Sensing and Shaping Emerging Conflicts: Report of a Joint Workshop of the National Academy of Engineering and the United States Institute of Peace: Roundtable on Technology, Science, and Peacebuilding

ISBN
978-0-309-28611-4

68 pages
6 x 9
PAPERBACK (2013)

Andrew Robertson and Steve Olson, Rapporteurs; National Academy of Engineering; United States Institute of Peace

SENSING AND SHAPING EMERGING CONFLICTS

Report of a Workshop by the
National Academy of Engineering and United States Institute of Peace
Roundtable on Technology, Science, and Peacebuilding

Andrew Robertson and Steve Olson, *Rapporteurs*

NATIONAL ACADEMY OF ENGINEERING
OF THE NATIONAL ACADEMIES

UNITED STATES INSTITUTE OF PEACE

THE NATIONAL ACADEMIES PRESS
Washington, D.C.
www.nap.edu

THE NATIONAL ACADEMIES PRESS 500 Fifth Street, NW Washington, DC 20001

The Roundtable on Technology, Science, and Peacebuilding, the sponsor of the workshop on which this report is based, is supported by funding from the U.S. Department of Defense (JDDM-3663-1), Qualcomm, National Science Foundation (ENG-1136841), U.S. Department of Agriculture (59-0790-2-058), U.S. Department of State, and CRDF Global. Any opinions, findings, or conclusions expressed in this publication are those of the workshop participants.

International Standard Book Number-13: 978-0-309-28611-4
International Standard Book Number-10: 0-309-28611-5

Copies of this report are available from the National Academies Press, 500 Fifth Street NW, Keck 360, Washington, DC 20001; (888) 624-8373 or (202) 334-3313; online at www.nap.edu.

For more information about the National Academy of Engineering, visit the NAE home page at www.nae.edu.

Printed in the United States of America

THE NATIONAL ACADEMIES

Advisers to the Nation on Science, Engineering, and Medicine

The **National Academy of Sciences** is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. Upon the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Ralph J. Cicerone is president of the National Academy of Sciences.

The **National Academy of Engineering** was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. Charles M. Vest is president of the National Academy of Engineering.

The **Institute of Medicine** was established in 1970 by the National Academy of Sciences to secure the services of eminent members of appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government and, upon its own initiative, to identify issues of medical care, research, and education. Dr. Harvey V. Fineberg is president of the Institute of Medicine.

The **National Research Council** was organized by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both Academies and the Institute of Medicine. Dr. Ralph J. Cicerone and Dr. Charles M. Vest are chair and vice chair, respectively, of the National Research Council.

www.national-academies.org

UNITED STATES INSTITUTE OF PEACE
Center of Innovation for Science, Technology, & Peacebuilding

The United States Institute of Peace is the global conflict management center for the United States. Created by Congress in 1984 to be independent and nonpartisan, the Institute works to prevent, mitigate, and resolve international conflict through nonviolent means. USIP operates in the world's most challenging conflict zones, and it leads in professional conflict management and peacebuilding by applying innovative tools, convening experts and stakeholders, supporting policymakers, and providing public education. The Institute translates its on-the-ground experience into knowledge, skills, and resources for policymakers, the US military, government and civilian leaders, nongovernmental organizations, practitioners, and citizens both here and abroad.

The Institute's permanent headquarters and conference center are located at the northwest corner of the National Mall in Washington, DC. The facility also houses the Academy for International Conflict Management and Peacebuilding and the Global Peacebuilding Center.

www.usip.org

WORKSHOP STEERING COMMITTEE

Prabhakar Raghavan (*Cochair*), Vice President of Engineering, Google
Lawrence Woocher (*Cochair*), Research Director, Science Applications International Corporation
Dennis King, Senior Humanitarian Affairs Analyst, Humanitarian Information Unit, US Department of State
Neil Levine, Director, Office of Conflict Management and Mitigation, US Agency for International Development
Patrick Vinck, Research Scientist, Department of Global Health and Population, Harvard Humanitarian Initiative
Duncan Watts, Principal Researcher, Microsoft Research

Staff

Genève Bergeron, Research Assistant, US Institute of Peace
Sheldon Himelfarb, Director, US Institute of Peace
Greg Pearson, Senior Program Officer, National Academy of Engineering
Proctor P. Reid, Director, NAE Program Office
Andrew Robertson, Senior Program Officer, US Institute of Peace
Frederick S. Tipson, Special Advisor, US Institute of Peace

Acknowledgments

This summary has been reviewed in draft form by individuals chosen for their diverse perspectives and technical expertise, in accordance with procedures approved by the National Academies. The purpose of the independent review is to provide candid and critical comments to assist the NAE in making its published report as sound as possible and to ensure that the report meets institutional standards for objectivity, evidence, and responsiveness to the study charge. The review comments and draft manuscript remain confidential to protect the integrity of the deliberative process. We thank the following individuals for their review of this report:

Dennis King, Senior Humanitarian Affairs Analyst, Humanitarian Information Unit, US Department of State
Jason Matheny, Program Manager, Open Source Indicators Program, Intelligence Advanced Research Projects Activity
Joseph Bock, Director of Global Health Training, Eck Institute for Global Health, Notre Dame University
Rita Grossman-Vermaas, Senior International Policy Advisor, Logos Technologies Inc.
Patrick Meier, Director of Social Innovation, Qatar Computing Research Group
Sharon Morris, Director, Conflict Management Group, Mercy Corps

Although the reviewers listed above provided many constructive comments and suggestions, they were not asked to endorse the views expressed in the report, nor did they see the final draft of the report before its release. The review of this report was overseen by Venkatesh (Venky) Narayanamurti, Benjamin Peirce Professor of Technology and Public Policy, Harvard School of Engineering and Applied Science, and director, Science, Technology and Public Policy Program, Harvard Kennedy School. Appointed by NAE, he was responsible for making certain that an independent examination of this report was carried out in accordance with institutional procedures and that all review comments were carefully considered. Responsibility for the final content of this report rests entirely with the authors and NAE.

Contents

Appendixes

1

Introduction and Themes

Technology has revolutionized many aspects of modern life, from how businesses operate, to how people get information, to how countries wage war. Certain technologies in particular, including not only cell phones and the Internet but also satellites, drones, and sensors of various kinds, are transforming the work of mitigating conflict and building peaceful societies.

Rapid increases in the capabilities and availability of digital technologies have put powerful communications devices in the hands of most of the world's population. These technologies enable one-to-one and one-to-many flows of information, connecting people in conflict settings to individuals and groups outside those settings and, conversely, linking humanitarian organizations to people threatened by violence. Communications within groups have also intensified and diversified as the group members use new technologies to exchange text, images, video, and audio. Monitoring and analysis of the flow and content of this information can yield insights into how violence can be prevented or mitigated. In this way technologies and the resulting information can be used to detect and analyze, or *sense*, impending conflict or developments in ongoing conflict.

On October 11, 2012, the National Academy of Engineering (NAE) and the United States Institute of Peace (USIP) held a workshop in Washington, DC, to identify "major opportunities and impediments to providing better real-time information to actors directly involved in situations that could lead

to deadly violence." The workshop brought together experts in technology, experts in peacebuilding, and people who have worked at the intersections of those two fields on the applications of technology in conflict settings, to consider uses of technology to sense emerging and ongoing conflicts and provide information and analyses that can be used to prevent violent and deadly conflict. As Fred Tipson, special advisor to the Roundtable on Technology, Science, and Peacebuilding (see Box 1-1), asked in his opening

Box 1-1
Roundtable on Science, Technology, and Peacebuilding

The Workshop on Sensing and Shaping Emerging Conflicts was the third of four workshops convened by the Roundtable on Science, Technology, and Peacebuilding. A joint initiative of the National Academy of Engineering and the US Institute of Peace, the roundtable consists of senior executives and experts from government agencies, universities, corporations, and nongovernmental organizations (NGOs). It was established in 2011 to make a measurable and positive impact on conflict management, peacebuilding, and security capabilities by bringing together leaders from the technical and peacebuilding communities. Its principal goals are:

1. To accelerate the application of science and technology to the process of peacebuilding and stabilization;
2. To promote systematic, high-level communication between peacebuilding and technical organizations on the problems faced and the technical capabilities required for successful peacebuilding; and
3. To collaborate in applying new science and technology to the most pressing challenges faced by local and international peacebuilders working in conflict zones.

The first workshop concerned ways to augment agricultural extension systems to serve the purposes of peacebuilding. The second was on enhancing the ability of actors in the peacebuilding community to share information in the interest of solving common problems.[a] The fourth workshop will be on harnessing systems methods to think more systematically and holistically about peacebuilding problems.

[a] Summaries of the workshops are available on the NAE website, http://www.nae.edu/publications.aspx, and at the USIP website, http://www.usip.org/publications-tools (May 14, 2013).

remarks, "Where are the opportunities, the sweet spots, in developing not only the concepts and applications of the technology but the strategies by which the information arrived at can be applied for the purposes of intervening to shape the conflict itself?"

THE ROLE OF INFORMATION IN SENSING AND SHAPING CONFLICT

The application of technology to many problems, including sensing and shaping conflict, has generally followed a simple three-step template, said workshop cochair Prabhakar Raghavan, vice president of engineering at Google. The first step is the gathering of information. The second is large-scale analysis of the data, a science that is still being developed. The third step is conversion of the insights that result from analysis into actionable information and transmission of that information to operators and actors in the field. This broad paradigm may sound too generic, said Raghavan, but it has actually served the field well in maintaining certain critical distinctions.

Consideration of the roles that technologies can play in sensing and shaping emerging conflict is complicated by the great breadth of activities encompassed by both "technology" and "peacebuilding," said Lawrence Woocher, a research director at Science Applications International Corporation (SAIC) and the other workshop cochair. Peacebuilding involves political, diplomatic, social, economic, legal, and security activities. It can be undertaken by individual actors, local groups, national groups, international organizations, and the private sector. It is not just the absence of violence but includes aspects of positive attributes such as freedom and justice. (Box 1-2 provides a perspective on the many capabilities encompassed by the term "technology.")

Notwithstanding this diversity, Woocher identified several common elements of information used to support peacebuilding. First, it includes (or enables) a broad assessment of the relative risks of the outbreak or escalation of violent conflict. Such information can be critical for actors engaged in peacebuilding, whether they are working globally to identify regions or countries that are at greatest risk or locally to identify which neighborhood, county, or province in a country is susceptible to conflict.

Second, information for peacebuilding contains or implies some form of conflict analysis. In its most useful form, such an analysis yields insight about the roots of a conflict. Who are the actors and groups involved? What

Box 1-2
From the World Wide Web to Google Earth

Dennis King, a senior humanitarian affairs analyst with the Humanitarian Information Unit of the US Department of State, provided a personal perspective on the important changes in technology that have occurred over the past two decades. In the mid-1990s, when he was working for the US Agency for International Development, USIP mounted an initiative known as *Virtual Diplomacy* driven, in part, by the question of why the 1994 genocide in Rwanda was not anticipated. At that time, two new technologies had just become available: the World Wide Web and civilian access to high-resolution satellite imagery. The Virtual Diplomacy initiative was designed to explore the degree to which these and other technologies could influence peacebuilding, conflict prevention, and early warning about conflicts.

