment in India,” *Accountability India* (2010). http://www.accountabilityindia.in/sites/default/files/documentlibrary/regulationandgovernance_peisakhin.pdf.

27. R. Shrivnisan, “Don’t pay a bribe, file an RTI application,” *Times of India,* May 2, 2011. http://articles.timesofindia.indiatimes.com/2011-05-02/india/29495522_1_ration-card-rti-request-rti-application.

28. Asian Centre for Human Rights, “RTI Activists: Sitting Ducks of India” (New Delhi, India: September 2011). http://www.achrweb.org/ihrrq/issue3-4/India-Sitting-Ducks-2011.pdf.

29. Rebecca Zausmer and Dixie Hawtin, “Taking back our services,” Global Partners and Associates, March 2012. http://global-partners.co.uk/wp-content/uploads/Corruption-in-service-delivery.pdf.

30. Ibid.

31. IATI, “Organisational Incentives and Buy In,” 2012. http://iatistandard.org/getting-started/policy-considerations/organisational-incentives-and-buy-in.

32. Z. Christensen et al., “Transparency Squared: The Effects of Donor Transparency on Aid Recipients’ Corruption Levels” (Washington, DC: Aid Data, 2010). http://s3.amazonaws.com/aiddata/TransparencySquared_aiddata.pdf.

33. Publish What You Fund, “Findings and Recommendations” (London, United Kingdom: 2011). http://www.publishwhatyoufund.org/resources/index/2011-index/findings-and-recommendations/.

34. Ibid.

35. Mulley, “Donor aid.”

36. Access Info, “Not Available! Not Accessible!” (Madrid, Spain: October 2009). http://www.access-info.org/documents/Access_Docs/Advancing/Aid/Not_Available_Not_Accessible_Access_Info_Europe.pdf.

37. V. Ramkumar, and P. de Renzio, “Improving Budget Transparency and Accountability in Aid Dependent Countries: How Can Donors Help?” (Washington, DC: International Budget Partnership, 2009. http://internationalbudget.org/budget-briefs/brief7/.

38. Ibid.

39. D. Brautigam and S. Knack, “Foreign Aid, Institutions, and Governance in Sub-Saharan Africa,” *Economic Development and Cultural Change* 52: 2 (January 2004): 255-285.

40. Ramkumar and de Renzio, “Improving Budget Transparency.”

41. Matthew Collin et al., “The Costs and Benefits of Aid Transparency” (Bristol, Somerset, United Kingdom: Aid Info, April 2009), p. 7. http://www.aidtransparency.net/wp-content/uploads/2010/06/1140-100407-Framework-for-Costs-and-Benefits-of-transparency-with-Annexes.pdf.

42. R. McGill, P. Boulding and T. Bennet, “Mozambique State Financial Management Project” (Stockholm, Sweden: Swedish International Development Cooperation Agency, 2004). http://www.sida.se/Documents/Import/pdf/0429-Mozambique-State-Financial-Management-Project-SFMP2.pdf.

43. W. Easterly, “Review of Dambisa Moyo’s *Dead Aid*” (Commissioned by *London Review of Books* but then rejected by LRB for publication. It was never published.) http://williameasterly.files.wordpress.com/2011/07/moyoreviewforlrbjune2009neverpublished.pdf.

44. D. Moyo, “Does Aid Work?” *New Statesman* (June 2012). http://www.newstatesman.com/politics/human-rights/2012/06/does-aid-work.

45. L. Whitfield, "The Aid Critic: Bill Easterly," *GEG Blog* (February 2012). http://www.globaleconomicgovernance.org/blog/2010/02/the-aid-critic-bill-easterly/.

46. OECD, "Development: Aid to developing countries falls because of global recession" (Paris, France: April 2012). http://www.oecd.org/document/3/0,3746,en_2649_37413_50058883_1_1_1_37413,00.html.

47. D. Cave, "Asia's emerging donors transform aid," *The Interpreter* (New South Wales, Australia: Lowy Institute for International Policy, February 9, 2012). http://www.lowyinterpreter.org/post/2012/02/09/Asias-emerging-donors-transform-aid.aspx.

48. Mulley, "Donor aid."

49. Ibid., pp. 32–33.

50. Mulley, "Donor Aid," p. 32.

51. W. Easterly, "Review of Dambisa Moyo's *Dead Aid*."

52. OECD, "Aid Risks in Fragile and Transitional Contexts: Improving Donor Behavior" (Paris, France: 2011). http://www.oecd.org/development/conflictandfragility/47672264.pdf.

53. Ibid.

54. OECD, "Aid Risks."

55. Ibid.

56. Jere Behrman, Piyali Sengupta, and Petra todd, "Progressing through PROGRESA: An Impact Assessment of a School Subsidy Experiment" (Washington, DC: International Food Policy Research Institute (IFPRI), April 2001). http://www.ifpri.cgiar.org/sites/default/files/publications/behrmantodd_progressing.pdf.

57. B. Olken, J. Onishi, and S. Wong, "Should Aid Reward Performance?" (October 2012). http://economics.mit.edu/files/6923.

58. Christensen et al., "Transparency Squared."

59. Ibid., see Abstract.

60. Mulley, "Donor aid."

61. Publish What You Fund, "Pilot Aid Transparency Index 2011" (London, United Kingdom: 2011). http://www.iwaweb.org/Docs/News/2011-Pilot-Aid-Transparency-Index.pdf.

BIBLIOGRAPHY

Access Info. "Not Available! Not Accessible!" Madrid, Spain, October 2009. http://www.access-info.org/documents/Access_Docs/Advancing/Aid/Not_Available_Not_Accessible_Access_Info_Europe.pdf.

Aid Info. "Aid Transparency Movement." Bristol, Somerset, UK, 2010. http://www.aidinfo.org./about-us/aid-transparency-movement.

Aid Transparency. "The Costs and Benefits of Aid Transparency." April 2009. http://www.aidtransparency.net/wp-content/uploads/2010/06/1140-100407-Framework-for-Costs-and-Benefits-of-transparency-with-Annexes.pdf.

Asian Centre for Human Rights. "RTI Activists: Sitting Ducks of India." New Delhi, India, September 2011. http://www.achrweb.org/ihrrq/issue3-4/India-Sitting-Ducks-2011.pdf.

BBC News. "Millions wasted in Afghan reconstruction projects, finds report." July 2012. http://www.bbc.co.uk/news/world-us-canada-19052539.

Behrman, Jere, Pigali Sengupta, and Petra Todd. "Progressing through PROGRESA: An Impact Assessment of a School Subsidy Experiment." Washington, DC, International Food Policy Research Institute, April 2001. http://www.ifpri.cgiar.org/sites/default/files/publications/behrmantodd_progressing.pdf

Brautigam, D., and S. Knack. "Foreign Aid, Institutions, and Governance in Sub-Saharan Africa." *Economic Development and Cultural Change* 52: 2 (January 2004): 255-285.

Cave, D. "Asia's emerging donors transform aid." *The Interpreter*. New South Wales, Australia, Lowy Institute for International Policy, February 9, 2012. http://www.lowyinterpreter.org/post/2012/02/09/Asias-emerging-donors-transform-aid.aspx.

Christensen, Z., R. Nielsen, D. Nielsen, and M. Tierney. "Transparency Squared: The Effects of Donor Transparency on Aid Recipients' Corruption Levels." Washington, DC, Aid Data, 2010. http://s3.amazonaws.com/aiddata/TransparencySquared_ aiddata.pdf.

Commonwealth Human Rights Initiative. "State Level RTI: Rajasthan." http://www.humanrightsinitiative.org/programs/ai/rti/india/states/rajasthan.htm.

Easterly, W. "Review of Dambisa Moyo's *Dead Aid*." (Commissioned by *London Review of Books* but then rejected by LRB for publication. It was never published.) http://williameasterly.files.wordpress.com/2011/07/moyoreviewforlrbjune2009never-published.pdf.

Engineers Without Borders. "10,000 Canadians Ask for IATI." Canada, October 2011. http://legacy.ewb.ca/en/whatsnew/story/102/10-000-canadians-ask-for-iati.html.

Fukuda-Parr, S., P. Guyer, and T. Lawson-Remer. "Does Budget Transparency Lead to Stronger Human Development Outcomes and Commitments to Economic and Social Rights?" *International Budget Partnership* 4 (December 2011). http://econpapers.repec.org/paper/esswpaper/id_3a4707.htm.

Fung, Archon, Hollie Russo Gilman, and Jennifer Shkabatur. *Technologies of Transparency for Accountability: An Examination of Several Experiences from Middle Income and Developing Countries*. October 1, 2010.

International Aid Transparency Initiative (IATI). "Organisational Incentives and Buy In." 2012. http://iatistandard.org/getting-started/policy-considerations/organisational-incentives-and-buy-in.

Lockhart, Clare. "The Failed State We're In," *Prospect*, 2008. http://www.prospectmagazine.co.uk/magazine/thefailedstatewerein/.

McGee, R. "Annex 5: Aid transparency." *Institute of Development Studies*, 2010, p. 16. http://www.ids.ac.uk/files/dmfile/IETAAnnex5AidTransparencyMcGeeFinal28Oct2010.pdf.

McGill, R., P. Boulding and T. Bennet. "Mozambique State Financial Management Project." Stockholm, Sweden: Swedish International Cooperation Agency, 2004. http://www.sida.se/Documents/Import/pdf/0429-Mozambique-State-Financial-Management-Project-SFMP2.pdf.

Mazdoor Kisan Shakti Sangathan (MKSS). "About Us." http://www.mkssindia.org/about-us/.

Ibid. "Story of MKSS." http://www.mkssindia.org/about-us/story-of-mkss/.

Moyo, D. "Does Aid Work?" *New Statesman*, June 2012. http://www.newstatesman.com/politics/human-rights/2012/06/does-aid-work.

Mulley, S. "Donor aid: New Frontiers in transparency and accountability," *Transparency and Accountability Initiative*. 2010. http://www.transparency-initiative.org/wp-content/uploads/2011/05/donor_aid_final1.pdf.

National Campaign for People's Right to Information (NCPRI). "Activities of the NCPRI." http://righttoinformation.info/about-us/activities-of-the-ncpri/.

Organization for Economic Cooperation and Development (OECD). "Aid Risks in Fragile and Transitional Contexts: Improving Donor Behaviour." Paris, France, 2011. http://www.oecd.org/development/conflictandfragility/47672264.pdf.

Ibid. "Development: Aid to developing countries falls because of global recession." Paris, France, 2012. http://www.oecd.org/document/3/0,3746, en_2649_37413_50058883_1_1_1_37413,00.html.

Ibid. "The High Level Fora on Aid Effectiveness: a History." Paris, France, 2011. http://www.oecd.org/document/63/0,3746, en_2649_3236398_46310975_1_1_1_1,00.html.

Olken, B., J. Onishi, and S. Wong. "Should Aid Reward Performance?" October 2012. http://economics.mit.edu/files/6923.

Peisakhin, L., and P. Pinto. "Is transparency an effective anti-corruption strategy? Evidence from a field experiment in India." *Accountability India*, 2010. http://www.accountabilityindia.in/sites/default/files/documentlibrary/regulationandgovernance_peisakhin.pdf.

Publish What You Fund. "Aid Transparency in the Busan Outcome Document." London, UK, May 10, 2010. http://www.publishwhatyoufund.org/news/2011/12/aid-transparency-busan-outcome-document/.

Ibid. "Findings and Recommendations." London, UK, 2011. http://www.publishwhatyoufund.org/resources/index/2011-index/findings-and-recommendations/.

Ibid. "Pilot Aid Transparency Index 2011." London, UK, 2011. http://www.iwaweb.org/Docs/News/2011-Pilot-Aid-Transparency-Index.pdf.

Ibid. "Why Aid Transparency Matters, and the Global Movement for Aid Transparency." London, UK, May 10, 2010. http://www.un.org/en/ecosoc/newfunct/pdf/luxembourg_bp1_why_aid_transparency_matters.pdf.

Ramkumar, V., and P. de Renzio. "Improving Budget Transparency and Accountability in Aid Dependent Countries: How Can Donors Help?" Washington, DC, International Budget Partnership, 2008. http://internationalbudget.org/budget-briefs/brief7/.

Ringold, Dena, et al. "Citizens and Service Delivery." *Overseas Development Institute*, 2012. http://www.odi.org.uk/events/docs/4871.pdf.

Shrivnisan, R. "Don't pay a bribe, file an RTI application," *Times of India,* May 2, 2011. http://articles.timesofindia.indiatimes.com/2011-05-02/india/29495522_1_ration-card-rti-request-rti-application.

Task Team. "CSO Development Effectiveness and the Enabling Environment: A Review of the Evidence." Härnösand, Sweden, March 2011, p. 6. http://www.cso-effectiveness.org/IMG/pdf/final_task_team_on_cso_development_effectiveness_and_enabling_environment_evidence_of_progress_on_aaa__en__.pdf.

Whitfield, L. "The Aid Critic: Bill Easterly." *GEG Blog,* February 2010. http://www.globaleconomicgovernance.org/blog/2010/02/the-aid-critic-bill-easterly/.

Security in the Information Age

Cybersecurity and Modern Grand Strategy

Sarah Granger & Lorelei Kelly

OVERVIEW

With the complex shifts in international security resulting from increased global volatility and interconnectivity, new kinds of challenges have emerged. These challenges are distributed across the spectrum of traditional national security policy and will require an approach unlike any in our nation's history. In order to adequately prepare for this unprecedented shift, we must look to both traditional security practices and to innovative strategies for a hybrid policy method. Given the expanding public demand for transparency and participation, the process for building a next-generation framework to protect our information, infrastructure, and our people must be conducted primarily through open and inclusive communications while respecting that containment of virtual threats is no longer a viable strategy. This new framework will enable prioritization and development of a resilience-themed network strategy and a policy framework that is adaptable and sustainable through the coming decades.

DEFINING THE GRAND STRATEGY

With the ability to communicate comes power, and today power is distributing across the globe.

The volatile and uncertain circumstances generated by this untethered potential present a paradox. Just as technology is neutral, distributed access to communication can feed innovation and enterprise for good or for bad purposes. Value frameworks help elected leaders and national policymakers navigate risks optimally. While options like retaliation in kind will always be a significant asset, several distributable security concepts need to evolve for the United States to obtain well-rounded strength: To become a twenty-first century power, the United States must move

- away from coercion and toward credible influence,
- away from exclusion and toward participation,away from borders and toward networks,
- away from secrecy and toward transparency,
- away from reaction and toward resilience, and
- away from containment and toward sustainment.

These modern security concepts illustrate a dramatic shift from the last century. They intersect diplomacy, development, and security in myriad ways. They stand in stark contrast to last century's Cold War—an ideological battle characterized by competitive military preparedness between the

United States and the Soviet Union. In those days, leaders sought security through war prevention with enough nuclear weapons to guarantee mutual assured destruction. Yet the guns vs. butter battles of yesterday have been recast. Nearly every U.S. engagement since 1991 has involved volatile, ongoing crises requiring political and social solutions. Our tools left over from the Cold War have proved inadequate for these challenges, which require a commitment to building societal resilience. In 2006, the Center for Naval Analyses brought this theme home when it issued a report on *National Security and the Threat of Climate Change.*[1] Today, an organizing concept for U.S. security is emerging from the military, the State Department, and other federal agencies. It is *sustainment*—a broadly inclusive and bottom-up ability to adapt, persevere, and prosper.[2] The operational moniker for sustainment is "building resilience."