Since then, Web 1.0, which was based on mostly static websites, has evolved to the more interactive Web 2.0 and then to the 3.0 Web of social media, blogs, wikis, and other innovations. At the same time, low-cost, portable handheld devices have moved computers from offices to the field, inaugurating an era of truly personal and omnipresent computing and communications. Another major change, said King, was the release in 2005 of Google Earth, which helped break the government monopoly on high-resolution satellite imagery.

Other changes have been institutional and cultural. In the 1990s, most of the people in government agencies who took an interest in technologies were what King termed "geek bureaucrats" who were somewhat marginalized in their organizations. Since then, a thriving virtual community has emerged of people who are focused on these issues and on putting technologies to work.

One thing, however, remains the same as in the 1990s, King said. The central problem is not one of technology but of political will (an issue discussed in chapter 5). "Political will is not an icon on your computer screen," King said. "Generating political will is the missing factor in peacebuilding and conflict resolution." Even in the Rwanda case, Rwandan nationals had communicated to outsiders that genocide was being planned. The international community simply lacked the political will to act.

are their interests, capabilities, and motives? What are the broad trends and contextual factors that affect the conflict?

The third common element involves communication of the information to the relevant actors—national governments, international organizations,

community groups, and other stakeholders. However, local groups may not have the kinds of electronic networks available elsewhere, they may have low levels of technological literacy, they may distrust the sources, and—most importantly—they may have motives and agendas that are not peaceful or constructive. We cannot assume that only providing more timely, accurate, and locally actionable information will lead to better behaviors and outcomes. Technology has a vital role to play in addressing barriers to access and getting information to critical actors in a timely way, Woocher emphasized, but it can also be used for nefarious purposes.

ARCHETYPAL CHALLENGES

Woocher identified four archetypal peacebuilding challenges as a way of stimulating the thinking of the workshop participants.

The first is what he called *the early warning problem*. How can information be collected and analyzed in such a way as to identify risks in a timely fashion, assess the nature of those risks, and communicate the results of the analysis to people who are in a position to prevent a conflict from breaking out or escalating? Many efforts have focused on ranking countries in terms of their susceptibility to conflict. But the greater challenge is getting information to the local level to help NGOs or local peacebuilding actors dedicate their resources most effectively. Furthermore, early warnings can be false warnings. Forecasts of relatively rare events sometimes result in warnings of conflicts that actually are not likely, even though the warnings can have serious consequences such as causing people to flee their homes or even to act preemptively in self-defense. Can technology mitigate the negative consequences of what might otherwise be an effective early warning system? A useful case study, said Woocher, is Liberia, where many people were concerned about risks surrounding recent elections, and investments were made in local early warning networks to counter these risks.

The second archetypal problem is *how to gain local support* for mediation of disputes that could escalate into violent conflict. Many past initiatives have sought to bring people together to engage in dialogue and resolve disputes nonviolently. Can technology increase the effectiveness of such initiatives? A useful case study in this regard is Kenya, where text messaging is being used to identify emerging disputes and enable preventive interventions.

The third type of problem is *promoting reconciliation* and understanding across identity groups. Can technology help groups come together after a war to start the process of long-term cooperation? In Sri Lanka, where groups are

extremely divided and traumatized after the country's civil war, some NGOs are using technologies to support reconciliation efforts.

The fourth problem is that of *promoting peaceful change* under extreme authoritarian settings or amid intense violence. The political space in such situations may be very narrow, requiring that activists using strategies of nonviolence to mobilize and work together. Can technologies be used to maintain and support cooperative and interactive relationships among identity groups in such circumstances? Syria is an obvious example of this problem, said Woocher, but many other cases exist.

THEMES OF THE WORKSHOP

Multiple broad themes emerged from the presentations and discussions, and they are summarized here.[1]

1. *Sensing as a Prelude to Shaping.* The act of sensing requires an answer to the question, "sensing to what end?" Only in relation to how the sensed information will be used to influence outcomes is it possible to know what kinds of information should be gathered, over what time frame, with whose involvement, and in what formats. Similarly, for data acquisition to have value, concrete analysis, dissemination, and action plans are equally important. Peacebuilding problems rather than technologies themselves must be the drivers of technological choices.

Tipson remarked that "Early warnings…can help people get out of the way, whether or not they change the course of events. But the focus still needs to be on how to assist the people engaged in theater to avoid the worst consequences of potential deadly violence." To provide actionable information, a sensing system must reduce rather than exacerbate uncertainty. Neil Levine, director of the Office of Conflict Management and Mitigation at USAID, observed, "Early warnings often present decision makers with the difficulty of uncertain information and high costs. Sensing can help in this respect by bringing clarity to how certain or uncertain information is."

[1] The workshop featured examples of several ITC technologies and their application to a class of peacebuilding problems related to sensing and shaping conflict. This summary, therefore, provides neither a comprehensive overview of the current state of the art, the gaps, and recommendations for technological research to fill those gaps, nor recommendations related to the application of particular technologies to specific problems in peacebuilding.

2. *Reconciling Values with Strategies.* All actors in postconflict societies are motivated by goals in addition to "peace" and "nonviolence." Simply eliminating violence, for example, is unlikely to create a self-sustaining peace: peace without justice, peace without progress, peace without some sort of social change is likely to be short lived. In developing strategies for peacebuilding intervention, however, NGOs, IOs, and governments need to recognize that not all actors will have the same values, priorities, and strategic assumptions regarding peace.

Melanie Greenberg, president and CEO at the Alliance for Peacebuilding, observed that most peacebuilders have a broader vision of the kinds of societies their work advances. Nonviolence is one goal, but their work typically embodies other objectives. As a result, explained Rafal Rohozinski, a principal at the SecDev Group, direct collaboration is often not realistic without negotiation, compromise, and accommodation. Without a conscious attempt to link sensing activities to a concrete strategy for change, there is no guarantee that better information will lead to either change or peace.

3. *Prioritizing a Few Key Problems and Sectors.* Conflict is a highly complex phenomenon, but peacebuilding can be made more manageable by focusing on recurrent challenges in specific settings. Organizing around a few priority problems and considering the use of technological advances to address specific problems may enable outcomes that can be generalized and applied more broadly. For example, Woocher distinguished four phases as potential settings for peacebuilding: preconflict, midconflict, postconflict, and political mobilization. And Chris Spence, chief technology officer at the National Democratic Institute, in his overview of election monitoring, highlighted the value of concentrating on particular problem areas, such as export of election data, consolidation in the cloud and remote access, collection and representation of basic political data, and communication of results.

4. *Understanding the Larger System.* The counterpoint to the preceding theme is that segmentation of problems must not ignore the social, cultural, and economic context within which they are embedded. In any project, the implications of potential changes in the wider social and political setting should be gauged so that the outcomes of change can be incorporated in a larger change management strategy.

For example, demanding that elections be held too quickly after a peace agreement could exacerbate conflict. And clumsy reporting of monitoring data can undermine the legitimacy of elections that were generally fair. In his presentation on sensing and data in postconflict elections, Spence noted, "In elections you want to focus as much on the positive as you do on the negative and tell a story which really does convey to the public what's actually going on and not just a random biased sample of negative reports."

5. *Communicating Ground Truths that Facilitate Change.* Rich opportunities exist to develop and refine ways of capturing and displaying conditions on the ground to facilitate efforts to change those conditions. In particular, the work of NGOs and activist communities could be better communicated and integrated with the work of formal institutional actors. Sharing is currently too one-sided, with government agencies—especially the military—capturing open source information but releasing very little of what they know or think to outsiders.

Duncan Watts, principal researcher at Microsoft Research, and Patrick Meier, director of social innovation at Qatar Computing Research Institute, among others, emphasized the need not only to continually improve real-time maps but also to facilitate a shared and wider understanding of the insights provided by those maps through better communications and engagement. New tools and applications that are more compelling and accessible to all actors could increase effectiveness in all phases of the sensing feedback loop from data acquisition, through information analysis, to warning. Better integration of images and video into such datasets could foster sharing and comparison of information. Tipson suggested that because UN agencies are largely precluded from political "intelligence gathering" or early warning activities, they may be more inclined to share analysis generated using more robust and authoritative nongovernmental inputs.

6. *Overcoming the Digital Divide.* A long-standing concern in the development community has been the creation of a digital divide between individuals, groups, regions, and countries that have and do not have access to information technology. Driven in part by Moore's Law—the observation that integrated circuits tend to double in performance roughly every two years—information and communications technologies are sufficiently inexpensive that they

are becoming commonplace in even the most fragile environments. Even if inequality and the "digital divide" have not completely dissipated, they are diminished and capabilities have increased for almost everyone.

Raghavan observed that analysts tend to overestimate the effects of technology one year out and underestimate them ten years out. Planners need to consider where technologies could be in the future, recognizing that additional investments will generate new capabilities. Even those lacking a "utopian" view of technology can appreciate technology's capacity to enhance social well-being and enable progress.

7. *Challenging Cyberspace Regulation.* The application of technologies for peacebuilding can make government performance more effective through enhanced rule of law, transparent budgeting, healthy enabling environments, competitive media, and so on. But there are competing visions of how governments should monitor, regulate, and control cyberspace, and widely divergent approaches to Internet governance specifically. Governments are not monolithic, however, and often have a range of views about managing openness.

Tipson noted "The impulse to protect citizens in other countries is strong and often admirable, but the United States should not assume that our version of openness always strikes the right balance for everyone. In some respects, the efforts by various governments to exert more political control over their citizens' Internet activities as much stems from fears of American dominance of cyberspace as from a desire to repress their own people." Rohozinski said that the creation of digital borders in cyberspace through economic or political mechanisms may be a foregone conclusion. Despite US companies' vital interest in the free flow of information across borders, international rules governing the Internet are being renegotiated and a number of nations are opting for much higher levels of regulation and control.

8. *Improving Transparency and Standards of Conduct.* Current processes for determining standards for Internet use are neither transparent nor inclusive. There are no widely accepted standards for conduct, corporate behavior, or transparency for any of the many stakeholders—including industry, government, and civil society—that use and benefit from the Internet.

Sanjana Hattotuwa, a special advisor at ICT4Peace, raised the question of corporate accountability on issues such as privacy, self-censorship, deference to government authorities, and the archiving of data for public access. Rohozinski referenced the role of telecommunications companies in establishing de facto conditions for online actions. Tipson cited Syrian activists who complain that Google's application of local standards of decency in deciding what to allow on YouTube inhibits their ability to display the brutality of the Assad regime.

2

The Technological Potential

Four presenters focused on the capabilities of new technologies in peacebuilding. The rapidly growing range and scope of applications point to tremendous potential, although the contributions of technology toward preventing and mitigating violence depend on both the specific application and the context.

THE TECHNOLOGICAL CAPABILITIES

Prabakhar Raghavan of Google described some of the many technological capabilities that are now available. For example, it is routine in many parts of the world to use the collective flow of information from smartphones on a highway to measure traffic; the information can then be conveyed back to individual drivers about the state of traffic and the time it will take to get somewhere. This approach of using a "swarm of sensors" has been completely mechanized and is no longer "deep" (futuristic) technology. Instead, creativity centers on the development of new applications for the technology. The variety of applications to which swarms of sensors could be applied was not foreseen ten years ago, Raghavan said. Indeed, people tend to overestimate what will be possible in one year but underestimate what will be possible in ten years.

Another new trend is the remarkable power of machine learning. In the past, computer scientists tried to dissect every problem in minute detail,

analyze it, and come up with the optimum solution, but over the past two decades they have made great progress using a different approach. Instead of analyzing problems, they feed large amounts of data into computers along with a machine learning algorithm. The computers then "learn" how to carry out actions based on their analysis of the data. For example, Andrew Ng and his colleagues at Stanford University have used this approach to teach an autonomous model helicopter how to fly patterns that no human pilot would ever fly.[1] "In some sense, 200 years of wisdom in fluid dynamics and aeronautics got compressed simply by throwing a lot of data" at the problem, said Raghavan. This approach is not universally applicable, but it has considerable promise. "This sort of machine learning and control has gotten us to the point where we almost have driverless cars on the road, and that's a very exciting development if it can cut 30,000 road fatalities a year."

The challenge is much greater for peacebuilding, Raghavan admitted. Once a machine learning program has seen 50 street corners, it has a pretty good model of what a street corner is. But machines will not perform as well after seeing 50 conflicts and trying to make inductive inferences about the 51st. Conflicts are far more detailed in their social and political underpinnings, so technological solutions can only go so far. Nevertheless, said Raghavan, "I'm a convert. I have tremendous faith in what machine learning is capable of accomplishing. There are times when you don't have to get to the bottom of the detailed analysis. Machines can do things for you that are remarkably powerful."

Raghavan also pointed out that most computer cycles are used not to compute but to communicate. In many emerging markets, many people do not have a car but they have a smartphone. In that sense, transportation is falling behind communication in the modern pyramid of human needs. People may not have 24-hour electricity, but they have enough to keep their phones charged. "There is something very powerful about that," said Raghavan, and peacebuilding needs to tap into that development.

As technologies continue to develop and be applied in unanticipated ways, Raghavan suggested that pressure from the peacebuilding community directed at technology developers to apply these new technologies to the cause of peace could have tremendous benefits.

[1] A video demonstration is available at http://heli.stanford.edu (May 14, 2013).

PERSPECTIVE FROM A SOCIAL SCIENTIST

Duncan Watts, a principal researcher with Microsoft Research, parsed the issues discussed at the workshop into three categories. In the first category is what he called the representation of ground truth, in which information is gathered and processed to yield a representation of what is happening. (Box 2-1 presents an example of such a representation.) What happens with that information can vary from good to bad, depending on who is using it.

The second category involves the ability to interpret a signal about what is happening to anticipate or predict what will happen. Technologically this

Box 2-1
Sensing Conflict in Syria

As an example of the capabilities of new technologies, Rafal Rohozinski, principal with the SecDev Group, described a sensing exercise focused on Syria. Using social media analytics, his group has been able to identify the locations of ceasefire violations or regime deployments within 5 to 15 minutes of their occurrence. This information could then be passed to UN monitors and enable their swift response. In this way, rapid deductive cycles made possible through technology can contribute to rapid inductive cycles in which short-term predictions have meaningful results for actors on the ground.

Further analyses of these events and other data also made it possible to capture patterns not seen through social media analytics. For example, any time regime forces moved to a particular area, infrastructure such as communications, electricity, or water would degrade, partly because the forces turned off utilities, a normal practice, and partly because the movement of heavy equipment through urban areas caused electricity systems to go down. The electrical grid is connected to the Internet, so monitoring of Internet connections provided immediate warnings of force movements. "These technologies are already quite powerful about being able to provide that kind of sensing," said Rohozinski.

However, there are ethical questions about whether gathering data at this level of granularity is consistent with international law, even for humanitarian actors. The collected data can become a risk to communities that humanitarian actors are trying to help. The shaping of conflicts can be countershaped by actors who pollute data streams to change the nature of the response. "It's not an uncontested environment and we can't simply see it as one that we own [either] from a technology or from a data point of view."

is no more difficult than the representation problem. But theoretically it is more difficult because it raises questions about what signals are informative.

The third category involves the facilitation of communication, resolution, and reconciliation. The technological problem in this category is comparatively simple, but the theoretical problem is immense. Giving people cell phones does not indicate whether things will change for the better—or worse.

Watts also classified the issues discussed at the workshop according to the audience to whom information is directed or the users of particular tools. External actors may be agencies, NGOs, and self-organizing communities focused on an issue or problem; internal actors include the local communities and people directly affected. The use of the information generated in any of the three categories above—representation, early warning, or communication and facilitation—is very different depending on which set of actors receives it. For example, early warning information bumps up against the problem of political will. Even if information indicates that something is going to happen, external agents may do nothing, or they may communicate information to a trusted network of internal actors. In the latter situation, internal actors need to worry about what to do with the information and what the likely consequences of that action might be. If a natural disaster is predicted, will a local population be better off or worse? Computer scientists refer to this kind of situation as the price of anarchy, where distributed decisions are not sorted by outcome. "Simply giving people more information doesn't necessarily lead to a better outcome, although sometimes it does."

Technical problems, such as building better real-time awareness tools, can yield an infusion of resources to produce better tools. But political and social problems, such as convincing a policymaker to take a particular action, tend to be harder to solve. Other such problems concern the coordination of responders who converge on a conflict zone to help, or the best ways to encourage local communities to resolve their conflicting agendas.

An experimentalist approach to political and social problems, noted Watts, might be to instrument the world, conduct field experiments to gauge the impacts of different interventions, and measure the results. Such an approach, however, would be insufficient. The technology challenges may be seen as low-hanging fruit for the near term, while agendas for research could be laid out in other areas to work toward long-term solutions.

This way of looking at the issues prompts several questions, Watts noted. Are human analysts the best way to combine and analyze information, or can this sense making be better handled by machines? How can that capability

be tested? If human analysts are used, how should they be organized? What kinds of people are needed? How can their division of labor be established? "These are standard questions in industrial organization and organizational sociology," said Watts, "and I think we have good answers to them, but this is certainly an interesting context in which to think about it."

The most important question is what to do with information once it has been gathered. The answer is associated with a spectrum of social dynamics issues. Communities and nation-states are complex organizations with multiple scales and many things happening simultaneously. Even if someone has a good picture of what is happening at the moment, the ways to improve a situation are not necessarily obvious. Decisions will also depend on whether actions are to be taken by an external or internal actor.

"I don't have any answers to any of these questions," said Watts. "But I wanted to emphasize that the technology is extremely exciting." Many things are possible today that were not possible ten years ago. But it is an illusion, he said, to think that gathering more data and applying more processing power is going to lead inevitably to better outcomes without understanding how systems work.

BIG DATA FOR CONFLICT PREVENTION

The world's population is generating and processing an immense quantity of digital information, observed Emmanuel Letouzé, a consultant for the United Nations and other international organizations and the author of UN Global Pulse's white paper "Big Data for Development: Opportunities and Challenges."[2] He quoted a figure from the University of California that the world's computers process about 10 zettabytes of information in a single year, the equivalent of 10 million million gigabytes. Furthermore, the number is increasing—"the growth is really ahead."

"Big data" is not well defined, but it is often characterized in terms of three Vs: volume, variety, and velocity. The volume ranges from kilobytes to petabytes, the variety from ephemeral texts to archived records, and the velocity from real time to batch processing, but all three dimensions are relative and contextual, said Letouzé. Intent and capacity are the central factors affecting the application of technology, but how these play out exactly depends on the technology and the context in which it is applied.

[2] The paper is available at www.unglobalpulse.org/sites/default/files/BigDataforDevelopment-UNGlobalPulseJune2012.pdf (May 14, 2013).

Global Pulse has defined four kinds of big data in its work on development. *Data exhaust* refers to the "passively collected transactional data from people's use of digital services like mobile phones, purchases, web searches, etc.," which create networked sensors of human behavior. *Online information* is "web content such as news media and social media interactions (e.g., blogs, Twitter), news articles, obituaries, e-commerce, job postings"; these data treat Web usage and content as sensors of human intent, sentiments, perceptions, and wants. Data from *physical sensors* include "satellite or infrared imagery of changing landscapes, traffic patterns, light emissions, urban development and topographic changes, etc."—information derived from remote sensing of changes in human activity. And *citizen-reported or crowdsourced data* refers to "information actively produced or submitted by citizens through mobile phone–based surveys, hotlines, user-generated maps, etc."; this information is critical for verification and feedback.

Global Pulse also has delineated three applications of big data. *Early warning* is "early detection of anomalies in how populations use digital devices and services," which can enable faster response in times of crisis. *Real-time awareness* is the use of big data to produce "a fine-grained and current representation of reality," which can inform the design and targeting of programs and policies. *Real-time feedback* is "the ability to monitor a population in real time," making it possible to understand where policies and programs are failing and make necessary adjustments.

For the use of big data in conflict prevention, Letouzé distinguished between structural and operational efforts. The goal of the former is to understand the ecosystem while identifying the structural drivers of conflict. The goal of operational prevention is to detect and respond to anomalies through, for example, early warning and response systems. Big data can contribute to both forms of prevention, especially as data become more people centered, bottom up, and decentralized, said Letouzé.

Global Pulse, in partnership with several other organizations, has analyzed situations analogous to conflict prevention to get a sense of the potential for big data to serve peacebuilding. For example, it has looked at the sociopsychological effects of a spike in unemployment, as measured by online discussions, to seek proxy indicators of upcoming changes, just as the food price index has been a predictor of food riots. And the ability of tweets to anticipate the official influenza rate in the United States similarly demonstrates how big data might provide early warning of emerging events.

Mapping unstructured data generated by politically active users is further evidence of the potential of big data in conflict prevention, Letouzé said.

For example, mining the social web during Iran's postelection crisis in 2009 revealed some evidence for a shift from awareness and advocacy toward organization and mobilization and eventually action and reaction. Similarly, data visualization of the Iranian blogosphere has identified a dramatic increase in religiously oriented users, while a study of tweets associated with the Arab Spring found that, in 2010, socioeconomic terms (e.g., income, housing, and minimum wage) largely prevailed whereas in 2011, 88 percent of tweets mentioned "revolution," "corruption," "freedom," and related terms.

The evidence, Letouzé explained, indicates that big data could help by providing digital "signatures" that can enhance understanding of human systems, along with digital "smoke signals" of anomalies for early warning and prevention.

However, big data also pose risks and challenges in conflict settings. (Chapter 4 discusses in detail the misuse of technology in conflict settings.) As Patrick Meier and Jennifer Leaning pointed out in 2009, information and communications technologies, including the use of big data, raise serious concerns about access and security because of the lack of economic development, the prevalence of oppressive regimes, and the increasingly hostile environment for humanitarian aid workers throughout the developing world.[3] In addition, the use of big data for conflict prevention faces many of the same challenges as its use for development, such as digital divides, lack of infrastructure and other resources, and political constraints.