Grand strategy is a concept that describes how a nation's leaders use instruments of power to overcome challenges, defeat adversaries, and generate a unity of spirit toward achieving the nation's common goal. The question, however, is how to think about U.S. grand strategy in a world where our security is unavoidably shared with distant and far different cultures and peoples—including with their long-term well-being. Today's world also reflects new norms characterized by distributed threats, not all of them man-made. Global risks like climate disruption, earthquakes, and disease have no simple solution and do not respect political boundaries. Other threats, like failing states, the preservation of dignity, and contagious extremist ideology do not respond well to the use of force. Moreover, today the U.S.'s persuasive influence (often called soft power) is a measurement of strength based on our credibility, much like military dominance was a generation ago. The theory goes that our willingness to invest in our own domestic strength boosts our resilience and our credibility, which in turn brings us more influence and scope of relationships with which to pursue mutual interests.

RETHINKING HOW TO DIVIDE UP SECURITY

Today, bottom-up societal resilience, i.e. "domestic strength at home," sits side by side with hardware dominance as a primary security concern. This systems framework stresses population security, hence robust health, education, communication, and transport are measures of modern strength. In addition, the threat assessments of this modern security strategy require the national capacity to withstand and bounce back from system shocks. Through this lens, connectivity issues have become a fundamental part of what is generally considered "critical infrastructure." The Congressional Research Service acknowledges that the definition of critical infrastructure is continually evolving and—because it is a large part of congressional budgets—always subject to debate. During the last decade, it evolved rapidly from public works to a more comprehensive list of domestic assets that are vital to U.S. social and economic well-being. These tend to be broad and often taken for granted. Add to the above list public interests like water, power grids, and generator plants. In twenty-first century America, critical infrastructure also includes the means for societywide communication, specifically telephone networks and the Internet.

Within this new paradigm of distributed power and need for resilience, understanding and leveraging collaborative networks is a vital asset. The credibility of our democratic governing style is under immense scrutiny in the current global push toward self-determination. In reports back from Iraq and Afghanistan, military personnel claim that our challenges there are more social than political, that we need more tools that recognize local tradition, that respect the need for dignity, and that create positive life chances for those we hope to influence. Meanwhile, the U.S.'s ability to model evolved democratic practice has been found severely wanting in the wake of the Arab and North African uprisings. If influencing these globally significant events is to be our new criterion for security, it underscores the need to move from the last century's reliance on the military for threat containment to a modern strategy of mutually beneficial relationships; an adaptive, resilient societal infrastructure; and improvements in connectivity, both digital and human.

If we define connectivity as a security principle, in today's world

- our security must address the safety of people across and within our own borders,
- we cannot achieve security alone, and
- we need a new combination of policies and resources to be secure.

This premise requires that we view security as a larger concept than war-fighting or hardware dominance. An ongoing problem for establishing a better civil-military balance in U.S. security strategy is the migration of programs from civilian budgets to military ones. Everything, from breast cancer research to funding for AIDS prevention, can be found in the defense budget; yet a significant recent trend reflects the functional ability of the Defense Department to "get things done" in contrast to other foreign policy agencies. The reasons behind these shifts are numerous: The defense budget receives less scrutiny, it has greater planning capacity, it has more personnel, and it runs under an operational culture. Indeed, the budget sequestration debate of 2012 illustrates perfectly why so much nonmilitary activity happens in the Defense Department's remit. The 2011 executive branch deal with Congress requires across-the-board spending cuts, if no budget is agreed upon. Nevertheless, a broad and bipartisan swath of members of Congress insists that defense spending be untouched. If carried out, this demand would, in effect, pit U.S. domestic resilience against the last century's war plans.

Besides being streamlined and well staffed and resourced, the military has the unique capacity for assimilating big picture analysis. This talent is called "situational awareness." It is a form of understanding that includes strategic judgment and especially pertains to individuals who must act quickly, despite many moving parts that could change and impact the results of the decision at hand. It is anticipatory, not reactive. In the federal government, the military has it in abundance of resources in comparison to other executive branch agencies. The military certainly has more analytical ability for trends and assessments than the U.S. Congress. This problem of agency capacities and competencies is pervasive and points to the need to rethink civil-military relations. In order to create a more balanced division of labor for security, especially for cybersecurity, one priority must be to stop the migration of policymaking to our military services and to impart this capacity for situational awareness to civilian federal agencies and to Congress. Across the board, the federal government is overwhelmed by information. Members of Congress receive up to 1,000 percent more contact from that outside world than in previous decades. Helping the legislature sort, filter, evaluate, and make useful quality information remains a key challenge.

To the extent that cybersecurity reflects the modernizing trend of sustainment over containment, it will be a catalyst for a new, national conversation about a 21st Century Grand Strategy for America. Our leaders' objective should be to inspire Americans to imagine a new and different U.S. presence in the world; to boldly take action; to claim the opportunities before us; and to move forward together to a more resilient, productive, and shared future.

Distributed power looks like complicated and sometimes lethal mayhem to average Americans. Because there is so much uncertainty in the global environment, our leaders must be able to explain the rationale and the possible trade-offs of credibility vs. control in our security choices. Today, explanations about the challenges we face are inadequate and often contradictory. For example, on the one hand the United States promotes rule of law and sees itself as exemplary, and on the other hand it relies increasingly on drone strikes that much of the world considers illegal.[3] Some believe that our response to distributed power is increasingly technological distributed violence rather than evolved democratic practice. On the one hand, we claim to be an open society. On the other, we cling to a culture of controlled access to information within government. These seemingly contradictory scenarios and gray policy areas will grow, play out, and require more interpretation and explanation as information supplies, transparency, and demands for inclusion increase. Indeed, the September 2012 attack on the U.S. consulate in Benghazi, Libya, illustrates the mix of forces at play. Several individuals were killed, including the U.S. ambassador and three other Americans, in a circumstance that included both coordinated militants and protesting masses alledgedly outraged by an Islam-slandering online video.

VISUALIZING CYBERSPACE

How do transparency and its accompanying volatility play out in the cyberspace realm?

"Big data" provides a contemporary example. This buzzword refers to a current human dilemma only made possible by technology. We have moved into an era where datasets have become enormous and often too complicated to parse, sort, filter, or otherwise render sensible. Examples run the gamut from phone logs and email to military surveillance and medical records. Security in this realm requires resilience, not a padlock. Examples of resilience are found in both machines and people, hardware and software, i.e., redundant data storage, distributed power grids, civic trust, and strong community identity.

Cybersecurity requires a good risk management formula, not a padlock. Moreover, much of the risk must be reduced at the individual level. Some typical examples from an everyday office setting are vulnerable network access points (from thermostats and scanners to downloaded games or applying patches that look legitimate when they are not). These are basic human error or human computer interaction challenges. Government's role in this realm is important, but limited. Government can come up with helpful processes, but the private sector will likely be more expedient. The challenge for cybersecurity policymakers will be to find the best practices of each of these contributors. Equally important, the U.S. government should be the standard bearer in its own workplaces.

To illustrate the interconnectedness of the Internet and envision our modern concept of "cyberspace," we can look to astronomy. Imagine a supernova exploding, bursting into bits that form into clusters, planets, moons, and cosmic dust. As matter expands outward, gravity and explosive forces control the connections between the matter and how it forms into galaxies and solar systems. In the case of the Internet, it all began when two computers connected, resulting in the explosive growth we have witnessed in recent decades.

Today, nearly one quarter of the world's population is online: over two billion users.[4] The indexed web has over eight billion pages. By 2011, there were ten billion network connections. By 2016, it is expected there will be nearly nineteen billion. In terms of data traversing the web, according to Cisco, 369 exabytes (369 billion gigabytes) traveled the Internet in 2011, with a forecast of 1.3 zettabytes (roughly one trillion gigabytes) estimated for 2016.[5] Mobile technology is expanding at extraordinary rates, and global penetration is evolving on a massive scale. What this means is that our Andromeda-like, galaxy-sized web of communication, engagement, and commerce cannot be steered like a ship at sea. It can only be guided along existing patterns as it grows at its own pace, continuously expanding in the ether.

The concept of ”cyberspace” began as a fictitious vision of the future, where man and machine became more closely linked. Coined by author William Gibson in his book, *Neuromancer*,[6] the idea gave rise to an entire subgenre called "cyberpunk" including notable films like *The Matrix*.[7] Possibly because of its dramatic nature, the term "cybersecurity" caught on in government circles and has become more prevalent in Washington in recent years, while becoming nearly extinct in Silicon Valley and other communities where the technology is being developed. Now, with military experts talking about their "cyber capacity" and "cyber growth," anything related to "cyber" has morphed into an eerie, dystopian image.

The legislative community has reacted with trepidation and "path of least resistance" inaction. A recent example came in January 2012. In the face of massive protest from the online community, both the House and Senate abruptly reversed themselves on two controversial bills, the Stop Online Piracy Act and the Protect Intellectual Property Act. Yet within a few months, the House passed, with 248 votes, the Cyber Intelligence Sharing and Protection Act, which would significantly limit online civil liberties. Its fate is yet to be determined.

The policy conversation about "cyber" issues is inadequate. Rather than reducing the technology and its weaknesses to the bits and bytes level, the concerns have become elevated to a dark, chaotic threat fit only for military management. In short, the terminology itself has taken a powerful hold over the issue, leading to a situation where some stakeholders prefer no action to a regulatory challenge of unprecedented dimensions. To many, it already seems like scaling the insurmountable.

One of the positive reasons terms like "cyberspace" and "cybersecurity" gained prevalence is that they assume a broader view on the reaches of the Internet, including mobile devices and future inventions yet to take root. "Cyberspace is all of the computer networks in the world and everything they connect and control," explains Richard Clarke in his book, *Cyber War.*[8] As such, we use these terms in this paper to illustrate the vastness of the space in which operations must take place to secure U.S. technology, our information, and our people.

The emerging threats we face include a wide range of individual actors, networks of hackers, hacktivists, and cyberterrorists. They all use the same types of weapons: computers, software, routers, Internet access, mobile devices, and the like. Those responsible for the largest cyber threats generally are groups that may or may not be attached officially to particular government entities, whether they work for them or for rogue organizations. Lines have become increasingly blurred, and attacks have become increasingly decentralized, where we might see hackers in Russia using networks in Iceland to run software that lives on computers in Germany, storing data on Chinese servers, infiltrating U.S. systems. As a result, we face highly complex multijurisdiction issues, because most incidents happen across several invisible boundaries.

Moving forward, in order to acknowledge the end of the containment era, we must

- broaden our concept of security,
- recognize the limits of force in a world of distributed threats,
- stand for fundamental principles as norms evolve,
- establish new decision rules in order to stay ahead, and

- employ new risk models to facilitate vast datasets for threat assessment and response.

For national security strategy purposes, the world used to be easily framed as linear and measured, with predictably scalable solutions. Now it appears more chaotic, and often random, and the solutions must include humans. How we define modern security is at play. Issues of war and peace are the most important responsibilities of citizens and elected leaders, yet our overreliance on coercion and control shows how much leadership continues to execute a strategy stuck firmly in an obsolete paradigm, one incapable of addressing the distributed and human-centered threats we face today.

Across the globe, a profound shift is underway. Demands for self-determination are redistributing power from hierarchies to individuals. The changes will ultimately be a blended mix of top-down and bottom-up strategies and directives. Attaining this goal will require a vigilant global network of individuals and groups who see themselves as stakeholders in power-sharing and legitimate voices in determining the future.

ASSESSING EXPANDING THREATS AND WEAKNESSES

Incidents over the past five years show how serious cybersecurity threats have become and what kinds of attacks we should expect to see in the near future. Recent reports[9] indicate that the United States likely orchestrated the Stuxnet virus that brought down some of Iran's nuclear centrifuges, as the primary weapon in a sophisticated program called *Olympic Games*. This is the first major case of U.S. offensive use of cyber weapons over a period of several years. While the National Security Agency (NSA), the National Security Council, and the Department of Defense (DOD) have alluded to expansive capabilities in the past, Stuxnet is the first such example we have seen and would likely not have been so widely publicized had it not gone rogue, infecting systems outside the centrifuges. As cyber weapons of this type become more common, the United States should expect an increase in attempted attacks and sophistication of attacks.

The numbers are already staggering. According to DOD, their fifteen thousand networks are scanned nearly ten million times each day. Hundreds of thousands of hacking attempts occur on government networks each year. And because attacks can be replicated through automated tools, one hacker can attempt to break into multiple systems simultaneously, and often hackers work in groups together, running multiple programs aiming at a wide range of networks. These hacker groups are generally termed Advanced Persistent Threats in the military, due to their dangerous activities. They can be independently run, hired by larger organizations, or affiliated with governments, but in most cases they are classified as nonstate actors, muddying the waters further.

According to most reports, Chinese hackers have infiltrated networks around the world, most notably in the United States, gaining intellectual property secrets, consumer data, website passwords, and other technologies that could potentially aid Chinese developers in obtaining advantages in the global marketplace. While there is less concern about Chinese military attacks on U.S. networks, it is widely known that “logic bombs,” or rogue code, now exists in most U.S. government networks that could be transferring information to the Chinese.

In the past five years, we have seen a significant increase in cyber attacks on financial and military systems. Some prominent examples include

- attacks on drones, air defense networks, and air traffic control systems in the United States and Israel,
- attacks on financial systems, banks of all sizes,

and financial services companies and organizations, including Citibank, Morgan Stanley, and the International Monetary Fund,[10]
- attacks on technology companies key to Internet development, including Intel and Google,
- attacks on power grids in Estonia and in Ohio, and
- attacks on government networks, including the National Aeronautics and Space Administration (NASA), the Department of Commerce, the Department of State, DOD, and the military Central Command.

While it may seem as if we are witnessing a break in the rash of attacks, they continue to happen every day. The good news is that many of the attempts to hack into critical systems are thwarted. In early May, the Department of Homeland Security warned of a "gas pipeline sector cyber intrusion campaign."[11] Intelligence in this area is crucial, and the media can play a role in disseminating information to entities operating critical infrastructure systems to raise the alert and help them seek and detect any such attempts. This is where information-sharing is crucial and must be conducted in ways where the most critical information is shared without putting private information about Americans at risk. It also points out the urgent need to build resilience into systems and into society in advance.

One of the biggest long-term challenges for policymakers lies in the exponential rate of change in both the quality and quantity of attacks, as well as the perpetrators. We have known for the past few years that it is only a matter of time before terrorist groups get their hands on adequate resources for causing damaging cyber attacks. A recent Al Qaeda video called for an "electronic Jihad"[12] on the United States, meaning our time is extremely limited before we face disruptive attacks. Whether and when terrorist groups obtain enough resources to do damage at the Stuxnet level is yet to be determined, but this is the most sobering threat we face. Al Qaeda does not care whether rogue code designed to take down financial systems or power grids damages other companies and individuals' computers or other unrelated systems in the process. As with the anthrax virus, we could see attacks on seemingly random targets at any time.[13] The worst kind of attacks we have yet to see—hybrid blends of cyber and kinetic destruction, such as biological viruses introduced through water systems simultaneously as power grids are taken down by cyber weapons.

In May 2010, the DOD authorized a new U.S. Cyber Command, headed by the director of the NSA. This command will manage dual responsibilities in parallel with the civilian agencies and is tasked with both defending U.S. military networks and attacking other countries' systems, a.k.a. cyberspace operations.[14] The NSA continues to conduct intelligence and protect U.S. government communications on the civilian side. This is a first and necessary step toward building capacity for coordinated intelligence and action but is only one critical piece of the puzzle.

Significant security challenges lie squarely in our future at this critical stage of the Internet's evolution. We can assume that any connected network can be hacked, and any data on any system in that network can be stolen, altered, or removed. We can also assume that hackers already have malicious code in many of the U.S. networks. It is a general rule that technology companies responsible for building the underlying hardware and software do not have enough monetary incentive or public pressure to fix all of their security holes. This gap is a double whammy, because both the government and private entities controlling the Internet and critical infrastructure tend to depend heavily upon software developed externally by these same companies. As a result, we continue to have security holes in critical networks. Finally, people will always be the weakest link, with human error allowing for simple mistakes that can unravel the most robust networks.

MODERN THREATS AND ANTIQUATED GOVERNMENT

Though both the executive and legislative branches of U.S. government are involved in policymaking on cybersecurity, Congress is far out-matched when it comes to expertise and comprehensive knowledge on the issues. Congress's analog processes—developed in the nineteenth century—are inadequate for the volatility and hyperspeed of digital twenty-first century challenges. This problem is most acute on issues that involve public interests, with technical inputs and second and third order implications—like cybersecurity. This sort of expertise is largely missing during Congress's policymaking process. From self-determination movements to the spread of dangerous nuclear knowledge through the Internet and other communication media, Congress often lacks even a basic understanding of today's fundamental technologies or emerging social/political forces. This lack leads to policy responses that undermine not only our own democratic governance but also our position in the world. This is slowly changing as more members and staffers find ways to bring expert knowledge to Capitol Hill, but the process is still much too slow to keep up with evolving technologies. This gap points to the need for technology subject matter experts to find a way to educate elected leaders about both the technical and the societal aspects of modern technology.

Significant challenges face companies that own much of the Internet infrastructure and control U.S. communications. As financial pressures to be lean and "first to market" trump security, without a push by corporate leadership, shareholders, and customers for prioritized security in products and services, weak links and security gaps will continue to be the standard.

Some areas where there is a need include the use of dated software in government systems that is no longer supported by updates or fixes. Another problem within government is the long timeline required for technology purchases and installation. By the time the vetting and procurement process takes place, the software that the government has purchased is dated, and vendors have little incentive to support the product. A larger systemic problem relates to global competitiveness. The United States is not keeping pace with the human resources necessary for the twenty-first century. U.S. schools are not graduating enough trained engineers every year. Indeed, the demand for a trained workforce is outpacing the supply of personnel. Despite the uptick of research and development investments in recent years, we are not keeping pace with the need. This will continue to be a problem until we can alter the investment landscape and security prioritization.

The Congress is the first branch of government that is outlined in our country's founding documents. The president and Congress, ideally, are coequal branches of government that engage in a healthy competition for influence over security policy. If the goal is to keep cybersecurity within the realm of civilian authority, those with special knowledge must work to balance the knowledge disparity about modern threats between the executive and Congress. The past decade has seen a shift in power from the Congress to the White House on matters of security. In addition, the defense portion of the federal budget increased 70 percent between 2001 and 2010.

This trend is a reaction to the terror attacks of September 11, 2001. Starting with the Authorization to Use Military Force approved within days, this lack of clear civilian control shows up in different ways. "Emergency spending" or supplemental spending requests for the war in Afghanistan have received hardly any scrutiny, much less strategic analysis on Capitol Hill. It also shows up in executive orders to use the military to achieve a policy outcome. Our experience in Afghanistan and certainly the aftermath of the "Arab Spring" illustrate the limits of force in today's world. Our constitution divides foreign policy power between the president and Congress. By law, the president is commander in chief, but only the Congress can declare war. These authorities generally give the Congress power over going to war but the president power over how to conduct it. How must this framework evolve in a world of redistributed power, where both the capacity to do good and the capacity to act treacherously are widely available?

The question can be specifically reframed: What would the division of labor for authority to respond look like after a significant cyber attack? The answer: It depends. Given the current shifting legislative landscape, we are faced with several dilemmas. For small-scale cyber attacks, we have mechanisms in place for rapid response. For large-scale attacks—particularly hybrid attacks such as those on critical infrastructure systems like electric grids—currently there is no lead authority for civilian response. This can pose all kinds of problems, particularly in terms of reporting and tracking incidents and related attacks.

Civilian and military leaders alike want to avoid the overreaction that comes with high adrenaline, such as rushed lawmaking amid uncertain crisis response. One productive step forward would be to find and scale up early efforts at problem-solving, outreach, and education. Some of the most innovative work to this end began over two decades ago in U.S. higher education. For example, Carnegie Mellon University hosts the Computer Emergency Response Team (CERT) dedicated to collecting information on security weaknesses and informing people of these weaknesses, coordinated in one place. CERT plays a huge role in helping companies and individuals secure their systems and networks when bugs are found.

CERT also participates in the national security community by contributing policy ideas and open source tools for individual implementation (a toolbox for creating a Computer Security Incident Response team, for example) along with other practical tools like security audits, network traffic analysis, and vulnerability discovery methods. The CERT experts are also looking at measured, iterative, and agile ways to operationalize preventive measures—like building security precautions into software design and defining how to defend against insider threats like intellectual property loss or sabotage.

Academic and research organizations are beginning to assess, analyze, and make recommendations about cybersecurity. One early leader on this task is the Center for Strategic and International Studies, which published a report[15] and recommendations for the incoming administration in January 2009 and then again in January 2011. The reports call for cybersecurity to be given a higher priority and for the cessation of voluntary compliance measures, including a tough, contractual regulatory backbone.

The Center for Strategic and International Studies' Technology and Public Policy Project Director, James Lewis, sums up the civil military challenge: "[The NSA] has been doing it for 50 years, and they have 800 of the world's best mathematicians and a giant supercomputer. There is some merit to the argument that NSA should protect national networks—except that politically, the U.S. just doesn't invite the military to do police work. So you have this misallocation: NSA has the capability; Department of Homeland Security has the responsibility. We've got to find some way for them to work together."[16]

The multistakeholder approach has been tried in Congress, with mixed results.[17] Congress created the Homeland Security Committee in 2003. Because of committee turf and the broad range of issues covered, the Department of Homeland Security must report to more than eighty panels on Capitol Hill.

This dilemma represents an extreme illustration of the legislature's dysfunction in interpreting modern, complex, global security threats.

To prevent the cyber equivalent of a Pearl Harbor or 9/11, we must act as a collective consciousness, with public and private resources aligned together in preparation, with a serious attitude toward security and safety. Unfortunately, we lack the political cohesiveness that is required for such a massive undertaking, and most likely the past will repeat itself, in a different form. It took Congress forty years to respond to steamboat accidents via policy, over fifty years to enact automobile safety regulations, and twenty-three years to apply air safety regulations after the first plane crash. Cybersecurity incidents have been plaguing us for over two decades, but only recently on a large scale. Cybersecurity bills have not made much headway in Congress. The latest to be introduced was the Cybersecurity Act of 2012. The arguments for and against the bill were significant, but the end result was an impasse in the Senate. Rather than bringing all stakeholders together—government, industry, and civil society—to collaborate and put the best ideas together toward working long-term solutions, we continue what seems to be more of a political stalemate than a forward-thinking security strategy.

A FRAMEWORK FOR CYBER RESILIENCE

In many ways, the U.S. national security narrative resembles an industrial era public relations script. Our policies continue to see the United States as the scheme of things instead of *in* the scheme of things. Wedded to hierarchy, we are still counting ranks while the rest of the world counts links. The technology classic, *The Cluetrain Manifesto*, notes how the Internet has changed "the market" into one big conversation.

> Conversations are where intellectual capital gets generated. But business environments based on command and control are usually characterized by intimidation, coercion and threats of reprisal. In contrast, genuine conversation flourishes only in an atmosphere of free and open exchange.[18]

This passage speaks volumes to our national dilemma over cybersecurity and its place in modern grand strategy. If we stay in the obsolete command-and-control mode, we will miss out on all the opportunities that come with innovation and change. Hierarchical governments—even in democracies—have limits to flexibility and nimble response. Yet one primary principle of resilience is well adapted both to business and to governing: Managing risk is less costly than managing crisis. Cybersecurity policy could also learn much from the world of development, where risk management strategies for rural farmers based on crop insurance, credit, and savings incentivize prevention and create the capacity to deal with volatility and uncertainty. Perhaps "civic resilience technology" would be a more productive and relevant label than "cybersecurity."

While cybersecurity may evoke bleak dystopia, civic resilience technology inspires hopeful opportunity. Resilience happens when today's communication technology harnesses information to provide early warning and vastly improve our response to system-stressing events such as natural disasters and pandemics. Technologies available now offer governments and engaged citizens much better early warning surveillance, situational awareness, and decision-making across all levels of response. This kind of informed action on behalf of a community or a nation is resilience in a nutshell.

Returning again to the example provided by CERT, the CERT Resilience Management Model includes "four essential operational assets: people, information, technology, and facilities."[19] Based on this model, we are farthest ahead in our information. The Department of Homeland Security has acknowledged a significant need for more human resources for cybersecurity programs,[20] we have already assessed our existing technological weaknesses, and our facilities will expand as we respond to the resource issues. What remains is a collection of unanswered questions and policy challenges.

A policy framework of *sustainment* rather than *containment* is intended to frame our national decisions regarding investment, security, economic development, energy, the environment, and engagement well into this century, looking beyond risk and threat with a more positive focus on converging interests and opportunities. The Obama administration has named this future with several initiatives[21] that include connectivity (hence cybersecurity) and will likely continue to put forward new organizing concepts that link connectivity to the direction our nation will take.

The policy process moving forward will be a hybrid. Federal agencies are already pursuing their strong suits. A type of cyber diplomacy is evolving with the 21st Century Statecraft focus at the State Department. This mission is thematically organized around connectivity and using the Internet as a multiplier of diplomacy. Other ways forward will be to look for areas where traditional security could be adapted to cybersecurity practices, such as re-calibrating the mission of nuclear weapons labs. Their resident knowledge about complex design, verification, and technical problem-solving is unmatched. The Cooperative Monitoring Center at Sandia Labs is one example, as is the rich endowment of knowledge that exists in the thirty-nine Federally Funded Research and Development Centers.

Historically, national security models have operated most often within a "need-to-know" framework, keeping information separated in order to ensure tight control. In cyberspace, where our battles happen instantaneously in a galaxy-sized web, we cannot operate in a one- or two-dimensional path for prevention or response. We must operate under the assumption that everything is connected, information is limitless, and data can be transferred in an instant. Information-sharing on multiple levels is critical to keeping up with the speed of the attacks by creating collective intelligence and defense mechanisms. Threats will be diverse and dispersed; therefore, the capability to respond must follow suit.

There is no way to control the chaos inherent in the global communications revolution any more than we can contain an exploding supernova. There is, however, the ability to maximize prevention at the node level, diffusing problems rapidly at each node, whether it is the size of one computer or one million, strategically selecting target nodes based on calculated risks. Containment of cyber attacks on a grand scale is no longer a viable strategy. As with a coordinated response to a biological virus, each system must be inoculated through a simultaneously preventative and reactive process. With thousands of viruses attacking millions of systems every day, containment attempts must be kept at a surgical level while taking a multidimensional approach to national security. This broader focus entails a combination of the traditional four pillars of power: diplomacy, information, military, and economic. A modernized diplomacy, information, military, and economic strategy might include coordinated intelligence collection, 21st Century Statecraft, strategic policy changes, technological advancements, and public education. This kind of resilience network and grand strategy will only occur through cooperation between the legislative and executive branches of government. Moreover, it will need public support. Transparency and sharing of information on a strategic level for the benefit of the greater good is a paramount concern. Given the level of dysfunction and acrimony in contemporary government, our challenge then becomes how to bridge the gaps that exist before our time runs out and—as a nation—we lose by default.

CONCLUSION

Moving forward, we must consider emergent circumstances and volatility not as our enemy but as an opportunity. Collectively embracing the new landscape and planning for resilience models will allow for greater long-term stability and global leadership. With new precedents waiting to be set, some questions still remain that must be answered, namely how pre-emptive and preventative cyber attacks will be considered under international law; how to avoid the escalation of threats; and how to appropriately balance civil liberties and security, including keeping a constant focus on transparency.

In today's world, where transparency is a condition more than a choice, democracies should have a home field advantage. Over time, this form of government has proved successful because it is more adaptive, flexible, and open. Ideally, these qualities will lend themselves to the kind of evolved democratic practice we need today, one that takes the overwhelming noise created by globalization and translates it into intelligent, inclusive, evidence-based decision-making.

Despite nearly two decades of investment in "interagency" and "whole of government" efforts, the need for the U.S. government to figure out better ways to collaborate, share, and optimize decisions remains with us. Since 1991, diplomacy, development, and security have not been separate lanes of policy, yet instead of a fundamental rethink, we have seen a significant migration of civilian tasks into the military's remit. In contrast, former Secretary of State Hillary Rodham Clinton's 21st Century Statecraft reflects a modern, inclusive strategy for engagement. This is a policy lens that views technology as a tool through which societies can be empowered and free speech enabled. What it cannot do, however, is overcome some of the fundamental contradictions between the U.S.'s declared values and perceptions of our policies "on the ground." Drone strikes and our perceived uncritical support for Israel are two examples. While the United States has been a stand-up champion for Internet freedom thus far, it is not clear what the trade-offs will be between security and transparency in the global realm, security and privacy in the domestic.

A best-case scenario in the near future will be if the executive branch continues to promote initiatives like open government and 21st Century Statecraft and to steer the conversation away from cybersecurity and toward civic technology and building resilience. A public engagement strategy to complement advances in transparency would benefit U.S. democracy at this time and give our nation some new models to share with countries that are looking for how to improve democratic practice in the digital age. Technologically enhanced public participation methods will be part of the future. From the Arab Awakening to Germany's liquid democracy, stakeholder engagement is the next big step. If the president and administration officials continue to lead, to reach out to Congress, and to pronounce these values of inclusion through a larger grand strategic lens—one that describes where we are going as a nation in the world—Americans will better understand the concepts, language, and policies we will need to modernize and lead the way toward a promising and more fully shared future.

ENDNOTES

1. Center for Naval Analyses, *National Security and the Threat of Climate Change* (Alexandria, VA: 2006).

2. Mr. Y, *A National Strategic Narrative* (Washington, DC: Woodrow Wilson Center for Scholars, 2011). "Mr. Y" is a pseudonym for Captain Porter and Colonel Mykleby.

3. William A. Owens, Kenneth W. Dam, and Herbert S. Lin, eds.,*Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, DC: The National Academies Press, 2009).

4. Graeme McMillan, "How Big is the Internet? Bigger Than Humanity," Techland, TIME.com, July 20, 2011.

5. *IT Business Edge*, "The Internet Forecast to Quadruple in Size in Four Years," 2012.

6. William Gibson, *Neuromancer* (Ace,1984).

7. *The Matrix*, film by Larry and Andy Wachowski, 1999.

8. Richard Clarke and Robert K. Knake, *Cyber War* (HarperCollins, 2010).

9. David Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *New York Times*, June 1, 2012.

10. Center for Strategic International Studies, "Significant Cyber Incidents Since 2006" (Washington, DC: May 4, 2012).

11. Tim Starks, "Cybersecurity: Rushing to Stall?" *CQ Weekly*, May 12, 2012.

12. Jack Cloherty, "Virtual Terrorism: Al Qaeda Video Calls for 'Electronic Jihad'," ABC News, May 22, 2012.

13. Seung Hyun Kim, Qiu-Hong Wang, and Johannes B. Ullrich, "A Comparative Study of Cyberattacks," *Communications of the ACM* [Association for Computing Machinery] (55: 3 (March 2012): 66–73.