A related important challenge concerns the balance between access to data and protection of data producers. Reliability in conflict settings is another issue, especially when people have an incentive to "play the system" or suppress signals (e.g., by destroying cell towers). Though many people think that data are easy to access, in fact not all data are produced in easily accessible and storable forms, said Letouzé. Furthermore, in a conflict setting, the privacy challenge can become a security challenge.

But the biggest problem Letouzé identified is what he called arrogance or overconfidence. People have a tendency to believe that data mining invariably yields the truth. They may see patterns where none exist, confuse correlation and causation, not understand sampling techniques, be misled by sample bias, or lack sufficient computing capacities to appropriately interpret the data. Data scientists or econometricians often do not know the context in

[3] Patrick Meier and Jennifer Leaning. 2009. Applying Technology to Crisis Mapping and Early Warning in Humanitarian Settings. Cambridge, MA: Harvard Humanitarian Initiative.

which data are generated to be able to distinguish between a joke, an offhanded comment, or a real threat.

Big data can jeopardize the security and privacy of individuals and communities, and this risk may be greater in conflict zones, where it can create a new digital divide between and/or within communities and regions. At worst, big data could function as a sort of Big Brother for a world that is atheoretical, acontextual, and all automated, according to Letouzé.

Contextualization is key, especially when lives are on the line, Letouzé concluded. Big data should build on existing systems and knowledge and should be applied incrementally, iteratively, and over the long term, as a tool rather than a driver of change. Nevertheless, big data will continue to grow and develop and will likely eventually play a significant role in conflict prevention.

TECHNOLOGICAL CHALLENGES FOR PEACEBUILDING

Shortly before the workshop, USAID and Humanity United issued the Tech Challenge for Atrocity Prevention. Five key challenges in peacebuilding were presented at the workshop by Patrick Vinck, a research scientist at the Harvard School of Public Health and associate faculty with the Harvard Humanitarian Initiative (HHI).[4] These challenges were:

1. Identification of uses of technology to deter enablers of violence—third parties such as multinational corporations and institutions that finance, arm, coordinate, or otherwise support perpetrators of violence.
2. Collection of evidence of sufficient quality to be used in court against the perpetrators.
3. Development of methodologies and indicators to assess vulnerability to inter- or intragroup violence.
4. Ability to communicate with and between conflict-affected communities and also the ability of affected communities to communicate with responders.
5. Development of simple, affordable, trainable, and scalable technologies to enable NGOs and human rights activists to gather or verify information from hard-to-access areas.

[4] More information is available at www.thetechchallenge.org/#!enablers (May 14, 2013).

The collection of information is a central component of these challenges, said Vinck. Significant progress has been made in mining information from new technological sources such as the Internet and social media. In a more active system, individuals in a community, whether volunteers or recruited for the task, would send information to a monitoring system. In particular, smartphones can be used to gather data more quickly, more accurately, and with better controls on where the information has been collected and when. An example from Eastern Congo is a project called Voix des Kivus, in which individuals were selected and trained to report information as it happened in the field. Another example of the adoption of a new technology is the use of satellite images to document the preparation of attacks, a step that has helped to democratize tools previously limited to military use.

These new technological tools hold promise, but there has been very little evaluation of their application, Vinck noted. And the evaluation that has been undertaken reveals a problem of linking information with responses. In the Central African Republic, for example, a system was set up to improve communication between affected communities in the Lord's Resistance Army area with humanitarian groups. After six months, hundreds of messages had been received from the community, but no humanitarians indicated having responded directly to any of these messages, even though the system was supposed to be a two-direction communication system. "They were gathering and collecting the information but they were not using it," said Vinck. The same thing happened with the Voix des Kivus project: it was a success in collecting information, but no humanitarians indicated having responded directly to that information.

Vinck also pointed to a disconnect between the technologies discussed at the workshop and what is actually happening on the ground. In some places, less than a third of the population has access to a cell phone, and of that only a fraction may use text messaging. Text messaging may be common among the most educated people in the community but not, for example, among poor women, so the resulting information may be biased. Access to technology may vary by geography within a country, which may also distort the information provided. In some places even simple technologies like radios may not work because of a lack of electricity, equipment, or local capacity to fix equipment. Technology has great potential, Vinck said, but biased results may be detrimental to the situation on the ground.

The information collected by communities through technologies is also typically available to those communities, which therefore have a responsibility to respond to that information, according to Vinck. Responses are no

longer solely in the hands of international organizations or governments. With satellite imagery, for example, if credible evidence shows troops massing outside a village, the people of that village can respond; they may flee, or they may respond with violence.

Whoever compiles and provides information to a community has a responsibility for what happens with that information, which raises a host of ethical questions. What does information mean? How should it be interpreted? How should it be shared and with whom?

Finally, technology can bear witness to what has happened. Sensitive data need to be archived and protected, said Vinck. Many groups in the public and private sectors have collected large amounts of data, but there is no clear responsibility for storing the data.

DISCUSSION

Melanie Greenberg, president and CEO of the Alliance for Peacebuilding, called attention to issues associated with the sharing of data gathered using technologies (the subject of a previous NAE-USIP workshop that she cochaired[5]). There are particular ethical considerations associated with the sharing of data with the military, for example, as such sharing can affect the security of NGO personnel and their local partners.

Matt Levinger, director of the National Security Studies Program at George Washington University, said his experience as an early warning analyst made him a skeptic about early warnings in general. "It's hard to predict the future…any number of potential futures are possible." A better approach, he said, is early detection and adaptive response. In his work on conflict analysis, he thinks of actors as either dividers (potential sources of polarization and conflict) or connectors (potential sources of cohesion). Generally speaking, peacebuilding involves trying to identify and mitigate the effects of the dividers and trying to identify and bolster the connectors. A key question, then, is, Where do technologies have the potential to make new kinds of connections and boost resilience? "If we start thinking about what information do we need and go from there, we will be in a much better place than if we ask what information the technology allows us to obtain."

Robert Loftis, a consultant and former State Department official responsible for conflict stabilization, discussed the need to separate sensing

[5] The report, *Using Data Sharing to Improve Coordination in Peacebuilding*, was released in December 2012 and is available on the NAE website (www.nae.edu/66866.aspx) (May 14, 2013).

and shaping. Sensing essentially involves reacting to something that is happening. But most conflicts are not surprises, even though their timing may not be known for sure. Sensing technologies can direct humanitarian aid, but, unlike shaping, they do not necessarily change the conflict. (Chapter 5 addresses the path from sensing to shaping.) The question, then, is whether the use of technologies can, in fact, prevent a conflict. Can they be used to help resolve land tenure disputes or differences over water rights before these become violent conflicts? This more anticipatory and active approach involves the dissemination and use of information to reduce differences among people and groups.

Joseph Bock, director of global health training for the Eck Institute for Global Health at the University of Notre Dame, wondered whether some aspects of big data might be overly hyped. Flashpoints are often single precipitating events, not related to complex pattern analysis, and understanding them may be more important than analyzing big data. Still, he said, the latter could be immensely useful in tracking sentiment through media and communications, which today is a labor-intensive task. Combined with the use of sensors to detect conversations, big data could be "incredibly powerful," though there is also a risk of being massively intrusive.

Fred Tipson called attention to the opportunities provided by technologies that promote collaboration. Peacebuilding is built on interactions among individuals and groups, and technology platforms can facilitate these interactions and broaden the range and effectiveness of the actors involved.

3

Uses of Technology in the Field

Several speakers described specific applications of technology in the peacebuilding process. This chapter looks at three such examples: election monitoring, crowdsourcing, and the dissemination of information through social media and other means. In all three cases—and in others mentioned during the discussions—technological applications bring new capabilities but also raise new considerations about their effective and responsible use.

ELECTION MONITORING

Work on governance and democracy overlaps with peacebuilding, said Chris Spence, chief technology officer for the National Democratic Institute (NDI), and among the most important areas of overlap are elections. When elections are held, citizens need to trust the electoral process. Election monitoring allows citizens to analyze in a systematic way the quality of an election and communicate what they saw. The monitoring begins well before an election, has a focal point during the election, and continues during the postelection period. It involves many groups—citizens, political parties, parliaments or legislatures, and international organizations.

Election monitoring typically involves training hundreds or thousands of citizens to go to polling stations from the time they open until they close, including the counting process, and to look for particular things. The moni-

tors report periodically throughout the day to a command center, often in the capital city. Analysts combine the monitors' reports and produce an assessment of the election process. These statements have to be carefully worded, because they can be a flashpoint for citizen reactions to an election. NDI has given particular attention to these messages, working on how to tell a story with data and visualize processes on a map.

Technology has greatly improved but also complicated election monitoring. The adoption of mobile telephones, for example, has "fundamentally changed and improved election monitoring around the world," said Spence. Before mobile phones, monitors made their reports on paper, which had to be gathered by people in vehicles or on foot before the reports could be analyzed. "That process was inefficient, slow, and inaccurate, and frankly election monitoring groups were making statements they couldn't back up with data, way too often, until mobile phones."

Voice reporting and text messaging with mobile phones have transformed the reporting system, and smartphones could bring further improvements. Smartphones will not be adopted soon at the grassroots level in many places, Spence cautioned, but they represent the "next level of phenomenal opportunity for all of us to start solving these data collection problems."

Technology also has improved the analysis of data, whether texts, data entries, or phone calls. It can filter data to determine which sample points are missing, and it can detect bad data and recontact observers to confirm information. "You can get much better quality data through these data tools and dashboards."

One problem with election monitoring is that analysts still typically work with the software tools they used in the days of manual reporting rather than the Web-based tools now available. "There's an opportunity that we've been trying to solve, and we welcome help."

Command centers have begun to use cloud computing, which makes it possible to not only store data remotely but also synchronize and compare data. Cloud storage broadens access to the data and protects them if a data or command center suddenly becomes inaccessible. And cloud computing facilitates the participation of analysts outside the country or in safer locations.

Better visualization tools and datasets are needed, Spence said. For example, acquiring data about past elections is very difficult in many countries, but these data can be very useful for checking turnout and other aspects. Similarly, an important preelection activity is a voter roll audit to determine whether voters are intentionally or otherwise being disenfranchised, but such rolls can be difficult to acquire. Even reliable maps of current

political boundaries may be unavailable. "I don't have to tell anybody in this room that boundaries often change, and there's often what we would call in this country redistricting going on around political events. It's hard to get those maps." An important future task will be to collect election data and make them easily accessible and open for all to use.

Finally, technology can help tell the story of an election. Many organizations believe that once a press release is carefully written detailing the results of an election monitoring effort, their work is done. But technology offers many other means to disseminate and elaborate on that message, from social media to new forms of visual representations. For example, NDI recently worked with a group in Senegal called One World and made significant progress in conveying the positive and not just the negative news about an election. Based on an analysis of reports, a map showed green areas where things were going well and red dots where there were problems. "In elections you want to focus as much on the positive as you do on the negative and tell a story that really does convey to the public what's actually going on and not just a…biased sample of negative reports."

Spence observed that a key way to mitigate or prevent conflict is to establish communication channels among potential combatants. NDI uses this technique with political parties in the election environment, though it cannot work with any group that condones violence, such as militant groups or terrorists. NDI and the UN took an approach in Libya that involved establishing codes of conduct for elections. Forty Libyan parties came together face-to-face and negotiated 14 principles to which they would adhere, such as not buying votes, respecting the election commission's final result, and not using violence. Technology was not involved in that meeting, but it could be used to facilitate such efforts. For example, political parties or other factions may be able to create collaborative platforms without coming together physically.