14. Zachary Fryer-Biggs, "U.S. Military Goes on Cyber Offensive," *Defense News*, March 24, 2012.

15. Center for Strategic International Studies, *Cybersecurity Two Years Later* (Washington, DC: January 2011).

16. Craig Collins, "Homeland Cybersecurity," *Defense Media Network*, April 1, 2012.

17. Kristin M. Lord and Travis Sharp, eds., *America's Cyber Future: Security and Prosperity in the Information Age* (Washington, DC: Center for a New American Security, May 31, 2011).

18. Rick Levine et al., *The Cluetrain Manifesto* (New York: Perseus Books, 2000), p. 15.

19. CERT, CERT Resilience Management Model (Pittsburgh, PA: Carnegie Mellon University, 2010).

20. Rene Marsh, "Feds need more computer defense experts, Napolitano says," CNN.com, April 21, 2012.

21. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, DC: The White House, May 2011).

Managing Volatility with the Expanded Access to Information in Fragile States

Joseph Siegle

INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) AND HEIGHTENED VOLATILITY IN AN EVOLVING SECURITY LANDSCAPE

In an eighteen-minute video uploaded to YouTube on May 1, 2012, the militant Nigerian Islamist group, Boko Haram, captured live footage of the bombing of the *This Day* newspaper offices in Abuja earlier that day in which eight people were killed and scores more seriously injured. In claiming responsibility, the group justified the attack for what it contended was the newspaper's favorable treatment of the government in its fight against the extremist group. Boko Haram warned of more such attacks against other media outlets unless their coverage of its movement improved. Several months later, more than thirty cellphone towers were destroyed in northeast Nigeria, Boko Haram's base, disrupting cellphone and Internet service. The targeting of the communications sector is revealing not just for the psychological impact, a common aim of terrorist attacks, but by the explicit effort to shape the group's image to the public.

In India, short message service (SMS), i.e., texting, and social media posts in August 2012 spreading rumors of imminent ethnic violence against Assamese minorities living in southern Indian cities such as Bangalore set off a mass exodus of tens and possibly hundreds of thousands of people. Train platforms were swarmed with panic-stricken families attempting to flee, forcing authorities to add train departures to accommodate the crush. The rumors were all the more believable in that they were supported by graphic photos and video images of casualties purportedly of attacks already begun. Only later was it realized that these images were falsely identified earthquake victims. In the attempt to curb the exodus, the Indian government banned mass texting for two weeks and blocked roughly 250 websites allegedly hosting inflammatory content.

In September 2012, an incendiary amateur video denigrating to Islam was uploaded to YouTube by its U.S. provocateurs, sparking protests and attacks on U.S. diplomatic missions throughout the Muslim world. The attacks in Benghazi, Libya, resulted in the burning of the U.S. consulate and the deaths of four U.S. embassy officials, including the ambassador. While linked to extremist Islamist groups, the attacks highlighted the fragility of Libyan state institutions at the early stages of transitioning from over four decades of coercive rule by Moummar Qaddafi.

These incidents demonstrate the heightened potential for volatility made possible by the growing accessibility of information and communications technology (ICT). This risk dovetails with the increasingly prominent role played by nonstate actors in the panoply of global security threats. The network of Al Qaeda franchises, transnational organized criminal networks, narcotics traffickers, piracy syndicates, warlords, urban gangs, and extremist groups all pose ever more destabilizing threats to international security. ICT has asymmetrically enabled the capability of these relatively small outfits with otherwise limited conventional military power by facilitating these groups' ability to communicate, plan, gather information, transfer funds, organize themselves, and establish command-and-control networks from disparate and at times highly isolated locations around the world. The global positioning system (GPS) and navigational technologies allow traffickers to evade detection and safely cross borders at will across vast stretches of Africa, Latin America and the Caribbean, Asia, and the Mediterranean. Mexican drug cartels use mapping software that tracks the location of police from high-tech control rooms.[1]

The security implications of these unconventional threats are nontrivial. As seen in Mexico, once criminal networks are well entrenched, the costs involved in uprooting them by even a relatively capable state are enormous. Mexico has suffered forty-seven thousand violent deaths in its fight against its narcotics networks since 2006, putting it far over the one thousand deaths per year threshold of an armed conflict. The global drug trade is estimated to involve at least $322 billion each year, reflecting the stakes and potential coercive capacity of these organizations while distorting the economies where these transactions occur at the expense of productive investments. In Africa, the growing collaboration between narcotics traffickers and Islamic militants has caused large swaths of the Sahel to fall out of state control. Oil bunkering is estimated to cost Nigeria 10 percent of its total oil revenues. Meanwhile, a single attack in the oil-rich Niger Delta can cost global consumers billions in increased prices.[2]

The developmental costs of this instability are, likewise, substantial. No conflict-affected country has yet achieved a single Millennium Development Goal.[3] Similar patterns are observed at the subnational level. Marginalized areas tend to experience more instability and continued deprivation. The instability caused by militias in the eastern Democratic Republic of the Congo, for example, costs thousands of lives, limits movement into or out of the area, and has forfeited countless children their access to a meaningful education. Countries affected by major conflict since 1980, over 90 percent of which are internal, are likely to have a poverty rate that is 21 percentage points higher than a country without armed violence.[4] The "piracy premium" insurance companies are charging shipping lines for cargo passing through the Red Sea or Gulf of Guinea significantly increases the cost of trade in Africa, limiting export opportunities and access to inputs.

In short, ICT-enabled nonstate actors pose an escalating risk of volatility in poor or weak states that is increasingly capable of disrupting the global system.

INFORMATION AND VULNERABILITY TO NONSTATE THREATS

The networked nature of these emerging, transnational nonstate threats allows them to move operations and resources as required regardless of national boundaries. Nonetheless, these nonstate organizations need bases of operation outside the purview of an intrusive state with interdiction capacity. Consequently, the global system's weak link—fragile states, with their porous borders and limited capacity, are an attractive forward base and enabler for these illicit networks. Illustratively, Al Qaeda made its first inroads in Sudan and Afghanistan. Its main subsidiaries are now in Yemen and the

Sahel. Piracy in the Red Sea and the Gulf of Guinea is largely a function of the lawlessness and absence of state capacity in Somalia and parts of Nigeria and Cameroon. Latin American cocaine networks have increasingly used Africa as a transshipment point because of its relatively weaker controls. The shantytowns expanding around many urban areas in the developing world have spawned a spate of organized criminal gangs that thrive in environments with little or no police capacity. Militias like the Lord's Resistance Army have sustained themselves for years in the largely lawless border areas of northern Uganda, South Sudan, and the Central African Republic. Reducing the scope for nonstate security threats, then, is linked to strengthening the capacity of these fragile states. In a globalized environment, enhanced stability in one state contributes to greater stability overall.

As one would expect, fragile states tend to have high levels of poverty. Of the twenty-eight countries listed on the Center for Systemic Peace's State Fragility Index as facing high or extreme fragility, twenty-four are also considered low income (even though roughly half of these are natural resource rich). Low-income countries, in turn, are also more susceptible to conflict. Since 1990, low-income countries have been in conflict one year out of four, on average. Fragile states are also typically characterized by low levels of legitimacy. Twenty of these twenty-eight fragile states are autocracies of one type or another. They govern, by definition, with a narrow base of power, usually involving a combination of political party, ethnic group, or geographic affiliation, along with control of the security sector. To maintain the support of this base, state resources and privileges are typically disproportionately directed to those within the ruling coalition. Over time, this leads to ever-greater disparities within a society. Coercion can maintain a degree of stability for some time, though eventually the combination of disenfranchisement, inequities in wealth and opportunity, and perceptions of injustice all contribute to higher propensities for conflict.[5]

Weak governance and capacity in these states also makes them vulnerable to cooption by nonstate actors, the preferred method of operation for illicit trafficking organizations, which thrive by not drawing attention to themselves or directly confronting state actors. To the extent that corruption is perceived as a "normal" way to get ahead, government officials will be receptive to entreaties from these illicit networks. The hierarchal structure of most autocratic states, moreover, makes it easy for narcotics syndicates to gain expansive access to government support once the traffickers have coopted a senior official. This has long been seen in Latin America, where politicians, the police, judges, key bureaucrats, and oversight officials are regularly brought onto the payroll of narcotics networks. Similar patterns exist in Central Asia and have been emerging in Africa.

Fragile states, regardless of their level of legitimacy, also provide a ready opening for "spoilers." These are individuals or groups that draw on or create perceptions of relative deprivation along ethnic or religious lines by presenting a narrative that portrays the marginalized population as victims of government policies attempting to mobilize an identity group to violence in order to reclaim their rights. An illustration of such a narrative is a statement from Abu Qaqa, a spokesman for Boko Haram, who said in January 2012 "we have been motivated by the stark injustice in the land. . . . Poor people are tired of the injustice, people are crying for saviors and they know the messiahs are Boko Haram."[6]

Given its mass personal reach and low cost relative to conventional communication channels, access to ICT greatly enables spoilers' capacity to convey their narrative. Governments that have a track record of corruption and fostering disparities stoke such characterizations. Even if the charges levied are unfounded, such polarizing claims are likely to resonate, especially if levels of trust for the government are low. And economic deprivation is a key mobilizer. According to the 2011 World Development Report, unemployment was by far the most commonly cited reason by members of gangs and insurgent groups for why they joined the movement. The widespread poverty in marginalized areas of fragile states makes these populations susceptible to recruitment by illicit or violent organizations, providing the foot soldiers and community cooperation needed for these insurgent networks to sustain themselves over time. These populations are the key target audience of this messaging campaign.

While legitimacy is in many ways a necessary condition for mitigating grievances, it is insufficient to ensure stability. If able, spoilers will use violence to destabilize a legitimate, though weak, government and intimidate a population in order to elevate the spoiler's influence. Such was the approach used by Islamic militants in northern Mali who had been eroding government authority for several years before gaining effective control of this territory (two-thirds of the country's land area) in April 2012, following a coup of the democratic government in Bamako by disgruntled, low-ranking military officers. Accordingly, legitimate governments must be capable of defending themselves and their populations from destabilization. Among other things, this means establishing a capable security sector and being able to deliver basic development benefits valued by citizens while maintaining social cohesion in the face of efforts to fragment the populace along ethnic or geographic lines.

In other words, there is a powerful psychological dimension to the struggle with nonstate actors. While genuine grievances undoubtedly exist in every society, the degree to which the public views a government as illegitimate, corrupt, and responsible for systemic inequities, the more susceptible it is to instability. Winning the battle for public support, then, is the lynchpin for the development-security nexus in fragile states. And, for this, information is a vital tool.

ICT LINKAGES TO SECURITY AND DEVELOPMENT

While ICT can amplify the reach of violent nonstate actors, it can also be a force for development and stability. Societies that have relatively greater access to information and independent perspectives are exposed to a more vibrant marketplace of ideas. Authorities are required to respond to alternative proposals and, in the process, justify their policy choices, leading to fewer ideologically driven and unchallenged policies. More open information environments, similarly, marginalize claims by radical groups or spoilers that can be held up to critical scrutiny and contested, something that many moderate imams in northern Nigeria have done vis-à-vis Boko Haram (sometimes generating a violent response).

Greater access to information also facilitates the sharing of development lessons learned, the adoption of best practices, and the introduction of new ideas and technologies from outside the society that improve living standards. With greater access to information, watchdog groups are better able to assess governmental budget priorities and allocations. This reduces the scope for corruption and improves the efficiency and equity of government. Greater levels of transparency and oversight, accordingly, contribute to greater stability.

ICT also contributes to greater legitimacy, one of the key stabilizing factors of fragile states. Election monitoring groups are able to conduct parallel vote counts at each local polling station and report these results back to a central headquarters, enabling real-time projections that challenge dubious official results. The growing ubiquity of mobile phones with video camera capability is also expanding the capacity of citizens to document abuses in the electoral process. It was through such methods that blatant ballot-stuffing during Russia's December 2011 parliamentary elections for President Vladimir Putin's United Russia Party was captured and disseminated on the Internet. The effect was to badly discredit Mr. Putin's claims of legitimacy. ICT was also believed to have contributed to what were hailed as Nigeria's cleanest elections ever in April 2011.[7] ICT is therefore redefining relations between governments and societies.

The ability of citizens to quickly access information from multiple sources is also fostering more accountable governance by making it harder for exclusionary powers to maintain their monopolies on information. Cellphones with the capacity for texting and access to Facebook and Twitter are providing citizens in many low-income countries with the enhanced ability to exchange information horizontally in a society, thereby reducing a key impediment to organizing ordinary citizens around their common interests.[8] This uphill battle to organize large, disparate populations has historically been a major advantage of autocratic governments and why they have been able to sustain governance and development policies that are injurious to the majority. With the elevated ability for citizens to communicate directly in large numbers, priorities for transparency, equitable development, justice, and participation are more likely to be advanced.

Local communities are now better able to monitor whether the designated expenditures on their local schools and health clinics are being made, while ensuring that local pharmacies remain adequately stocked with needed supplies. Farmers are better able to check prices at all area and regional markets when making planting and harvesting decisions, significantly empowering them in negotiations with marketers. Villagers in remote communities that heretofore have been highly vulnerable to predatory violence by state security forces or militias can now communicate with other local villages as part of collective security networks as well as notify government or United Nations (UN) agencies of their need for assistance, fostering more timely responses.

Greater access to information also enhances stability by contributing to more effective early warning systems in the face of humanitarian crises. More open societies have historically been much more responsive to droughts, earthquakes, hurricanes, and other disasters, because news of an emerging threat is more likely to be communicated to the capital city and disseminated on media outlets. This attention puts pressure on a central government to take urgent action to safeguard the lives of citizens in harm's way. Governments that are seen as unresponsive or incompetent lose the confidence of their populations and are subsequently unable to marshal the public support needed to govern. This feedback loop is one of the reasons democracies are better able to mitigate crises of various types. As Nobel laureate economist Amartya Sen, famously observed, "No substantial famine has ever occurred in any independent country with a democratic form of government and a relatively free press."[9] In contrast, autocratic governments are regularly the origin of preventable humanitarian crises. With their ability to monopolize the flow of information, they have historically been able to prevent the dissemination of news of such crises and can respond to them as suits the government's interests. The response by the militant group al-Shaabab to the severe East African drought of 2011 is a contemporary case in point to this recurring phenomenon. The group, which effectively controlled large parts of southern and central Somalia at that time, denied international humanitarian assistance agencies access to these areas, resulting in the deaths of untold thousands of Somalis. Neighboring Kenya and Ethiopia, faced with the same climatic conditions, suffered relatively few drought-related deaths.

Greater access to information similarly engages the international community in the build-up to a humanitarian or human rights crisis much sooner than would otherwise be the case. Guided by real-time and more reliable information, international actors are better able to overcome the ignorance that enables collective inaction in the face of systematic human rights abuses. This was seen in the decision by the international community to intervene to stop former Libyan leader Muammar Qaddafi's effort to violently repress a popular uprising in the country's second city, Benghazi, in 2011. While international intervention is not the outcome in every case of such state violence (such as in Syria in 2011–2012, largely due to deadlocks at the UN Security Council), the level of international attention and pressure is invariably greater than has been the case in the past, when these abuses took place in obscurity (consider the largely silent international reaction to the estimated twenty thousand to forty thousand deaths in Syria during the Hama massacre of 1982).

These channels by which ICT contributes to transparency and stability coincide with a global pattern of relatively greater development progress and stability observed during the past several decades in which information technologies have become more ubiquitous. For example, the frequency and magnitude of conflict have declined by 60 percent since the mid 1990s, reducing the number of countries in conflict from thirty-five to twenty-one in 2011.[10] While varying from year to year, the number of refugees around the world has similarly declined from eighteen million in 1992 to 10.4 million in 2011. Likewise, infant mortality rates, a reliable barometer for development more generally, have declined by 41 percent since 1990.[11] Accordingly, only countries affected by conflict are not on track to meet the Millennium Development Goals of halving poverty by 50 percent from 1990 levels. Annual economic growth rates for low-income countries have similarly been much more robust since 2005, averaging 3.3 percent (despite the global financial crisis of 2008–2009), than they were from 1990 to 1995, when average growth was effectively flat. Moreover, the variation in these immediate post-Cold War growth rates was more than three times as large, reflecting the greater volatility of that period. Cases of hyperinflation, which were not uncommon up through the early 1990s, are today relatively rare, an indication of the stronger commitment to macroeconomic stabilization and the more active role played by global financial institutions, particularly the International Monetary Fund.

To be sure, there have been other important, overarching global dynamics that have shaped the relatively more stabilizing patterns of the past two decades. These dynamics include the end of the Cold War, the greater willingness of the international community to mount peacekeeping operations in fragile states, the expansion of global trade, and the accelerated dissemination of development technologies, among others. Nonetheless, all of these other phenomena have been significantly enabled by the upsurge in communications capacity during this period.

It is similarly important to recognize that this expansion in the capacity for ordinary citizens to communicate and gain access to unprecedented amounts of information did not unfold in a contextual vacuum. Rather, the surge in ICT occurred simultaneous to the wave of democratization that swept Latin America, Eastern Europe, Africa, parts of Asia, and now the Middle East starting in the 1980s. The relatively greater openness of democratic governance structures to the free flow of information has facilitated the diffusion of information technology. Accordingly, it is important to recognize that ICT is part of a broader governance process. The development of an information and communications sector requires if not an enabling environment at least not a hostile one.[12]

In short, the commonly expressed concerns raised at the outset of this essay that the expanding accessibility of ICT is contributing to greater volatility in fragile states has been accompanied by an improvement in the security and development interests of many citizens in low-income countries. That is, the expansion of ICT appears to present a trade-off of greater potential short-term volatility from destabilizing nonstate actors versus the long-term, institutionally based, stability-enhancing benefits.

THE INDISPENSIBLE ROLE OF CIVIL SOCIETY AND MEDIA

While ICT may be reshaping state-society relations vis-à-vis development and security outcomes, it is important to recognize that, in the end, these are simply tools. In other words, ICT is value neutral. ICT requires reform-minded actors, generally civil society organizations (CSO) and the media, to be transferred into meaningful change for ordinary citizens. In other words, progress only occurs when these tools are anchored in organizational structures that can analyze, inform, and mobilize the majority around key reforms, maintain pressure on government officials for greater transparency and service delivery, and sustain this process over time. The issue of sustainability is particularly important, since institutional change does not happen quickly and is subject to setbacks (witness the challenges facing Egypt, Tunisia, and Libya in the initial stages of their transitions from long-established authoritarian rule). CSOs are particularly critical in sustaining momentum for reforms in these early years of a transition while governance institutions are reconstructed.[13] In fact, the depth of civil society networks in a society has been shown to be a strong predictor of this resiliency—and the likely success of democratic transitions.[14]

Independent media also play an indispensible role both in gathering and disseminating information to a mass audience, effectively empowering the broader society. Public exposure of corruption and ineffectiveness in the headlines of newspapers, radio, and television broadcasts, in turn, serves as a very powerful catalyst to spur government responsiveness. Founded in 2008, Mozambique's online (and most popular) newspaper, @Verdade (or "Truth" in Portuguese), has helped change the public dialogue by covering household issues like bread subsidies, electricity prices, and crime in the slums. Its investigation into the poor service of the state electricity provider has prompted an official inquiry and improved service.[15]

Media and civil society groups also play an instrumental role in generating and using information to improve governance. Research organizations and think tanks use information to contribute to the policy debate with independent analysis that may force government officials to respond to unwelcome data or alter their policy course. Watchdog groups provide the technical expertise to monitor budget expenditures and assess the degree to which these are meeting societal priorities. Human rights groups document and confront governments for abuses of citizens, highlight corruption or injustices in the court system, and advocate for reforms. Professional associations of journalists, teachers, and lawyers can set and uphold standards for their fields while accelerating the pace at which best practices and lessons are learned are disseminated. By identifying bottlenecks to accessing licenses, credit, or regulatory approvals, business associations representing mid- and medium-sized enterprises help level the economic playing field, spurring innovation, productivity, and jobs. In the process, they are strengthening the middle class, widening a potentially powerful constituency group for reform. By organizing workers, labor unions can help mobilize large numbers of workers for broader governance reforms.

The horizontal and vertical networks that these CSOs create have the potential to link societies across ethnic, geographic, and class boundaries, amplifying the effects that any one organization could realize. By doing so, these civil society groups are creating a societal "demand" for better governance and accountability. It is by linking these networks across a society that civil society can be a resilient force for reform in the face of inevitable pushback. CSOs may also have networks outside a country. This accelerates the access to best practices, technical assistance, and funding that can help advance citizen priorities.

ENHANCING ICT'S BENEFICIAL IMPACTS FOR SECURITY AND DEVELOPMENT

The development-security challenge in fragile states is ultimately a governance process. It often entails a battle for public support from a skeptical populace jaundiced by years of government propaganda and indifference to the concerns of ordinary citizens. This challenge is frequently exacerbated by an antagonist, also vying for popular support, in order to persuade youth in marginalized regions that they should take up arms to redress felt grievances. This struggle is joined by a third force—reformist CSOs and media—that aims to improve norms of transparency and accountability in a society so as to improve security and development. All sides of this struggle are seeking to maximize the impact of new information and communication tools that are potentially decisive to defining public perceptions. Strategies for enhancing the positive repercussions of ICT, therefore, must advance the capacity and effectiveness of reformist actors if they are to be effective.

Recognize that ICT Is Part of the Governance Process

ICT adoption has tended to flourish in more open societies where governments are more tolerant of the free flow of information. Accordingly, efforts to expand the positive impacts of ICT cannot treat governance as a neutral factor and solely focus on building the technological components. Rather, the type of governance system in place has a major influence in shaping the information environment. Reformers, therefore, should conceive of ICT initiatives from a broader governance framework and encourage norms tolerating dissent, freedom of speech and assembly, transparency, and freedom of information regulations.

Reform-minded domestic and international partners should also recognize that the transparency, stability, and development benefits from ICT do not occur spontaneously but are the result of development and activist organizations that can take advantage of the available information to advance these goals. Since these changes are only realized over time, investment in civil society and media institutions is needed. These domestic actors can then effectively sustain and employ information and communication tools to advance a constructive public debate, educate citizens, expose corruption, and establish public service watchdogs to strengthen accountability and foster needed course corrections. A multiplicity of media and information channels can also have a moderating effect by marginalizing extremist views as outside the mainstream. A broad array of information outlets also facilitates the speed with which rumors can be fact checked and stem the panic that is more likely to emerge when the few available media sources are not trusted.

An inevitable challenge of strengthening the media in fragile states, however, is the risk that media outlets will become platforms for hate speech and incitements to violence. This typically occurs when an outlet is aligned with a particular political party or ethnic group and may be controlled by wealthy patrons or politicians seeking to advance their agenda.

Left unchecked, these media vehicles can be highly polarizing in a society, trumpeting perceived grievances of one identity group vis-à-vis the presumed exploitation by a rival group. Proactive guidelines, ideally crafted with independent journalists, curbing such destructive uses of the media are needed. These must be balanced, however, by strong checks against political actors using such guidelines to stifle criticism.

Protecting Journalists, Bloggers, and Civil Society Organizations

For ICT to have a beneficial effect in a society, those individuals and institutions that are responsible for generating and disseminating information must be protected. By facilitating the flow of information, journalists, bloggers, watchdog groups, and human rights organizations play a unique role in a society by informing the public, fostering public debate, exposing corruption and abuses of power, and encouraging accountability. Since this threatens the privileges of actors who have benefitted from controlled information environments and exclusive governance arrangements, journalists and other information agents are regularly targeted for intimidation, violence, and murder. In fact, roughly seventy-five journalists around the world are killed every year for the stories they write.[16] Yet, over 90 percent of cases where journalists have been murdered go unsolved.[17] Many of these crimes are never even investigated.

More aggressive action is needed. Silencing journalists, after all, is more than an ordinary crime; it denies the entire society of the access to information and analysis that can help citizens make informed judgments on the priority issues faced. All states, especially those that are transitioning or fragile, should therefore be pressed to establish laws that explicitly recognize the basic civil rights of journalists, bloggers, and human rights defenders.[18] This includes decriminalizing charges of libel and defamation, which are tools frequently used to imprison journalists or cow them into self-censorship. Such statutes should also authorize independent investigations into the suppression of society's "eyes and ears." Since local authorities cannot be counted on to conduct such investigations impartially, these inquiries should be authorized at the national level, possibly with the participation of international partners.

International actors can further undergird efforts to protect journalists by withholding development funding to governments that do not uphold these protections. Doing so is justified not only on human rights grounds but also for development effectiveness. Without journalists and watchdog groups, development assistance will lack transparency and will be much more subject to diversion. Under such conditions, aid is highly vulnerable to inadvertently propping up autocratic systems that are detrimental to both development and security.

A Communications Strategy for a New Era

The greater accessibility of ICT provides new opportunities for governments to communicate directly to and hear from citizens, building a more constructive relationship between the state and society. In some cases, this will be the first occasion citizens will have to state their preferences to those in power. Yet there are relatively few models of governments in fragile states taking advantage of ICT to communicate more effectively with citizens, building the trust and cooperation needed to counter the appeals of spoilers and advance security and development.[19] The challenge is all the more difficult in these contexts because of the legacy of distrust that often exists between the state and its citizens. Still, it is imperative that reformist governments communicate to citizens the initiatives being undertaken to address the priority grievances held by communities. It should not be assumed that these undertakings are well known to the public.

Such communications efforts must be more than mere propaganda or public affairs announcements, however, as these forms of communication are familiar to many societies and will be quickly dismissed. Rather, an authentic communications strategy must be based on a sound array of policy priorities. For many communities in fragile states, this means greater attention to development, in particular, health services, schools, and agriculture, and infrastructural initiatives that can generate a large number of jobs. In this way, development is a tangible arena in which the battle for popular support takes place. That these development programs are conducted in a transparent and equitable manner is also essential in order to convince citizens that public resources are not primarily being used to advance the interests of favored identity groups or patronage networks. Perceptions of corruption are particularly debilitating, as they engender attitudes of injustice and grievance that can be more easily mobilized by spoilers. Governments can also demonstrate their commitment and responsiveness to the security of local communities by establishing ongoing channels of communication with vulnerable towns and villages.

An effective communications strategy will also involve outreach. Studies have shown that public messaging coupled with interpersonal contacts through a trusted network are most effective for generating behavior changes.[20] Networks of public health workers or agricultural extensionists, therefore, can be vital components of a communications strategy of development progress (and of government concern for citizens, more generally). CSOs with strong ties to local communities can be vital partners in this process, as well. Such outreach efforts also provide an opportunity to hear from citizens, making the dialogue a two-way process and creating more community ownership over the development efforts undertaken. It is here that ICT tools open more possibilities for direct citizen feedback and input to government officials than have previously existed.

In sum, information is and has always been central to the stability equation in fragile states. ICT amplifies this effect—both as an opportunity and as a threat. Given the legacy of distrust, ICT can indelibly reinforce negative reputations for governments. Therefore, it cannot be "business as usual" if these governments hope to gain popular support and stability. New means of communicating authentically to citizens must be learned. More fundamentally, governance standards of legitimacy and accountability will need to be raised in increasingly information-rich societies. Given the greater trust afforded CSOs and the media, these actors have ever more important roles to play in the security-development equation in the ICT era.

ENDNOTES

1. *Forum Citizens*, "Can Google Defeat Boko Haram?" http://forumcitizens.com/business/can-google-defeat-boko-haram/.

2. Khusrav Gaibulloev and Todd Sandler, "Growth Consequences of Terrorism in Western Europe," *Kyklos* 61: 3 (2008): 411–414.

3. World Bank, *World Development Report 2011: Conflict, Security, and Development* (Washington, DC: World Bank, 2011).

4. Ibid.

5. World Bank, *World Development Report 2011*.

6. Monica Mark, "Boko Haram Vows to Fight Until Nigeria Establishes Sharia Law," *Guardian* (UK), January 27, 2012.

7. Judith Burdin Asuni and Jacqueline Farris, "Tracking Social Media: The Social Media Tracking Centre and the 2011 Nigerian Elections" (Abuja, Nigeria: Shehu Musa Yar'Adua Foundation, May 2011).

8. Steven Livingston, "Africa's Evolving InfoSystems: A Pathway to Development and Security," *Africa Center for Strategic Studies Research Paper #2* (2011).

9. Amartya Sen, *Development as Freedom* (New

York: Knopf, 1999).

10. Monty Marshall and Benjamin Cole, *Global Report 2011* (Vienna, VA: Center for Systemic Peace, 2011).

11. UNICEF, *Committing to Child Survival: A Promise Renewed* (New York: UNICEF Progress Report 2012).

12. Shanthi Kalathil and Taylor Boas, *Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule* (Washington, DC: Carnegie Endowment for International Peace, 2009).

13. Joseph Siegle, "Building Democratic Accountability in Areas of Limited Statehood" (paper presented at the International Studies Association Annual Conference, San Francisco, CA, April 1–4, 2012).

14. Adrian Karatnycky and Peter Ackerman, *How Freedom is Won: From Civic Resistance to Durable Democracy* (New York: Freedom House, 2005).

15. Katherine Baldwin, "How One Newspaper Wants to Change Mozambique," *Time*, December 28, 2010.

16. Committee to Protect Journalists, "914 Journalists Killed since 1992" (New York: May 30, 2012). http://cpj.org/killed/.

17. D. Mijatovic, "Protection of Journalists from Violence" (Strasbourg, France: Council of Europe, Commissioner for Human Rights, *Issue Discussion Paper*, 2011).

18. Joseph Siegle, "Overcoming Dilemmas of Democratisation: Protecting Civil Liberties and the Right to Democracy," *Nordic Journal of International Law* (2012).

19. Shanthi Kalathil, John Langlois, and Adam Kaplan, *Towards a New Model: Media and Communications in Post-Conflict and Fragile States* (Washington, DC: The World Bank, Communication for Governance and Accountability Program, 2008).

20. J. F. Phillips, Mian Bazle Hossain, and Mary Arends-Kuenning, "The Long-Term Demographic Role of Community-Based Family Planning in Rural Bangladesh," *Studies in Family Planning* 27: 4 (July-August 1996).