Transitions are inevitable as institutions with older habits and technologies encounter new technologies, Spence said. The combination of the old and the new will create a hybrid in which different sources of data continue to have value. For example, social media streams can be phenomenal sources of data for election monitoring, but polling station information and political maps of countries also remain valuable. "Let's not forget about the fundamentals as we begin to merge and deal with new datasets." Similarly, observers can be deployed with clipboards to collect data even as new forms of data are gathered and analyzed. The challenge is to build bridges between the traditional approaches and actors and the new actors who are introduc-

ing new technological capabilities. "I'd encourage everybody to not just look at where we are going but where we are and the process of getting from here to there."

CROWDSOURCING IN KENYA

Ushahidi, which means "witness" in Swahili, is an open-source project set up by Kenyan bloggers during the postelection violence of December 2007 and January 2008. The Kenyan government was trying to downplay the severity of the situation by limiting what the mainstream media could publish. A blogger in Kenya named Ory Okolloh received evidence from hundreds of her readers about human rights abuses. They provided photographs and videos that were disseminated through Kenya's vibrant blogosphere. Okolloh published this information online, and the result was a technology for election monitoring that delivered a "live" map of human rights abuses.

The effects of this information on the conflict are difficult to gauge, said Patrick Meier, director of social innovation at the Qatar Foundation's Computing Research Institute, although he met people in the years following the violence who said they used the reports to make decisions about their movements. Such reports are anecdotal, however, and there is very little evidence to determine whether or how the conflict changed.

In a previous position at the Harvard Humanitarian Initiative, where Meier codirected a program in crisis mapping, he was involved in a project to compare georeferenced and time-stamped Ushahidi data with coverage from the national and local print and broadcast media.[1] The events reported in the mainstream media were manually geolocated and time stamped and compared with the digital traces of about ten of the most active citizen journalists in Kenya. The data were put into a mapping program and animated to understand the information flows and potential information consumption patterns in crisis-affected communities. The comparison showed that citizen journalists tended to be the first to report on escalating tensions, and the mainstream media tended to report on the event after violence had begun, according to Meier. The crowdsourced data also had greater geographical coverage. Thus, by combining information from different sources, information could be not only compared but expanded beyond that of any single source.

[1] See http://irevolution.net/2008/10/23/mapping-kenyas-election-violence/ for a summary evaluating the impact of crisis mapping on postelection violence in the 2007 Kenyan elections (May 14, 2013).

Crowdsourcing has several distinct advantages in sensing conflict, Meier observed. It is available in real time. It can create shared awareness among the members of a crisis-affected community, and that shared awareness can be critical in catalyzing social movements. And it can provide real-time situational awareness through social media to sense conflict in ways that have not been possible before.

Meier is currently involved in a project in Kenya called PeaceTXT, which uses text messaging as a way to change behavior, based on observations that public health text messaging can significantly change people's behavior.[2] (A prominent model for PeaceTXT was a Chicago-based project called CeaseFire, which used early warning and quick responses by former gang leaders to prevent and reduce street violence.) Based on work in areas prone to conflict, including focus groups with former perpetrators of violence, PeaceTXT has developed 40 to 50 specific text messages geared toward different triggers and phases of conflict. The system now has about 40,000 subscribers, and new subscribers are being enlisted through grassroots partners. Evidence of its effectiveness has begun to accumulate, but "it remains to be seen whether and how this might have an influence on shaping potential conflicts during the next elections."

The Arab spring was a textbook case of the use of technology in conflict settings. As one activist in Cairo put it, "we use Facebook to schedule our protests, Twitter to coordinate, and YouTube to tell the world." "Deliberate, planned uses of technology and civil disobedience and resistance are very powerful," said Meier. But important lessons remain to be learned about how people have used and can use these technologies to shape social movements.

TECHNOLOGY IN SRI LANKA

Sanjana Hattotuwa, special advisor to the ICT4Peace Foundation, has experienced firsthand both conflict and the application of technology to peacebuilding. He was six years old when civil war broke out in Sri Lanka in 1983, and in 1993, when his neighborhood was badly affected by ethnic violence, he saw "things that no child should see."

His work in Sri Lanka is difficult, he said, and technology does not make the life and work of a peacebuilder any easier. Data points, information agents, and analysis engines do not mean that the risk is mitigated. For one thing, the existence of information does not mean that a demand for

[2] See http://iRevolution.net/2013/03/04/peacetxt-kenya-2/ to learn more about the PeaceTXT project (May 14, 2013).

the information exists, whether from policymakers or the public at large. In Sri Lanka, he said, the general population is not necessarily interested in the country's contemporary history, what happened, and the costs of the war that helped end the violence in 2009. People are tired of war and share a feeling of relief and happiness that they can walk on the street and not be worried about a suicide bombing. Moreover, raising hard questions through technology risks the resumption of violence. "It's an open question whether some things are better left unsaid and buried literally and metaphorically."

Yet Hattotuwa added that his bias is toward providing information that the public can question and debate. Government should not have a monopoly on information so that it can issue only the information that it finds convenient. During and since the war he has produced information "in almost every imaginable form" to help people understand what they experienced. For example, he has sought to visualize human rights violations using maps, as part of a broader effort to explain concentrations of power and their implications for future conflict. He also has created a website called Groundviews, which puts out reports about what people see. "It's the simplest thing really. It's not Twitter analytics. It's not massive computing database visualizations. It's just what people see on the ground that contests official narratives."

A major problem in Sri Lanka is not literacy per se—the country has one of the highest literacy rates in South Asia—but media literacy. People believe what they read and tend not to be able to distinguish between propaganda and life-saving information, said Hattotuwa. "That level of critical comprehension and questioning is simply not there in the population."

Thus the same technologies that can promote peacebuilding also can exacerbate the spread of violence and hate. When people believe what they read and retransmit that information, geographically dispersed violence can occur over a very short period of time, which can lead to ever larger and longer-term systemic problems. Sri Lanka has rich traditions of storytelling within communities, so if one person has access to technology, information can be communicated verbally from that person throughout an entire village.

Gender is also an important factor, Hattotuwa said. Multiple reports have documented that the education of girls in countries such as Sri Lanka is a major determinant in avoiding future violence. "I very strongly believe that there needs to be an emphasis on the gendered use of technology," he said.

Reconciliation in Sri Lanka has been very complex. For the current government, it is simply a matter of economic development, said Hattotuwa. Accountability, allegations of war crimes, and the events accompanying the

end of the war are ignored. The report of a commission that looked at war crimes has been translated into Sinhala and Tamil only because Hattotuwa's organization did so. Furthermore, the ICT4Peace Foundation's efforts to use technology to strengthen reconciliation risk sparking the ire of the government, which can have implications for individuals' families and security. "Ironically, championing the agenda of reconciliation through what we do has very definite implications for the peacebuilders in the country. Technology is not a safety net, and it is very, very contested."

As an example of how technology can intersect with peacebuilding concerns, Hattotuwa mentioned a story he did that used Google Earth to document the hundreds of thousands of people living in a tiny sliver of land in the northeast of the country. However, Google has no corporate policy on the retention of historical layers in Google Earth, raising the question of whether this information will continue to be accessible. "The point that I was making through the article was that this is a slice of a three-year-old Sri Lankan history that's hugely contested but absolutely vital to our children and our future that exists nowhere else apart from Google."

Hattotuwa has written other stories and disseminated other information to keep Sri Lanka's history alive. For example, his organization has given people cameras to take photos showing what reconciliation means in very practical terms. "Bearing witness is very important for us."

Although regularly accused of being a terrorist and interested in regime change, Hattotuwa said that he is not interested in regime change because it would not address the systemic factors that led the government to do what it did. Rather, he is interested in using technology to bear witness to inconvenient truths that otherwise would not be debated or archived for posterity. "That is fundamentally important for me because it places the value of ideas and data above my own life and the lives of peacebuilders. You can kill us, but you cannot kill the data, you cannot shut down a site today and expect that inconvenient truth to be erased. So, in that sense, it's larger than us." Authoritarian governments believe they can intimidate people and control information, "but today information is free," said Hattotuwa. "You can… physically replace people in a country, but the information will always find a way out."

Hattotuwa urged using the full range of technologies to keep public debate alive and "help people ask the questions that need to be asked." Technology needs to be democratized, he said—made available at the lowest possible grassroots level and not used just by elites. Both sensing and shaping need to include all people, not just those who are inherently in a position to

use technology. He uses social media such as Twitter and Facebook in both his private life and his work. These technologies are being used in the Sri Lankan diaspora, and they will help determine how Sri Lanka addresses its past and designs its future. Such technologies, driven by the observations of ordinary citizens, document what actually occurred, and challenge the narrative that the government wants to portray.

Sri Lanka could still return to violence, but discussions are taking place there thanks to technologies that did not exist a few years ago and those technologies are helping Sri Lankans see a different future. "I'm committed to that future, and I truly believe the discussion about what we should be doing and the future to which we should be heading. And the many other interpretations of that future can only occur because of the technologies that we are talking about today."

DISCUSSION

An interesting discussion arose about the use of satellite imagery as both a deterrent and early warning system to prevent violence. Ivan Sigal, executive director of Global Voices, spoke about the power of the "long zoom," where a figurative camera in outer space moves from one location of the planet to another. Through the resulting satellite imagery, the long zoom provides a fundamentally different perspective on war than photojournalism. Photojournalism portrays wars as personal through interrelationships and actions, through kinetic movements of bodies through space, as being mostly about individuals—or about the de-individualization of people in the face of machines. The long zoom, in contrast, provides a structural and data-driven perspective on war, and can be combined with photojournalism to yield topographic photography, further connecting data, geography, and imagery.

Nate Haken, senior associate at the Fund for Peace, spoke about the potential of integrating different types of technologies for triangulation. Satellite imagery can be used to count livestock or track environmental degradation, both of which can be a correlate or driver of violence. These data can then be layered on other types of information to yield a multidimensional analysis. "If there are ways that we can find synergies to integrate these approaches, there would be some enormous potential for moving forward."

Dennis King, a senior humanitarian affairs analyst in the Humanitarian Information Unit at the US Department of State, briefly described some of the limitations of satellite photography. Though it can document scenes and let people know they are being watched, satellites do not provide images in

real time, they do not cover all regions equally, and clouds, vegetation, and nighttime can obscure the ground. In some places, satellite imagery can see structures and estimate populations, but it is less useful in urban areas. It is useful for tracing bombardments but not for documenting ground fighting.

That said, King described several instances in which journalists and policymakers were able to confront rulers with satellite images of atrocities, which can be very powerful. For example, when huts were burnt to the ground in Darfur, they were clearly visible on satellite photographs. But satellites have a limited capacity to provide early warnings, and the perpetrators of violence are learning how to hide their activities from satellite surveillance.

Melanie Greenberg mentioned the possibility of gathering other types of advance indicators of conflict. For example, if teenage boys in several villages start selling their bicycles to get money to buy guns, peacebuilders could use that information to take action. "What are the unusual patterns we might be able to see from this great conglomeration of data?"