If You Are Seeking an Advantage, Information Does Not Matter

James Valentine & James Herlong

INFORMATION DOMINANCE: A TRANSPARENTLY INADEQUATE STRATEGY

In the U.S. military and intelligence realms, the term "information dominance" is popular jargon for discussing the relationship between intelligence, policy-making, and the modern information environment. John Arquilla first coined the phrase in his 1994 article, "The Strategic Implications of Information Dominance." It is most accurately defined, he states, as "knowing everything about an adversary while keeping the adversary from knowing much about oneself." He made a compelling argument that modern technology had enabled the emergence and possible supremacy of "control warfare," which paralyzes the enemy and prevents them from acting; it removes their capacity to make war despite an abundance of will, materiel, and military know-how.[1]

Equally popular is "decision advantage." While it is hard to pinpoint the exact origin of this term, the U.S. government certainly embraces it. The phrase occurs thirteen times in the director of National Intelligence document "Vision 2015," which states that the *role* of intelligence in national security is to "create decision advantage."[2] A quick Google search reveals the use of these words in document after document, geared toward military, intelligence, or policymaker use. The definition of decision advantage is as difficult to pinpoint as its origin but might be expressed as the ability to arm friendly decision-makers with better information than their adversaries. This, presumably, will enable better decisions, all other things being equal.

If we accept that information is a lynchpin in national security, because it can be "operationalized" into decision advantage, then information dominance makes a great deal of sense. The U.S. Navy agrees; it promulgated *The U.S. Navy's Vision for Information Dominance*, in May 2010, which defines "Information as warfare."[3] In addition, it created a deputy chief of Naval Operations for information dominance, combining its intelligence, communications, and network staff into a single organization focused on both information and the technology that allows the navy to operate in the electromagnetic (EM) environment. This vision promises to make information a "main battery of 21st Century seapower."[4]

The views expressed herein are those of the authors and are not to be construed as official or reflecting the views of the Commandant or of the U.S. Coast Guard.

It is quite clear that the U.S.'s national security apparatus, from the military to intelligence agencies to policymakers has embraced the role of information and information technology in national security and power. The only problem is that the strategy of information dominance to create decisional advantage or superiority is already hopelessly out of date. Information dominance was conceived in an era where access to the EM domain was the purview of countries and regions that were well off; only the global "haves" could publish to, and scrape content from, the EM information environment. The high level of transparency and interconnectedness that exists today, enabled by geospatially independent access to information, existed then only in science fiction and, perhaps, minds at the bleeding edge of information technology (IT). Because of our modern degree of transparency, in the greatest paradox of the "information age," information does not matter.

FROM OPACITY TO TRANSPARENCY

To be fair, the previous statement is a touch flip. Information clearly matters, from the perspective that without information, decisions are made in the dark. This, obviously, is hardly optimal. However, the strategy of information dominance is predicated on the idea that information and its associated technology provide strategic advantage. That is, if the United States possesses information and the right technology to exploit it, shape it, and deliver it as needed, then it will occupy some kind of decisional high ground, compared to competitors.

Today this notion is wrong, and it will be for the foreseeable future. The problem is with the way things have changed in the nearly twenty years (almost a generation!) since Arquilla wrote his article. In 1994, the digital age was in its revolutionary stages. There was no Wikipedia. The text message was celebrating its second birthday. Google was two years away. Apple would not introduce the iPod for seven more years. Despite the digital revolution, the requirements for power, infrastructure, and expensive equipment limited the revolution to people and countries that could afford it. This also meant that digital content was limited, because only people who had the equipment and expertise could push information to and through the web,[5] or access it.

The upshot of the information environment in 1994 was that it looked almost precisely like the information environment in 1894, from a strategic perspective. Both eras were defined by informational scarcity, asymmetry, and friction. Information was scarce, because it was expensive. It took time, sweat (sometimes blood), and treasure to come by, collect, or generate information. Asymmetry existed because geography mattered; different entities in different places had access to different pieces of information. This asymmetry was perpetuated by friction. The rate of information transfer was so slow that asymmetry was never corrected. While information might be more or less scarce, asymmetrical, or subject to friction at any given place or time, overall, from a global perspective, these characteristics have defined the information environment since the dawn of human history. Conquering them has traditionally taken a herculean investment of people and resources, the creation of bureaucracies and procedures, and lots of collective time.

SECURITY IN AN INFORMATIONALLY OPAQUE ENVIRONMENT

States pursuing security exploited these traits of the information environment just as they exploited the physical environment. Because information was expensive and scarce, the return on investment regarding the collection of information was very high. Having a lot of information conferred an inherent superiority over an adversary that had less. Further, that superiority was scalable; the more information you had compared to your competitors, which were almost certainly states that could expend similar amounts of energy, the greater your superiority. There was great incentive to expend national resources on having large volumes of relevant information.

Similarly, asymmetry meant that information you did acquire was unique, or nearly so. The information you had painstakingly, perhaps secretly, collected was unknown to your adversaries, or at least the fact that you knew it was unknown to them. This created a security analogy to the economics concept of informational asymmetry; when one party has access to information that others do not, that party possesses an advantage in economic transactions. Similarly, informational uniqueness in the realm of national security allowed you to have insights that others could not, providing a strong element of decisional superiority.

Finally, the natural, high level of environmental friction meant that information could be kept secret from others with relative ease. States exploited this by instituting cheap and effective methods of informational security, many of them physical, to increase friction even more. As with the collection of information, the return on investment for security was very high. With low to moderate effort, informational asymmetry, in terms of both volume and uniqueness, could be preserved.

When you line up information volume, uniqueness, and security as the most efficient and natural strategies for states to adopt in an environment defined by information scarcity, asymmetry, and friction, the result is to "know as much as possible about relevant things while preventing others from knowing that information, or knowing we know it." This sounds strikingly similar to Arquilla's more war-centric definition of information dominance."[6] Information dominance has been the national security strategy for information for thousands of years. We just did not have a coherent name or explanation for it until 1994—when it still made sense as a strategy.

TRANSPARENCY: WHAT HAS IT WROUGHT?

Unfortunately for the U.S. Navy, things have changed. Pictures, videos, and text can now be exchanged between all nodes of the web in the literal blink of an eye. Mobile multimedia devices, which we call "smartphones," allow personal computing to be done in the palm of our hands. The technology for these multiple-use, mobile devices is so cheap, and so available in every corner of the globe, that entire economies in Sub-Saharan Africa—the least developed region of the world—depend upon them for economic transactions of all kinds.[7]

Information used to be scarce; now it is so ever present that our problems are not about obtaining information but organizing, parsing, and sorting it. A study in 2009 estimated that the average U.S. consumer ingests 3.6 zettabytes a day, which corresponds to a stack of books seven feet high covering all of the United States.[8] At least one study estimates the entire storage capacity of humanity at 295 exabytes (a one with twenty zeros) and notes that our processing capability is "growing at an exponential rate."[9]

Similarly, informational asymmetry has been supplanted by people in the developed and developing worlds largely having access to the same datasets, the same news, the same raw facts and information the world over—a never-before-seen kind of information parity and relative transparency[10] enabled by geospatially independent access to information. Given the surge of mobile access even in the poorest areas, it is entirely possible that currently disadvantaged states and people will achieve similar parity and transparency, as South Korea did in a few short decades—an occurrence that could remake the global security map as previously weak players gain access and power.

While information transfer rates used to be governed by friction, on June 20, 2009 Neda Agah-Soltan was murdered at a protest by a member of Iran's *basij* militia. #Neda became a top trending topic on Twitter, and her death made international headlines the same day.[11] This all happened despite Iran's constant monitoring and restriction of Internet access.

What has changed is not the fundamental properties of information or communication. Rather, the information environment itself has dramatically evolved. The properties of scarcity, asymmetry, and friction have been replaced by ubiquity, symmetry, and simultaneity. These new properties describe an information environment altogether different from our classical model.

UBIQUITY, SYMMETRY, SIMULTANEITY, AND SECURITY

In an environment defined by informational ubiquity, information is no longer expensive or resource intensive to gather and maintain. Digital communication through the EM domain is cheap, nearly approaching universal, and can transfer lots of data very quickly. Storage continues to increase in density and decrease in price, while search engines or other methods of parsing data are increasingly capable and refined. Informational symmetry means that we all have access to roughly the same data and datasets. Simultaneity ensures that the time lag due to geography is negligible; information is no longer geospatially constrained. While that information may need to be parsed into something usable, it is still accessible worldwide via the EM domain.

Importantly, none of this would be possible without the physical properties of the EM domain. Because the EM domain exists all around us, as long as we have access to it we function in the modern, nonclassical, information environment of ubiquity, symmetry, and simultaneity. In this context, IT becomes absolutely necessary to any state or other entity seeking any of the elements of power, because it allows *operation* in the EM domain. Without these IT tools, you cannot function in the new environment and are at a distinct disadvantage, a point Arquilla highlighted when discussing the lack of Iraq's effectiveness against U.S. and allied forces in Operation Desert Storm in 1990–1991.[12]

These new properties of the information environment raise serious questions about the validity of the information dominance model. Because information has become so cheap, having large volumes of it confers no inherent advantage over an adversary, who likely has access to a similar stockpile of information. Further, asymmetry and friction, be they natural or security driven, cannot be strategically relied on to maintain a favorable balance of informational power. We also have a new strategic need: to be constantly connected to the EM domain and its information or to suffer immediate and dire social, political, economic, and military consequences. Given these facts, information dominance cannot be an effective strategy for advancing state power on any front.[13]

The solution lies in advancing and extending Arquilla's, and the U.S. Navy's notion of operationalizing information. Information is only half of an equation that leads to "real-world" power: expertise, of all forms and kinds, is the other. In yet another irony, exercising the digital revolution for maximum benefit requires a strategic investment in people and their social constructs. Melding information and human knowledge together, using the modern information environment created by IT and the EM domain, yields a strategy we will call "cognitive dominance."

COGNITIVE DOMINANCE: PUTTING PEOPLE BACK IN SECURITY STRATEGY

Cognitive dominance differs from information dominance by making people and their expertise the centerpiece of its construct. Where information dominance focuses on information, IT, and security to create a decisional and thus a competitive advantage, cognitive dominance focuses on knowledge, people, and active resilience. Information dominance is rife with discussions of platforms, net-centric architecture, cyberattacks and other arcane matters of IT. Cognitive dominance posits that the IT capabilities already exist and are in use; just because some states and massive bureaucracies are having trouble adjusting to the new environment does not make it any less real or extant. Therefore, the strategic advantage lies not in IT or information but in the ability to operationalize the information—make it useful for decisions—faster, better, more accurately, more safely, and more consistently than the adversary. This can be achieved by improving your own organizational cognition or by degrading the adversaries' abilities to operate in the EM domain.

To execute cognitive dominance as a strategy, people and the social networks that they are a part of must be deeply connected; possess large bodies of expansive and specific expertise; demonstrate a high degree of individual and collective analytical intelligence; conquer multiple or quickly changing analytical challenges at once; be connected to the EM domain, and therefore, to each other at all times; and be able to recover from a localized or generalized catastrophe with minimal disruption. Given this, there are five components of cognitive dominance that must be pursued and developed:

1. *Cognitive depth*—Developed wells of useful and relevant knowledge, both explicit and in the form of expertise and experience, that are superior to the adversary's;

2. *Cognitive strength*—The ability to generate conclusions with greater accuracy and precision than the adversary;

3. *Cognitive agility*—The ability to bring the right information and the right expertise together more quickly than the adversary;

4. *Cognitive defense*—The passive and active ability to protect all parts of your cognitive cycle and its network[14] from disruption and exploitation; and

5. *Cognitive resilience*—The ability to effectively rebound from major losses, defeats, or other catastrophes.

In fairness, information dominance implies certain aspects of the above principles. However, it does not focus on, nor address, any of them completely. States, nonstate actors, and their apparatuses of power ignore cognitive dominance at their peril—the lack of Afghanistan and Iraq experts, be they linguists, anthropologists, historians, or civil affairs personnel in the U.S. military and intelligence community, for example, is well documented and has caused a great deal of concern and occasional difficulty in achieving even narrow goals.

There are also obvious, practical difficulties: Who is an expert? Where does that expert reside? Just how expert is this person, and what type of expertise does he or she they possess? How do I get in touch with that expert? Fortunately, modern IT does offer ways to tackle these problems efficiently and effectively. The U.S. intelligence community has taken the first steps toward this by implementing "Web 2.0" technologies such as wikis and social networking across its classified and unclassified systems. Because these tools link a unique identifier to an individual, "who knows what, and how well," is much simpler to establish than it ever has been before. But this is a far cry from adopting an overall coordinated and crisply executed strategy of cognitive dominance as a cornerstone of power.

COGNITIVE DOMINANCE IN INTEGRATED NETWORK ELECTRONIC WARFARE

While there are no perfect examples of cognitive dominance in the world today, at least one country is half running, half lurching in that direction: China. The Chinese government has relentlessly pursued a strategy of educating and training its populace while adopting and implementing modern IT. Information to truly confirm if China has implemented and successfully carried out cognitive dominance would likely go beyond openly available information. However, by its own open press reporting, China has appeared to set the right strategic context, and in some cases has examples of, the capabilities necessary to achieve cognitive dominance in electronic warfare.

China's strategic foundation is the premise that the electromagnetic spectrum is a war-fighting domain. Based on this premise, the Chinese have developed their concept of integrated network-electronic warfare (INEW). This concept is derived from a deep understanding and well-articulated strategic context that generates objectives, plans, and capabilities focused on creating a wide range of strategic and operational effects against their adversaries while at the same time defending against attack.

China learned how to operate successfully in a complex EM by studying U.S. operations in the first Gulf War.[15] China was also influenced by the observation that electronic warfare has evolved over the last one hundred years; as new ways to exploit the electromagnetic spectrum for operations were developed, so were the variety and scope of countermeasures.[16] China viewed U.S. electronic operations collectively as a system of sensors, connections, transport networks, processors, and controls that create effects within and across the electromagnetic domain. Shaped by their understanding of the progression of electronic warfare, they also realized that each element necessary for rapid and effective theater operations is also a key target. What China realized was needed was an integrated approach that goes from "the acquisition, forwarding, and control of information to the entire process of information flow, to include processing and exploitation."[17]

China's concept of INEW was first explained in an article by Major General Dai Qinqmin, then head of the People's Liberation Army (PLA) Fourth Department. INEW is a seamless integration of electronic warfare and computer network warfare to disrupt an adversary's information systems while protecting one's own systems. Computer network warfare targets network layers where information is processed and where humans gather information to make decisions. Electronic warfare targets the networked systems themselves as well as "informationalized" weapons, which rely on electronics to obtain the information that is necessary for them to function.[18]

Evident in public documents and within the media, China, with its strategic context defined, has set a steady and measured approach to achieve its strategy. The 2007 PLA training guidelines highlighted the need to be able to operate in a "complex electromagnetic environment."[19] China's 2008 Defense white paper again emphasized this need, stating "[t]he PLA is spreading basic knowledge of electromagnetic-spectrum and battlefield-electromagnetic environments, learning and mastering basic theories of information warfare, particularly electronic warfare."[20] The PLA is involved in exercising, too. As far back as 1999, Chinese military units were conducting exercises with elements of computer network warfare and electronic warfare.[21] Most recently, exercises in 2007 and 2009, in the Jinan and Nanjing military regions, were using "new tactics" including "hacker attacks and electromagnetic interference."

Guided by a well-defined and proper strategic context, China appears to be well on its way in setting the right objectives and plans and developing the right capabilities to operate offensively and defensively in the electromagnetic domain. Below is an assessment, based upon open source reporting, on how well China, framed in the context of information warfare, is prepared to carry out operations in cyberspace.