Noel Dickover, new media advisor at the US Department of State's Office of eDiplomacy, mentioned Secretary of State Hillary Clinton's Civil Society 2.0 initiative, which has brought together leaders of local civil society with technologists, creating a bottom-up approach to sensing that can complement a top-down approach. "If you can find people who are already in a country doing great stuff on the ground, you can expose them in a very interactive way to some of these enabling technologies." Small groups of six or seven people engage in a series of activities to see what is possible and come up with ideas about how to apply technologies. Funders then can help convert these ideas into solutions. "We can start acting like angel investors, where instead of deciding, funding, and implementing the project ourselves, we're trying to engage really innovative teams." Dickover's group has applied this approach around the world and is putting the results online so that others can learn from them.

Christina Goodness, chief of the UN Peacekeeping Information Management Unit, cited a number of factors to consider in data gathering. One unresolved issue is the legal ownership of the information gathered, especially when multiple political actors and corporations are involved. With cloud storage, if data are collected in Syria, stored in Italy, and accessed from New York, which country's governance applies and what are the legal standards for using the data? Corporations are beginning to take a greater role in offering services previously offered by governments or civil actors, gaining greater control over the data they provide.

Goodness returned to questions about the right of privacy among data contributors and groups. Do they have the right to destroy evidence they have contributed? What are the obligations of carriers, not only legally but morally, especially when they operate in multiple countries? What are the rights of individual contributors to retain and perhaps obtain copies of the data they contribute?

There are also questions associated with the long-term viability of data. If data systems are not interoperable, it will be difficult to aggregate data and detect long-term trends. The long-term storage of data, whether by government or the private sector, has not been resolved for many applications.

Local peacebuilders and local peacekeeping communities are enthusiastic about using technologies to collect, store, disseminate, aggregate, and distribute information from alternate sources, Goodness observed, but there are no hard and consistent data to gauge the benefits and costs of using these data. "Perhaps now is the moment to explore the interoperation of the humanitarian with the political and security aspects of field operations," she said. The definition of a crisis could be expanded to include humanitarian, political, and security crises, and technologies could provide diverse sources of information about these interconnected dimensions of conflicts.

4

The Misuse of Technologies

Two presentations at the workshop addressed the use of technologies to repress political change, perpetuate conflict, or otherwise undermine peacebuilding agendas. Countries, organizations, and individual actors can have objectives that are at odds with those of peacebuilders. In response to the application of technology to peacebuilding, they can be expected to both counter those applications and use technologies for their own ends. Peacebuilders need to recognize these countervailing forces and plan and act accordingly if they are to make progress in reducing conflict and violence.

EXERTING CONTROL OVER INFORMATION

Ivan Sigal, executive director of Global Voices, which conveys to global audiences the voices of bloggers, writers, digital media activists, and translators who work in the developing world, began his examination of the misuses of technology by analyzing one of the two broad themes of the workshop: the means used to shape conflicts.

Conflict involves contestation, and those involved—including peacebuilders—have both intention and agency. Thus the activists represented by Global Voices have agency and seek to shape or influence their communities, as do their opponents in governments. Many of these activists use a collaborative and distributed form of knowledge to push ideas forward. To do this,

they need not only access to authority and power but also relationships in information networks that allow them to influence those networks.

In the Arab spring, maps of Twitter influence revealed important "nodes" in information networks. The individuals in question were not gatekeepers to authority and did not have exclusive access to resources, but they were good listeners and understood what kinds of skills could be of use to the communities they were addressing. For example, the activist who helped to overthrow the Ben Ali regime in Tunisia had been active in a distributed network for six or seven years testing different information strategies, including the use of big data tactics and distributed data to demonstrate why the regime was corrupt. A follow-on of WikiLeaks was Tunileaks, which led to a series of stories revealing the extent of Ben Ali's corruption from the perspective of the US government. These stories validated the claims of the opposition and further drove the conflict.

Governments, whether oppressive or not, can react to technology-enabled peacebuilding through their own use of technology. They may try to control leaks or access to information (as described in the next section). Moreover, oppressive regimes appear to be learning from each other and collaborating in their use of technologies, Sigal noted—techniques used in Syria to conduct surveillance or filtering are almost identical to those used by Iran, and many countries in the Commonwealth of Independent States have very similar filtering systems that appear to be the result of collaboration.

Sigal also observed that countries have collaborated on Internet governance that would treat the Internet as media and therefore subject to state jurisdiction. The model of a "territorialized Internet, one where telecommunication borders and national borders are congruent, is one that is broadly appealing" among countries that seek to control Internet use. The United States and other countries "don't have a vision for what we want the Internet to be—they do."

Sigal also described efforts by governments to use economic rather than political means to block Internet use. The government of Kazakhstan, for example, has been able to essentially create a national firewall without declaring one by incentivizing the largest telecommunications company in the country to provide free access to any kind of data, whether file sharing, music, or videos, while people who go outside the network pay for the data they access. "Suddenly going to Google…becomes a decision. Do I want to go to Google, or do I want to go to the one that I can get for free with KazakhTelecom?" While it may be easy to criticize China for erecting

a firewall around the country, it is more difficult to argue that the price KazakhTelecom charges for people to search Google is a travesty of choice.

At a deeper level, Sigal warned about the temptation to view Big Brother as a metaphor for the evolution of cyberspace. Such a view assumes that regimes are monolithic, but they usually are not; rather, they shift or split their alliances to achieve multiple and contrasting objectives. A better paradigm is Aldous Huxley's *Brave New World*. "Given enough freedom, we surveill ourselves. It's not that there's a watcher who will control everything that we do. [It's] us, especially in free societies."

Policymakers can take several steps to help communities of activists and prodemocracy organizations oppose the actions of oppressive governments. For example, some projects funded by the State Department have helped provide anonymity for activists. Since many of the technologies that repressive regimes use to track, spy on, and otherwise monitor activists come from Western companies, export controls can clamp down on the distribution of these technologies. However, this approach is more difficult with nondemocratic countries that are nominally allies, and such controls do not affect unfriendly countries where some of these technologies are made.

Some technology companies are working actively, though quietly, with activists toward positive ends. Some have hotlines and mediation processes so that if a government attempts to take down a posting, a company can assert that it is in fact a piece of rights documentation. "I want to commend those companies," said Sigal. "That kind of process that allows for some kind of clarification about what the political value of that material is has a lot of impact." Companies that build surveillance and privacy tools also have the option of conducting human rights audits among their clients, a strategy backed by many freedom-of-expression advocates.

A critical aspect of interpreting the information generated by technologies, said Sigal, is the creation of a frame for analysis. A set of events can occur that will not necessarily predict an outcome but make it more likely. For that reason, Global Voices analyzes, translates, and aggregates local citizen media for global audiences, focusing mostly on the developing world, and systematically tracks threats or events in fragile states. "We can see these events occur, almost like a rhythm, within a set of 50 to 60 countries around the world. That's reactive, but it gives us a policy framework for imagining where these events might occur."

He also noted that peacebuilding is not the only framework for looking at sensing and emerging conflicts. People involved in conflicts do not necessarily see them in a negative light. Through a lens of justice, democracy

building, or other activist frames, the same sort of data can be applied to a different agenda. He urged questioning "the normative assumption that conflict is always necessarily a bad thing. Because there is, I think, more of a continuum often between conflict which is creative, conflict which drives change, and conflict which is violent and negative."

THE NEW SOCIAL REALITIES OF CYBERSPACE

Cyberspace has created a new social reality, said Rafal Rohozinski, principal with the SecDev Group, and laws have not been well adapted to govern this new reality. The use of new technologies to either protect or deny rights has not been defined legally or normatively. The result can be strong disruptions and distortions in political systems depending on how those systems operate.

Rohozinski observed that Western governments to some extent exhibit what he called "the complacency of empire" with respect to information technologies. The Internet was invented, developed, and propagated around the world by the West. This technology, which has grown far beyond its original intended purpose, has created a platform for extending diplomacy through NGOs. The scale, scope, and reach of NGOs have expanded in ways that would not have been possible without the Internet, as have the business models of companies such as Google that were founded on the characteristics of the Internet. As a result, people in Western countries tend to take their freedom of navigation through cyberspace entirely for granted.

But the Internet is changing. The vast majority of Internet users are no longer in North America, which represents only about 13 percent of the global Internet population and is declining. Two-thirds of all global Internet users are under the age of 35, and 40 percent are under the age of 25. Three out of five new Internet users live in states that are considered either failed or at risk of fragility. "The center for innovation, the drive to create things in this space, the impetus to try to describe it in policy terms, is no longer in Washington, no longer in Ottawa, the UK, or anywhere else. It's shifting slowly but distinctly to the South and to the East," said Rohozinski.

This shift will have an impact on the governance of cyberspace, Rohozinski predicted. As people have come online, so have state interests and politics. This makes sense, said Rohozinski, since "a space that is colonized by a majority of your citizens is going to have all sorts of behaviors which, if those behaviors are translated into real life, would have real consequence." Thus, cyberspace has become a place to be regulated and policed.

Because of the way the Internet is run, governments do not have the ability to create the equivalent of a physical border around their corner of cyberspace and keep their citizens inside it while keeping others away. But they have an interest in doing so. One possibility is that in the future the Internet will no longer be neutral but will be subject to national laws. This could legitimate filtration, censorship, surveillance, and other forms of control pertaining to media, defamation, and other acts. People may no longer have the freedom of passage through cyberspace to which they are accustomed. Instead, the Internet could become much more fragmented and more like national telecommunication spaces.

One enabler of this change is that the intelligence in the Internet has shifted from the periphery to the center. Today, telecommunications providers have much more control over the Internet than in the past because they carry much more data, through television, mobile telephony, radio, and other forms of content. As a result, these companies are now able to measure, monitor, parcel, and direct traffic in ways that they could not before. As these central controllers pass cell phone service from one tower to the next, they can identify and track the user of that service. This may not matter as much in the United States as it does in other countries, but under authoritarian regimes, governments now have a way to know a lot about any individual "by essentially having them carry a digital dog tag everywhere."

Intelligent networks that enable this kind of monitoring are spreading fast outside North America. Advanced networks have greater penetration in some parts of Africa and Latin America than elsewhere, "which means those intelligent networks are being built exactly in the places where their capabilities can be turned inwards for surveillance purposes." Surveillance also has become a much greater undertaking since the days of wiretaps. Furthermore, because the media environment is more complex, the kind of data that individuals generate through systems to which they are connected is much richer. As a result, new players have entered into that space, both in the United States and elsewhere, and these companies can break encryption in almost real time, in part because law enforcement in the United States and elsewhere requires domestic surveillance to support the needs of law enforcement.

Governments have gotten much smarter about how to exercise their monopoly on the use of violence, force, and regulation not only within their physical borders but in cyberspace. National firewalls can prevent unwanted content going into or out of a country. Countries suffer negative consequences from erecting such barriers, so probably only about 12 to 15 do,

said Rohozinski, but more could do the same if they chose to create a border around their cyberperimeter.