THE PEOPLE'S REPUBLIC OF CHINA (PRC) AND INEW

Information warfare can be defined as any operations directed at information in any form, stored and transmitted by any means, or operations directed at the entire physical and personnel infrastructure supporting the management of information. An information-based attack is one in which unauthorized users acquire, alter, or disrupt the flow of information.[22] With communications a critical component in the daily operations of individuals and organizations, stolen, altered, or untimely information is a serious concern.

China is conducting information warfare through an active offense utilizing cyber reconnaissance and computer network exploitation activities. Facilitated by a large pool of technologically savvy military and private citizen hackers, ubiquitous information technology resources, and access to malware, and supported by a stratified training and education plan, China has developed a strong "cyber workforce" to carry out its information warfare operations. China believes these operations are necessary in order to maintain information and knowledge superiority and bolster economic and military advantage.

The assessment below, also known as a Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities analysis, commonly used by military planners, provides a brief discussion of China's information warfare doctrine.

Doctrine

China's doctrine, or what it calls "rules and regulations," is not something freely shared. It does not publish unclassified doctrine on the Internet as the United States and other nations do. However, through a review of open source reporting and comments from China and its PLA, the thought and strategy (the "why") behind China's use of information warfare can be understood.[23] A review of open source material on Chinese theory by Timothy Thomas, an analyst at the Foreign Military Studies Office at Fort Leavenworth, Kansas, and Toshi Yoshihara, a professor in the Strategy and Policy Department at the Naval War College in Newport, Rhode Island, shows that China believes critical components of its national strength will come from the ability to be an economic power and successfully conduct information warfare. The tools to conduct this warfare are an active offense utilizing cyber reconnaissance and computer network exploitation activities to bolster its economic and military advantage.

The U.S.'s use of high technology in Iraq, Afghanistan, and Kosovo has actually helped to change China's historic view of defense to a belief that only those forces that establish information superiority will win.[24] A 2000 article in *China Military Science* highlights the need for an active offense in order to maintain information control and provide an advantage over a superior force. The article also states that offensive information can be used to sabotage an opponent's information systems.[25]

Cyber reconnaissance is a key component of an active offense. This reconnaissance is necessary to map an adversary's commercial, weapons, and critical infrastructure networks to identify vulnerabilities or leave behind "back doors" and other control mechanisms. Under Chinese doctrine, in advance of a kinetic conflict, the electric grid and other commercial, critical infrastructure, and weapons networks will be attacked.

The second component to an active offense is the use of computer network exploitation to steal information. Military information gives China the ability to build weapons systems comparable to the United States or to develop appropriate defenses. This information also hastens China's development of the right military organization required to effectively attack or defend itself in a major conflict. Gaining economic information, such as intellectual property, means that China does not have to spend years and dollars on research and development. Thus, China can produce the same high-quality products as the United States and other countries but at a much lower price. Computer network exploitation gives China the tool it needs to seek the right information to provide a military and economic advantage.[26]

Organization

Two main components in China carry out information warfare. The first is the PLA, including the reserve force. The second is private citizens, including "gray hat" hackers or those motivated by patriotism.

The PLA is China's unified military organization. It is comprised of the army, navy, air force, second artillery force (nuclear forces), the armed police force, and reserve forces.[27] Although China's White Paper on National Defense does not specifically call out a separate information warfare or cyber force, a review of several articles from China (as far back as 1999) talk of creating offensive and defensive "computer confrontation forces" to carry out and defend against cyber attacks. In 2000, the journal *Guangjiao Jing* stated the PLA had established information warfare departments in its headquarters organizations. More recently, articles from 2003 indicate that specialized information warfare units would be set up within all PLA armies, including reserve forces.[28]

There are over 250 hacker groups in China. These hacker groups embody China's concept of the "people's war," leveraging the citizens to conduct cyber attacks against the nation's adversaries. These groups, made up of private citizens, provide the PLA and Chinese government additional capability but no blame or responsibility for the attacks.[29]

Training

Training is how an organization prepares to fight. The PLA accomplishes this task by incorporating information warfare components in its military exercises. There is no information on how, or if, private citizen "gray hats" and patriotic hackers conduct exercises to support their cyber activities.

There are several examples of the PLA incorporating information warfare components into its exercises. In November 2000, two army teams in the Beijing Military Region conducted a "confrontation campaign" on a computer network.[30] The Chengdu Military Region conducted a similar exercise the same year.[31] And lastly, exercises in the Jinan Military Region in 2007 and the Shenyang and Nanjing Military Regions in 2009 utilized hacking techniques.[32] These exercises were not limited to specific PLA components and included an electronic warfare regiment, air force command post, and an armored regiment.

Materiel

Successful information warfare, specifically computer network operations, requires the right malicious software, known as malware, and the right network access. Malware and network access are not necessarily unique. The hardware and software required to conduct computer network operations is available in the United States and in China. The difference is in the individual malware exploits developed and how they are used.

There are several types of malware, including worms, viruses, trojans, and hacker utilities. Worms are malicious codes that spread via local area networks and always cause at least some harm even if only reducing bandwidth. Generally worms spread as files in email attachments, through chat programs, as links to infected web sites, and through peer-to-peer file-sharing services. Viruses are a form of malware that copy and spread throughout a single machine to carry out a specific action against that machine. Trojans may be the most useful of the malware set. These programs perform certain actions, such as collecting data and sending them to another host, destroying or altering data, causing a computer to malfunction, or even "hi-jacking" a machine to be used later as part of a denial-of-service attack. Hacker utilities refer to a broad collection of tools such as programs to construct malicious software, malware program libraries, and any other programs designed to damage or disrupt a user's machine.[33]

The malware program libraries are important. The availability of these libraries makes the materiel necessary to conduct computer network operations available to a wide range of people quickly. In fact, a January 2009 report on badware (spyware, malware, or deceptive adware) web sites showed that China hosted 48 percent of these sites on the Internet. This is more than double its closest competitor, the United States, which had 21 percent of the badware sites.[34] While this report does not distinguish between the types of malware on Chinese sites, it is an example of the prevalence of the malicious software available.

Leadership and Education

The PLA's information warfare training and education is set by age group. The first group is the decisionmakers, those over age forty. The focus for this group is to make senior leaders literate in information technology and to understand the value of this new type of warfare. Midlevel leaders, ages thirty to forty, represent the future leaders of the organization. The focus for this group is on the skills and knowledge necessary for information warfare command. Personnel aged thirty or less represent the last group. These individuals are already technologically savvy. Their training and education focus on advanced information technology concepts and command skills.[35]

In order to conduct this training and education, the PLA set up several information warfare focused universities such as the Communications Command Academy in Wuhan, the Information Engineering University in Zhengzhou, the Science and Engineering University, the National Defense Science and Technology University in Changsha, and a PLA Navy Engineering College.[36]

Personnel

These individuals can be part of the military, active or reserve, or private citizens. With 729 million people available for military service and a general population of over 1.3 billion, China indeed has a large pool of potential information warfare personnel.[37] But these individuals need to be qualified. They should be technologically savvy and have a good background in math, engineering, or computer science.

There are no statistics detailing the number of personnel in China's "cyber force." However, there are data suggesting that China produces a large number of the type of individuals suited to conducting information warfare, a number significantly greater than the United States. According to a 2007 report on education, 50 percent of all undergraduates receive degrees in natural science or engineering. In the United States, it is 27 percent. In 2004, it is estimated that China graduated 650,000 engineers, computer scientists, and information technologists with either a three- or four-year degree. During that same period the United States only graduated 225,000.[38] This represents a considerable amount of Chinese people well suited to conduct information wafare activities.

Facilities

The facilities necessary to support China's information warfare activities include offices and labs owned and operated by the government, military, academia, industry, and even private homes. In conducting cyber operations, both the development of malware and hacker tools and the carrying out of attacks themselves, the physical location and facility support are not important. A computer and network access are the basic requirements.

As information technology becomes more ubiquitous, the "places" that can be used to train, prepare, and conduct information warfare operations will grow. Malware, for instance, can be produced on any personal computer and, while computer labs may offer better and safer computer resources to build malicious code, this is not a requirement. Network access is also a key factor. In order to conduct successful information warfare, access to the "net" is required. China's access to the Internet grew over 1,200 percent between 2000 and 2008, and China currently has about one-fifth of all Internet users (approximately three hundred million).[39] This access, wired or wireless, represents a lot of potential attack origination points.

CHINESE COGNITIVE DOMINANCE STRATEGY IN INEW

The above analysis shows that the Chinese government has correctly marshaled its resources, including its human talent, to develop cognitive dominance in the realm of INEW. The Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities analysis and stated goals of the Chinese military link directly to five cognitive dominance principles, as defined in Table 1.

ADAPT OR DIE

While China has explicitly laid out its strategy in terms of conflict and information warfare, it is executing this strategy via cognitive dominance. It is training its population to be experts in INEW and ensuring that the cycle and systems whereby that knowledge and experience is translated into effective action are never disrupted in quality, speed, or mass. China moved well beyond information dominance by trying to maximize not the amount of information flowing through its pipelines and into its databases but by the ability to create, distribute, maintain, identify, and connect collective expertise in INEW.

To be clear, China's strategy of cognitive dominance is not limited to military conflict. Rather, it is exercising its INEW capabilities across the entire range of its interests in a bid for increased power. China's economic espionage, for instance, is an open secret. Of the 108 countries attempting espionage on proprietary U.S. technology, China and Russia topped the list.[40] A 2008 article from the *National Journal* reported that one large U.S. company (which remained unnamed for obvious reasons), realized its negotiating strategies—stored on company networks—had been compromised when its Chinese counterparts knew the company's bottom line on every negotiating point. Similarly, another company noted that at its negotiations with the Chinese, the delegation "based their starting points for negotiation on the Americans' end points."[41]

In an example more directly linked to "hard power," between 2002 and 2006 several attacks believed to have originated in China were conducted against multiple National Aeronautics and Space Administration (NASA) facilities and its headquarters. In 2002, rocket design information was stolen from the network of the Marshall Space Flight Center in Huntsville, Alabama. In 2005, in what is believed to have been the most serious attack, infor-

Table 1.

Cognitive Dominance	Chinese Actions
Cognitive Depth—Developed wells of useful and relevant knowledge, both explicit, and in the form of expertise and experience that are superior to the adversary's.	Investment in skilled/educated population. Training of leadership echelons. Creation of malware repositories.
Cognitive Strength—The ability to generate conclusions with greater accuracy and precision than the adversary.	Creation of truly expert hackers. Successful INEW attacks/exercises. Cyber-reconnaisance/espionage.
Cognitive Agility—The ability to bring the right information and the right expertise together more quickly than the adversary.	Massive investment in Internet access. Encouragement of "gray hat" ethos/community.
Cognitive Defense—The passive and active ability to protect all parts of your cognitive cycle and its network from disruption and exploitation.	Significant monitoring/security in place. "Cyber confrontation" incorporated into PLA training.
Cognitive Resilience—The ability to effectively rebound from major losses, defeats, or other catastrophes.	Wide pool of possible talent. Wide pool of extant INEW warriors. Distributed Internet access nodes.

mation that could help build, fly, or sabotage a space shuttle was stolen from the Johnson and Kennedy Space Centers. The investigation into this incident suggests the information ended up in mainland China. In another breach at the Johnson facility, evidence pointed toward one of NASA's contractor's network, Lockheed Martin, as the gateway into the NASA systems.[42]

This was not just an attack on NASA; every partner that NASA has its network connected to is a gateway into its systems, and vice versa. The Chinese attacks effectively breached the partner networks as well. The amount of information that the Chinese gleaned about the science, technology, and engineering involved in space flight could easily be applied not only to its own space program or "spin-off" industries but obviously to military hardware as well.

While these may seem like fairly innocuous examples of how China has employed its INEW capability, three points must be raised. First, the reason these attacks were relatively harmless is because the United States is not at war with China; the same INEW capabilities could be used in a state-on-state conflict, potentially crippling enemy warfighters. The U.S. way of war, for instance, emphasizes mobility and maneuver, made possible by advanced technology and communications systems—all of which are ripe targets for INEW. Second, these hacking-style attacks allow the Chinese formal and informal army of experts the opportunity to hone their skills and practice their craft. Third, these acts of espionage are the direct result of a coordinated national strategy to create and gain cognitive dominance within the EM domain. Each attack demonstrated that the Chinese, through national investment, had created the ability to "out-think" their adversaries at the strategic level, creating accurate and precise decisions before their rivals even had a chance to orient themselves.

Emphatically, the point of these examples is not to cast China as the next bogeyman for U.S. national strategy. The authors of this paper, in fact, emphatically disagree with casting China as a grave threat to the safety and security of the United States. Instead, the INEW and EM domain expertise China has developed should be seen as driving home the central theme of cognitive dominance: Because IT and informational disparity is rapidly diminishing around the world, they can offer no strategic advantage. They are necessary as a "cost of business," and you will lose without them, but they are not decisive or advantageous in and of themselves. Therefore, the modern information environment requires not just information and the tools to process and deliver it but also the individual and collective ability of people to "think and act better and faster" than the enemy. And because only people can think (for now), China has invested massive amounts of resources in the people it is educating and training as part of its strategy.

Whether the Chinese think of their strategy as cognitive dominance is of course immaterial; what is important is that the actions of the Chinese government demonstrate a clear understanding of the modern information environment, using the principles this paper outlines. They have successfully delivered tremendous INEW and EM domain capabilities, creating tangible decisional improvements, and in some cases, superiority.

The implications of the modern information environment, and its impact on security and stability, cannot be ignored. Poorer regions of the world have already "leapfrogged" over expensive legacy or intermediate infrastructure and technology, expanding both the regions and sources of informational transparency and the access to the EM domain. Properly leveraged, these represent cheap sources of strategic power. Self-organizing groups of "digital natives"—people born almost literally with a mobile device in their hand—effectively used modern IT and its access to the EM domain to challenge, destabilize, and bring down regimes in the Arab Spring. It is both easy and reasonable to envision such uprisings elsewhere.

Given the above facts, informational ubiquity, symmetry, and simultaneity are not normative; they do not favor any party over another. Rather, they are facts of the "terrain of power." Those who use the terrain properly will gain an advantage over potential threats and adversaries. Those who do not will find their position compromised. Information dominance, unfortunately for the United States, does not take full advantage of today's information environment. But, as China demonstrates, cognitive dominance does and provides with it the competitive edge that states seek in power transactions.

ENDNOTES

1. John Arquilla, "The Strategic Implications of Information Dominance" (Monterey, CA: Naval Postgraduate School, 1994). http://www.nps.edu/academics/Centers/IOCenter/docs/publications/The%20Strategic%20Implications%20of%20Information%20Dominance.pdf

2. Office of the Director of National Intelligence, "Vision 2015" (Washington, DC: July 2008), p. 6. http://www.dni.gov/Vision_2015.pdf.

3. "The U.S. Navy's Vision for Information" (May 2010), p. 4. http://www.insaonline.org/assets/files/NavyInformationDominanceVisionMay2010.pdf.

4. Ibid., p. 3.

5. In this case, the "web" refers to all the connection equipment, devices, content, etc. that exist in a digital context and are connected to each other. It is not just web pages, websites, and so forth.

6. Arquilla, "The Strategic Implications," p. 25.

7. http://pubs.aeaweb.org/doi/pdf/10.1257/jep.24.3.207.

8. UC Newsroom, "How much information do we consume?" (University of California: December 9, 2009). http://www.universityofcalifornia.edu/news/article/22528.

9. *Science Daily*, "How Much Information Is There in the World?" February 11, 2011. http://www.sciencedaily.com/releases/2011/02/110210141219.htm.

10. This transparency is far from complete, but it is a windowpane compared to the past.

11. CNN World, "Neda becomes rallying cry for Iranian protests," June 21, 2009. http://articles.cnn.com/2009-06-21/world/iran.woman.twitter_1_neda-peaceful-protest-cell-phone?_s=PM:WORLD.

12. Arquilla, "The Strategic Implications."

13. This is distinct from tactical maneuvers on the battlefield, in diplomacy, economic exchange, etc. At the tactical level, the time lag between when you and an adversary know something can be exploited to dramatic effect. Information dominance could also be a "strategy," when facing a far inferior adversary with poor EM domain presence. However, it is likely that an adversary of that nature is going to lose anyway.

14. Network is inclusive of the IT tools that enable networking, and the social network itself.

15. Toshi Yoshihara, "Chinese Information Warfare: A Phantom Menace or Emerging Threat?" (Carlisle Barracks, PA: U.S. Army War College, Strategic Studies Institute, November 2001). http://www.au.af.mil/au/awc/awcgate/ssi/chininfo.pdf.

16. Dai Qingmin, "On Integrating Network Warfare and Electronic Warfare," *Beijing Zhongguo Junshi Kexue*, February 1, 2002, as translated and downloaded from the Open Source Center.

17. Ibid.

18. Timothy L. Thomas, "Chinese and American Network Warfare," *Joint Forces Quarterly* 3rd Qtr: 38 (July 2005): 77.

19. Michael S. Chase, "China's 2007 Military Training Guidelines and the PLA's Evolving Approach to Military Training," *China Brief* 7: 12 (June 13, 2007) (Washington, DC: The Jamestown Foundation). http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews%5Btt_news%5D=4227&tx_ttnews%5BbackPid%5D=197&no_cache=1.

20. China.org.cn, "White paper on national defense published," 2009. http://www.china.org.cn/government/central_government/2009-01/20/content_17155577.htm.

21. Yan Hong and Zhou Meng, "Beijing Military Region Conducts Computer Exercise," *Beijing Jiefangjun Bao*, April 8, 2000, as translated and downloaded from the Open Source Center.

22. Clay Wilson. "Information Warfare and Cyberwar: Capabilities and Related Policy Issues: RL31787" (Washington, DC: Congressional Research Service, 2004), p. 2.

23. Timothy L. Thomas, "China's Electronic Long-Range Reconnaissance," *Military Review* 88: 6 (November-December 2008): 53-54.

24. Thomas, "China's Electronic Long-Range Reconnaissance," p. 48.

25. Ibid., p. 49.

26. Thomas, "China's Electronic Long-Range Reconnaissance," p. 53; Yoshihara, "Chinese Information Warfare," p. 6.

27. China.org.cn, "White paper on national defense published."

28. Thomas, "China's Electronic Long-Range Reconnaissance," pp. 48–51.

29. Ibid., p. 53.

30. Hong and Meng, "Beijing Military Region Conducts Computer Exercise."

31. Xu Wenliang and Wan Yuan, "Chengdu MR [Military Region] Conducts Confrontational Exercise on Internet," *Beijing Jiefangjun Bao* (Internet Version-WWW), July 10, 2000, as translated and downloaded from the Open Source Center.

32. An Chenguang, "PRC [People's Republic of China]: Jinan Military Region Electronic Warfare Regiment Adds 'Hacking' to Tactics," *Jinan Qianwei Bao*, May 25, 2007; Li Jia and Wang Daqun, "PRC: Shenyan MR Air Force Command Post Executes 'Trojan Software' in Online Drill," *Beijing Kongjun Bao*, February 3, 2009; Mao

Xiuguo and Xiang Haoyu, "PRC: Nanjing MR Armored Regiment Improves Information Confrontation Capability," *Nanjing Renmin Qianxian*, February 11, 2009. All as translated and downloaded from the Open Source Center.

33. Viruslist.com, "Malicious Programs Descriptions."

34. stopBADware.org, ""Where's the badware?" http://blog.stopbadware.org/2009/03/03/wheres-the-badware.

35. Timothy L. Thomas. "Like Adding Wings to the Tiger: Chinese Information War Theory and Practice" (Fort Leavenworth, KS: U.S. Army Foreign Military Studies Office). http://fmso.leavenworth.army.mil/documents/chinaiw.htm.

36. Ibid.

37. *The World Factbook*, "Military China" (Langley, VA: Central Intelligence Agency). China, https://www.cia.gov/library/publications/the-world-factbook/geos/ch.html.

38. National Academy of Sciences, National Academy of Engineering, and Institute of Medicine, "Rising Above the Gathering Storm: Energizing and Employing America for a Brighter Economic Future" (Washington, DC: The National Academies Press, 2007), p. 16.

39. Information Warfare Monitor, "Tracking GhostNet: Investigating a Cyber Espionage Network" (Ontario, Canada: University of Toronto, Munk School of Global Affairs, March 29, 2009), p. 9. http://www.infowar-monitor.net/ghostnet.

40. Center for Strategic and International Studies, "Threats Posed by the Internet" (Washington, DC: CSIS Commission on Cybersecurity for the 44th Presidency, Threat Working Group, 2008), p. iii.

41. Shane Harris, "China's Cyber-Militia," *National Journal,* May 31, 2008.

42. Keith Epstein and Ben Elgin, "Network Security Breaches Plague NASA," Businessweek.com, November 20, 2008, under "Yanking Cables." http://www.businessweek.com/magazine/content/08_48/b4110072404167.htm.

About the Authors

Séverine Arsène was the 2011–2012 Yahoo! Fellow at the Institute for the Study of Diplomacy. She is the author of *Internet and Politics in China* (Karthala, 2011, France). As an expert on Internet governance and online mobilizations, Arsène has worked with Orange in Paris and in Beijing. She was previously an assistant lecturer at the University of Lille 3, France in the Department of Information and Communication where she taught courses on information technologies. Arsène holds a Ph.D. in political science from Sciences Po in Paris.

David M. Faris is an Assistant Professor of Political Science and Director of International Studies at Roosevelt University. He received his PhD in Political Science from the University of Pennsylvania in 2010. He is the author of *Dissent and Revolution in a Digital Age: Social Media, Blogging and Activism in Egypt* (forthcoming from IB Tauris and Co.). His research focuses on both global digital activism as well as the development of political institutions in the Middle East, and is currently in the process of completing projects on the growth of Iranian social media, the rise of digital diplomacy and digital inequality in the Middle East. His academic work has appeared in A*rab Media & Society*, *Middle East Policy*, *Politique etrangere*, as well as *The Routledge Participatory Cultures Handbook*. Faris also serves as a Strategy Group Advisor for the Meta-Activism Project (MAP), which seeks to build foundational knowledge about digital activism. He has published op-eds and features for the *Christian Science Monitor*, NPR.org, *The Daily News Egypt*, *The Philadelphia Citypaper*, *Sightings and Insights on Law and Society*.

Sarah Granger is the founder of the Center for Technology, Media & Society. She is also a Fellow at the Truman National Security Project, cochairing their cybersecurity group. She began her career working in cybersecurity for the Lawrence Livermore National Laboratory after graduating from the University of Michigan. She worked as a network security consultant for several years before becoming the Project Director for the Computer Professionals for Social Responsibility, where she served as a delegate to the World Summit on the Information Society at the U.N. in Geneva. Granger was a contributing author of *Ethical Hacking*, and she has edited books on mobile security, cryptography and biometrics. She currently blogs for *SFGate* and *The Huffington Post*. Other publishing credits include *Security Focus,WSJ.com*, *Forbes Russia*, and *IEEE Spectrum*. For more information, see sarahgranger.com.

Craig Hayden is an assistant professor in the International Communication Program at American University's School of International Service. His current research focuses on the discourse of public diplomacy, the rhetoric of foreign policy related to media technologies, as well as the impact of global media and media convergence on international relations. He is particularly interested in the comparative study of public diplomacy and media culture as a pivotal resource for international relations, as well as the impact of communication technology on international influence. Dr. Hayden received his Ph.D. from the Annenberg School of Communication at the University of Southern California. He is also the author of *The Rhetoric of Soft Power: Public Diplomacy in Global Contexts* (Lexington Books, 2012).

James Herlong is a forward-thinking, strategic intelligence and information technology leader and cyber strategy and security subject matter expert. Herlong has a comprehensive background including a wide range of national security and cyber issues. He has made notable contributions to homeland security developing the nation's first program to screen incoming merchant ship crew, passengers, and cargo for intelligence and law enforcement issues and the building of the Coast Guard Cyber Command. In 2004, Herlong was awarded the Admiral Frederick Billard award, the Coast Guard's top intelligence honor. Mr. Herlong is a graduate of the United States Coast Guard Academy, holds a Master of Science in Information Systems from the University of Baltimore, and a Master of Strategic Intelligence from the National Defense Intelligence College where he was the top Reserve graduate.

Gerald F. ("Jerry") Hyman has been Senior Advisor at the Center for Strategic and International Studies and the President of its Hills Program on Governance since 2007. From 2002 to 2007, he was the director of the U.S. Agency for International Development's Office of Democracy and Governance, a senior management position. Between 1990 and 2002, he held a number of posts at USAID dealing primarily with democracy and governance, including (from 2001 to 2002) a USAID Senior Management Group position as director of the Office of Democracy, Governance and Social Transitions in the Bureau for Europe and Eurasia. He developed the programming strategy paradigm for USAID democracy and governance assistance. From 1985 to 1990, he practiced corporate law at Covington & Burling in Washington, DC. Between 1970 and 1982, he taught in the Department of Sociology & Anthropology at Smith College. He also taught courses at Williams College. He holds a B.A. in Philosophy and a Ph.D. in Anthropology from the University of Chicago and a J.D. from the University of Virginia. He is the author of numerous articles and publications. He is a member of the Advisory Board of National Endowment for Democracy's Center for International Media Assistance and of the NED's Research Council of the its International Forum for Democratic Studies.

Lorelei Kelly is the founder or director of five projects in Washington, D.C. with the purpose of system-level change in information flows between Congress and American citizens. She joined the New America Foundation's Open Technology Institute to pilot Smart Congress—a decentralized system of expert knowledge and civic participation methods for the U.S. Congress. OTI's mission is to build an open and free global town square, enabled by twenty-first century communications technologies. Kelly is a civil–military expert, and part of her work at OTI looks at the impact of distributed power and the components of a security strategy for civil society. She attended Grinnell College. After living in Berlin while the Cold War ended, she taught Peace Studies at Stanford, moved to Washington, DC to work in Congress, and attended the

Air Command and Staff College of the U.S. Air Force. She is the co-author of two books, both free and available online.

Shanthi Kalathil is an international development consultant and adviser, focusing on the intersection between development, democracy and, international security. Kalathil is coauthor of *Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule*, a widely cited work that examined the Internet and political transition in eight authoritarian contexts. Over the past decade, Kalathil has advised the U.S. government, international organizations, and nonprofits on the policy and practical aspects of support for civil society, media, transparency and accountability as a function of democracy and good governance. Previously a Senior Democracy Fellow at the U.S. Agency for International Development and a regular consultant for the World Bank, she is currently an adjunct professor at the Monterey Institute of International Studies and codirector of the Institute's Colloquium on Evolving Global Security Challenges. She has authored numerous policy and scholarly publications, including the recent *Developing Independent Media as an Institution of Accountable Governance*, published by the World Bank. A former Hong Kong-based staff reporter for the *Wall Street Journal Asia*, Kalathil is a member of the Advisory Board for the National Endowment for Democracy's Center for International Media Assistance.

Andrew Puddephatt is a founding Director of Global Partners & Associates (www.globalpartners.co.uk). He has worked to promote human rights for twenty years and has specific expertise in freedom of expression, transparency, the role of media and digital communications in society, and implementing human rights. He is currently managing projects in Brazil, Egypt, the United States, Iraq and China. Puddephatt has played a leading role in securing a Bill of Rights for the United Kingdom and in January 2003 was awarded an OBE for services to human rights. He holds several Board positions in the non-profit and public sector: he is Chair of Danish-based International Media Support, a Danish based NGO that provides emergency support to journalists in conflict areas; the Deputy Chair of the Sigrid Rausing Trust; and he is on the board of the European Council for Foreign Relations.

Andrew has led human rights organisations in the not-for-profit sector for more than fifteen years. Previous to founding Global Partners he was Executive Director of ARTICLE 19, a pioneering organisation working on freedom of expression from 1999 to 2004. As Executive Director, Andrew led the organisation and was responsible for the strategy, management and policy direction.

Joseph Siegle is a Senior Research Scholar at the Center for International and Security Studies at Maryland (CISSM) and the Director of Research at the African Center for Strategic Studies at the National Defense University. Siegle has written widely on the political economy of democratic transitions, stabilizing fragile states, and establishing institutions of accountability, including the coauthored work, *The Democracy Advantage: How Democracies Promote Prosperity and Peace* (Routledge, revised edition 2010). His background combines policy analysis, academic research, and field practitioner experience from over 40 countries, including numerous stabilization, postconflict reconstruction, and fragile state contexts. Previously, Siegle has held positions as Douglas Dillon Fellow at the Council on Foreign Relations, a Senior Advisor for Democratic Governance at the international consulting firm, DAI, and a Country Director with the international NGO, World Vision. Dr. Siegle earned a Ph.D. from the University of Maryland's School of Public Policy and a M.A. in Agricultural Economics from Michigan State University.

James Valentine is currently the Chief of Intelligence for U.S. Coast Guard District 11. Previous tours include the Maritime Intelligence Fusion Center Pacific, in Alameda, California, the Coast Guard Intelligence Coordination Center, Coast Guard Headquarters, and the USCG cutter SHERMAN. He is a 2005 graduate of the Joint Military Intelligence College (now the National Intelligence University), and holds a Master's Degree in Strategic Intelligence. He earned his B.S. in Government, emphasis International Affairs, at the U.S. Coast Guard Academy in 1997. He has published two articles on the implications of information technology on cognition and warfare, and holds a Black Belt in Brazilian Jiu Jitsu.

Board of Directors

Institute for the Study of Diplomacy
1316 36th Street NW
Washington, DC 20007

Telephone: 202-965-6612
Web: http://isd.georgetown.edu

Diplomacy, Development, and Security in the Information Age

There is far more to understand about international relations in what is commonly termed the information age. Changes in the speed, volume diversity, nature and accessibility of information, as well as the ways in which it is exchanged, have contributed to a variety of emerging and evolving phenomena. These include the rise of non-traditional security threats (cyber and otherwise); networked forms of organization; asymmetrical conflict; decentralization; recentralization; altered global governance structures; multicentrism; information asymmetry; new development models; contested global norms; and much more. All of these present challenges and opportunities for states and nonstate actors, and require a substantial rethink of the lens through which we view international affairs.

Taken as a whole, the papers in this series give rise to several broad suggestions for policymakers and practitioners of foreign policy.

- To better understand and devise solutions for the information age, do not lead with technology.
- Transparency and volatility are inherently difficult for large bureaucracies but promise opportunities for innovation in statecraft and other areas.
- While transparency and volatility can have positive impacts, they also may be manipulated to suit various actors' aims.
- To harness opportunities . . . states and nonstate actors alike should focus on a strategy of resilience, credibility, and adaptability.

georgetown university school of foreign service   institute for the study of diplomacy