Countries may also make information resources unavailable when it serves their purpose, through denial-of-service attacks, targeted filtering, or intentional disruption of protocols to make sure that opposition websites do not load. They may implement regulations and legislation to criminalize some online acts; in Belarus, for example, defamation of the president can be a cybercrime. Under this provision, the government can charge an independent media source with defamation and either filter a website or take it down. And governments can apply media law to all media content, forcing media to register locally or be subject to arbitrary filtration by the government. Finally, various activities can be criminalized, so that communication with known criminals, for instance, can become a criminal offense.

A final approach is to use technological means to identify and target dissent and to confound readers about posted information. For example, the Iranian revolutionary guard cyber command has a Facebook-like page where it posts pictures of protesters online and asks people to crowdsource who they are, which has the additional effect of intimidating people who might be considering activism. In Syria, for example, the regime uses a technique called "eggshelling" on Twitter. Eggshelling is a way for a regime to control discourse on the Internet by putting out messages with ambiguous registrations that appear to support the government's official positions. "Nobody really quite knows what it is. Is it a rumor? Is it really government stuff? If it's not, is it quasi-believable? The sheer volume of it ends up pushing to one side a lot of stuff that comes from the opposition, which is less connected." In other cases, criminal gangs have been hired to harvest damaging information or spread malware. Big data also can be misused; digitized census records or weapons registrations can be sold to third-party commercial entities that then sell them to risk security companies. "Although the initial collection of that data…may have been for a very worthy cause, the way that it's actually put to use by others ends up being antithetical to the kind of security that it was supposed to create for the community."

Some kinds of activism require a public presence, which often requires divulging identity, Rohozinski observed. Some people may be willing to risk jail because it legitimizes their actions and their movement. In other cases, activists may not use the Internet, may work through multiple virtual private networks, or may work through external relationships. But even then, security may be impossible. "I have a community of friends who are part of the core Russian opposition movement," said Rohozinski, "and they have

decided as part of their core tactics that they will do everything absolutely in the open. They have public meetings, and if you are not willing to be completely transparent about who you are and what your intentions are you can't show up, because they figured they can't beat the Russian security."

There is some good news, said Rohozinski. "The more authoritarian a regime is, the more they're caught in their own trap." Governments want the benefits of modernization without the liabilities, yet the two are not easy to separate. "They want it both ways and realize that they can't have it. They want to be connected and benefit from being members of a global community where science is cheap, where supply chains are accessible, etc., but at the same time they don't want the politics of it." As a result, governments do not want to jettison or ignore systems that activists can use to get around government restrictions. "Their headlong rush into the modern world also ties their hands because of the dependencies that it creates for them internally as well as externally." What may be necessary in such an environment is to counter disinformation, as in the days of the Cold War. "Cyberspace is going from being the exceptional domain to one that reflects the complexity of real life. So I'm an optimist," Rohozinski said.

Rohozinski also recommended looking at the work done by the World Health Organization on violence mapping and prevention as a public health issue. This work has combined precursor indicators of violence, drawn from such measures as demographics, economic conditions, reports of homicide, and the prevalence of a grey economy to gauge the likelihood of conflict at different levels. For example, the introduction of policing in ungoverned spaces in Brazil has relied heavily on this public health approach of understanding the precursors of violence, including messages sent on social media. This is a slightly different approach to the application of technology, because it is more about raising awareness. This awareness has not necessarily translated itself into action by the peacebuilding community, "but it should be incorporated."

Rohozinski observed that security services are starting to be seen as a necessity, not an option. The professionalization of the provision of security tools will happen through market forces, which will gradually displace efforts offered through government agencies or other sources. USIP and the NAE could contribute to this evolution, he said, by acting as a focus of innovation for peacebuilding activities in both the public and private sectors.

Individuals and organizations that recognize the new reality will be the ones that survive, he said, so training is essential to ensure that they remain up to date about the tools they use. The US State Department offers many

good programs that can help prepare civil society organizations for the environments in which they operate, he said. He also pointed to organizations—domestic and international, public and private—that offer technical advice. "I don't know if anybody has done an inventory of them, but there's quite a few and they're actually pretty good."

Rohozinski concluded that cyberspace is now a domain where conflicts will occur and need to be mediated. It is a space of maneuver, not one where people have freedom of navigation. It will need to be treated like physical terrain, and individuals and organizations will need the capacity to operate in it as they do in physical space.

DISCUSSION

Several participants discussed various negative applications of technologies. Dennis King reiterated the use of new technologies to spread misinformation, disinformation, rumors, and incitement. Once incorrect information goes viral, correcting mistaken ideas can be very difficult. The fact that regimes use the new technologies to target individuals and organizations is more apparent with the use of social media than in the past. "Individuals connected to NGOs who've been involved in promotion of governance and technology have been imprisoned, killed, and attacked, and their NGOs have been banned," he said. "The humanitarian space is already dwindling and shrinking. This is another way that the bad guys, the dark side, can further use [technology] to shrink the humanitarian space and access, and target civilians and human rights activists."

Sanjana Hattotuwa asked what would happen if 3D printers could be used to make exact digital duplicates of AK47 rifles? In this and other ways, technology could be used to exacerbate rather than prevent conflict.

Chris Spence cited the social component of misuse, beyond the technical issues. People are fooled into giving up their passwords, or they let their computers be taken over by malware. "No matter what we do, the humans who aren't thinking about this every day are the ones who are the soft targets." Although his staff rely heavily on training, even they remain a target.

Sigal said that security is a process and not an end state. It requires continual investments as well as attention to the tools used to protect security, which can be turned against their creators to erode security. Hackers in some countries have been able to reverse engineer security tools and thereby put people at risk. "We need a Google for security," he said, "a company that sees a business model in providing" security services.

He also added that the dark side/light side division, or skeptic versus utopian, is a misleading way of framing the issues. People accused of being utopians are often the most skeptical, because they have the practical experience of trying different things and realizing what works and what does not work.

5

Major Issues Discussed at the Workshop

This final chapter captures the major issues that arose repeatedly during the workshop discussions. The most significant revolved around the question of how peacebuilders can use data gathered from sensors, online communications, and other sources to shape emerging conflicts. The other issues concerned the existence and significance of a digital divide, the role of the private sector, and the need for unity among peacebuilding organizations.

FROM SENSING TO SHAPING

Fred Tipson set the context for the discussion of shaping policies on the basis of data by noting that the peacebuilding community often lacks actionable strategies to convert sensing into shaping. Early warnings, for example, can help people get out of the way, whether or not they change the course of events. The focus needs to be on how to assist the people involved to avoid the worst consequences of potential deadly violence. A continual challenge, he said, is "to think about how to translate information into action."

One need is to engage policymakers who are in a position to shape conflicts. Several workshop participants observed that the Arab Spring movement has not been as influential as many hoped because it has been unable to gain much political representation and engage political institutions. As Chris Spence observed, the situation has been in some ways analogous to the

Occupy Wall Street movement, a leaderless movement that has been largely ineffective in bringing about policy change, compared with the Tea Party movement, which has been able to engage political institutions.

Libbie Prescott, strategic advisor to the US Secretary of State on science and technology, noted that the subject of political will arose several times during the workshop. Not all policymakers are comfortable with data and methodologies, she observed, and the information gathered through sensing may not be as self-evident to those who need to express the political will to act. Policymakers have preexisting agendas, and just presenting them with data does not guarantee a response. Presentations may need to be adapted to the individual. "The same data will not convince [different] people of the same outcome regardless of how accurate the data is. I don't know if there is a technological fix for that, but it's something to keep in mind."

Prescott added that political will depends on a combination of the perceived certainty of information, the perceived cost of action, and the perceived cost of inaction. Data measurement and transparency can strongly influence these perceptions. As Secretary Clinton has said, data not only measure progress but inspire it. "Providing data in these environments allows for better accountability and greater governance," Prescott said.

Prescott also asked whether a society is better off being able to detect something if it has no ability to change that thing. Surveillance is useful when there is a clear way to act on the information gathered. When policymakers receive information, they typically want to know what to do next, and asking for more money to study the situation further is typically not a satisfactory answer. If specific recommendations for action are lacking, policymakers may distance themselves from those who put them in an awkward situation, she said.

Neil Levine, director of the Office of Conflict Management and Mitigation at USAID, elaborated on this point by observing that early warnings often present decision makers with the difficulty of uncertain information and high costs. Sensing can help by clarifying the certainty or uncertainty of the information. Also, to the extent that sensing provides information further in advance of the onset of violence, it broadens the choices for policymakers and often reduces the cost.

Also on the issue of political will, Sanjana Hattotuwa noted that an emerging information landscape will make it more difficult for policymakers not to act when presented with actionable information. Information about atrocities such as ongoing genocides will inevitably reach the rest of the world rather than staying in a particular region, as might have happened in

the past. Policymakers may still choose not to act, but not because of a lack of information.

THE DIGITAL DIVIDE

Despite the rapid advances of technologies in recent years, several workshop participants wondered whether digital divides between individuals, groups, regions, and countries still limit progress in the application of technology to peacebuilding. As technologies have become less expensive and more widespread, concerns about creating a culture of information haves and have-nots have faded, Prabhakar Raghavan noted, although he recognized that digital divides have not completely disappeared. But Moore's law, which holds that computing power roughly doubles every two years, promises that divides will continue to diminish as computing devices become cheaper and more powerful.

Lawrence Woocher wondered whether digital divides will persist as more advanced technologies appear. "Perhaps we shouldn't assume that there's going to be a convergence but just a continuing trajectory upward around the world, [with] different paces for different places." Raghavan acknowledged that the divide may never completely disappear, but technologies no one thought would become global are becoming routine everywhere, even though they may not spread in their most advanced form.

Duncan Watts clarified that inequality in communications technology is substantially smaller than other forms of inequality, such as access to health care, clean water, transportation, or education, and may even help reduce some of these other forms of inequality. Innovation will almost always accrue first to the wealthier parts of the world, he said, but inequality is less striking in communications than in other areas.

THE ROLE OF THE PRIVATE SECTOR

The role of the private sector in both advancing technology and contributing to peacebuilding came up in several contexts. Hattotuwa expressed concern about the privatization of information, noting that he is more comfortable with information being held by the United Nations than by corporations or other private organizations. Even when corporations want to be helpful, they may use information in a manner that differs from the expectations of the people who provided it.

Rafal Rohozinski made the related point that how the Internet functions depends on the deliberate acts of individuals and institutions. A generation of individuals has been behind the institutions running the Internet for the past 25 years, and that generation is now retiring. Instead, commercial interests are starting to colonize those institutions, including companies outside the United States.

Raghavan countered that companies want to not only make a profit but continue to exist. That desire "is not well served by doing anything that's tactically expedient and strategically evil." Companies such as Twitter have tried to act in a responsible manner, while institutions like the United Nations do not necessarily have the infrastructure to undertake similar functions. "Hopefully the people running these companies aren't going to compromise their long-term integrity for a quick buck."

Private companies may, however, apply standards to the posting of information. Fred Tipson recalled a comment made at a meeting by a Syrian activist who said that he and his colleagues count on YouTube to document the atrocities of the regime and mobilize the Syrian people and the international community. But YouTube has standards about what it will and will not allow in video depictions of violence and cruelty, which can undermine this strategy. Similarly, Google makes decisions about what to make available in different countries and what not to make available. "How transparent should the process be by which Google makes decisions around those issues?" There are no authoritative standards for privacy, transparency, or responsibility. "I think Google is trying to behave as responsibly as they can. I know they usually require a legal standard before they will take down something. . . . But that still raises the question of whether or not these activists deserve transparency in allowing people to see how awful the behavior of the regime has been."

Companies confront the same ethical difficulties as other holders of information. In modern and open societies, information almost inevitably comes out after the fact, heightening the tension between transparency and caution. If analyses of information generate serious concern, should that information be made public, even if it could cause a panic? As smartphones make it possible to identify at least the approximate locations of their users, will phone companies allow geographic information to be sent with text messages? These are among the many practical questions that need to be answered as technologies continue to diffuse throughout societies.

Finally, Rohozinski made the point that global Internet companies should be worried because the creation of digital borders in cyberspace

through economic or political means could unravel their business models. These companies, too, have a vital interest in peacebuilding and in the free flow of information across borders. But the international rules relating to government controls on the Internet are up for renegotiation at the upcoming World Conference on International Telecommunications (WCIT-12), December 3–14 in Dubai.

THE NEED FOR UNITY

Rita Grossman-Vermaas, senior international policy advisor for Logos Technologies, spoke about the need for greater collaboration and coordination between the peacebuilding and technology communities. For example, the peacebuilding community could identify the nature of conflicts and become part of the process to determine what kinds of technologies might be applied most usefully to those conflicts, from text messaging to satellite imagery.

Hattotuwa approached this issue in a somewhat different way. Some groups in the peacebuilding community demonstrate a marked resistance to sharing information, he said, and even are reliant on withholding information. "The assumption that the peacebuilders themselves are benevolent creatures working in the best interests of their communities and their nations and their peoples is, I think, something that we need to question, because that is not always the case."

Melanie Greenberg called attention to the intersection of peacebuilding organizations with organizations focused on democracy, development, health, education, and other issues as a way of building unity. Many of these organizations increasingly see themselves as engaged in peacebuilding, she said, and even those that do not are sensitive to doing their work in such a way as not to exacerbate tensions.

Patrick Vinck similarly pointed to the need to develop collaborations between established organizations and new organizations that have emerged around specific technologies. He mentioned Human Rights Watch and Physicians for Human Rights, which have considerable expertise with consent forms that new organizations could use.

Noel Dickover called for efforts to bridge the gap between formal organizations and the volunteer technology community. People will show up at a crisis. The Red Cross now brings in technology volunteers in the same way they do people for food distribution. Can other institutions take advantage of technology volunteers to build a situational awareness network?

LOOKING AT THE BIG PICTURE FOR PEACEBUILDING AND TECHNOLOGY

In wrapping up the workshop, Woocher returned to his original observation that peacebuilding is very broad and encompasses many different activities. He noted that the workshop was most successful in generating practical ideas when participants considered specific applications of technology, such as election monitoring. One way to extend this success may be to move discussions into the field. An example of this, noted earlier in the day by Dickover, is technology camps, where people go to a community and work with local actors could facilitate the identification of key issues and approaches to moving forward.

Tipson spoke more broadly of the need for groups to know what kinds of societal goals they wish to achieve. "To some extent the peacebuilding community talks too much about peace and not enough about the agendas that peace should be part of." If an organization's only objective is peace, someone who does not have that objective has a major advantage. Peacebuilders need a positive agenda that attracts new and different sets of players for whom nonviolence is a key objective. "That's true in all of the peacebuilding problems that we're looking at—there has to be a broader agenda for what change we want to see a society accomplish."

As an example, Tipson pointed to the need to be more insistent about determining rules governing the Internet. Governments need to come together to develop "some kind of consensus around the way the Internet and these technologies surrounding it are going to be managed," he said. The United States needs to be proactive in engaging with other countries to counter the efforts of the governments of China, Russia, and other countries to advance a more restrictive approach. As governments have gotten more sophisticated in their approaches to controlling communications, countries and groups that support liberalization need to become more sophisticated as well.

Technology can serve civil disobedience and civil mobilization, Tipson said, as a component of broader strategies for political change. It can help people organize and mobilize around particular goals. It can spread a vision of society that contests the visions of authoritarian regimes. And it can contribute to experiments in peacebuilding, such as better elections or formal "truth and reconciliation" processes.

Tipson urged the workshop participants to clearly identify peacebuilding problems and then ask how technology could help solve those problems. The problems may be related to conflict prevention, conflict management,

dispute resolution, postconflict reconciliation, or opposition to authoritarian regimes. Those involved in peacebuilding and technological development can benefit by working together to determine what capabilities would help in each of these settings, and how technology can help provide those capabilities.

Appendix A

Agenda

NAE-USIP Roundtable: Workshop on Sensing and Shaping Emerging Conflicts

October 11, 2012

National Academy of Sciences
2101 Constitution Avenue NW, Room 120
Washington, DC

The Objective of this Workshop is to identify major opportunities and impediments to providing better real-time information to actors directly involved in situations that could lead to deadly violence. We will consider several scenarios of potential violence drawn from recent country cases, and consider a set of technologies, applications, and strategies that have been particularly useful—or could be, if better adapted for conflict prevention or mitigation by people in a position to do so.

AGENDA

8:30 a.m. **Breakfast**

8:45 a.m. **Roundtable Charge to the Workshop**
By the end of the day, we seek to identify promising strategies for direct application of technology tools and techniques to emerging conflicts. The goal is to provide insights and information to inform the design of field tests of collaboration between local actors, supportive peacebuilders, and expert technologists to increase the constructive impacts of sensing technologies and applications.
Roundtable Advisor: *Fred Tipson, USIP*

9:00 a.m. **"Peacebuilders" Meet "Data Scientists"**
How can various sensing technologies assist local populations and peacebuilders in zones of conflict or potential conflict to anticipate, understand, and prevent deadly violence?

Candidate Peacebuilding Problems/Settings
Joint Presentation: *Lawrence Woocher, SAIC*
Dennis King, State Department
Fred Tipson, USIP

Candidate Technologies:
Joint Presentation: *Prabhakar Raghavan, Google*
Duncan Watts, Microsoft
Patrick Vinck, Harvard Humanitarian Initiative

10:30 a.m. **Break**

10:45 a.m. **Recent Experience in Zones of Tension/Conflict**
How was technology used by local actors, whether citizens, government agencies, or outsiders, to understand their situations and influence the outcomes of events?
Speakers: *Patrick Meier, Ushahidi (Kenya)*
Sanjana Hattotuwa, ICT4Peace (Sri Lanka)
Moderator: *Lawrence Woocher, SAIC*

12:15 p.m. **Lunch and PeaceTech Lab Presentation**
Speaker: *Sheldon Himelfarb, USIP*

1:00 p.m. **Factors Affecting the Use of Technologies in Conflict Settings**
What is the process, whether facilitated or not by outsiders, by which technologies are adopted/adapted in local settings? What are the challenges these capabilities could best address?
Speakers: *Chris Spence, National Democratic Institute*
Emmanuel Letouzé, UN Global Pulse
Commentator: *Joseph Bock, University of Notre Dame*
Moderator: *Prabhakar Raghavan, Google*

2:30 p.m. **Break**

2:45 p.m. **The Darker Side of Technologies Used to Sense Conflict**
For all of the potential benefits of various technologies in facilitating political participation and change, various actors may take advantage of these very capabilities to repress change and even provoke deadly violence. What are the ways that repressive governments or reactionary groups have exploited technologies (or might do so) to stifle expression or target activists, and how can these "darker" uses be prevented or mitigated?

Speakers:	*Ivan Sigal, Global Voices*
	Rafal Rohozinski, The SecDev Group
Moderator:	*Lawrence Woocher, SAIC*

4:15 p.m. **Next Steps**

5:00 p.m. **Adjourn**

Appendix B

Attendees

NAE-USIP Roundtable:
Workshop on Sensing and Shaping Emerging Conflicts

October 11, 2012

National Academy of Sciences
2101 Constitution Avenue NW, Room 120
Washington, DC

Cochairs

Prabhakar Raghavan
Vice President of Engineering
Google

Lawrence Woocher
Research Director
SAIC

Steering Committee Members

Dennis King
Senior Humanitarian Affairs Analyst
Humanitarian Information Unit
US Department of State

Neil Levine
Director, Office of Conflict Management and Mitigation
US Agency for International Development

Patrick Vinck
Research Scientist, Department of Global Health and Population
Harvard Humanitarian Initiative

Duncan Watts
Principal Researcher
Microsoft Research

Expert Participants

Joseph Bock
Director of Global Health Training, Eck Institute for Global Health
University of Notre Dame

Richard Boly
Director, Office of eDiplomacy
US Department of State

Jim Coffey
The MITRE Corporation

David Combs
Aerospace Experimental Psychologist
Naval Research Laboratory

Noel Dickover
New Media Advisor, Office of eDiplomacy
US Department of State

Katie Dowd
Innovation Advisor to the Secretary
US Department of State

Christina Goodness
Chief, Peacekeeping Information Management Unit
United Nations

Melanie Greenberg
President and CEO
Alliance for Peacebuilding

Rita Grossman-Vermaas
Senior International Policy Advisor
Logos Technologies, Inc.

Nate Haken
Senior Associate
The Fund for Peace

Sanjana Hattotuwa
Special Advisor
ICT4Peace

Joseph Hewitt
Evaluation Specialist
US Agency for International Development

Emmanuel Letouzé
Technology Consultant
UN Global Pulse

Matthew Levinger
Director, National Security Studies Program
George Washington University

Bob Loftis
Independent Consultant

Philippe Loustaunau
Open Source Indicators Program
IARPA

Kay McGowan
Senior Policy Advisor for Afghanistan
US Agency for International Development

Patrick Meier
Director of Social Innovation
Qatar Computing Research Institute

Libbie Prescott
Strategic Advisor to Science and Technology
Advisor to the Secretary
US Department of State

Rafal Rohozinski
Principal
The SecDev Group

Elmer Roman
Oversight Executive, Office of the Secretary of Defense
US Department of Defense

Ivan Sigal
Executive Director
Global Voices

Chris Spence
Chief Technology Officer
National Democratic Institute

Maria Wrzosek
Bureau of Population, Refugees, and Migration
US Department of State

Staff Participants

Genève Bergeron
Program Assistant
US Institute of Peace

Jeff Canfield
Interagency Professional in Residence
US Institute of Peace

Sheldon Himelfarb
Director, Center of Innovation for Science, Technology and Peacebuilding
US Institute of Peace

Sue Nelson
Interagency Professional in Residence
US Institute of Peace

Greg Pearson
Senior Program Officer
National Academy of Engineering

Proctor Reid
Director of Programs
National Academy of Engineering

Andrew Robertson
Senior Program Officer
US Institute of Peace

Ryan Shelby
Christine Mirzayan Science & Technology Policy Fellow, J. Herbert Hollomon Fellow
National Academy of Engineering

Frederick S. Tipson
Special Advisor, Center of Innovation for Science, Technology, and Peacebuilding
US Institute of Peace