global issues

The Evolving Internet

An Electronic Journal of the U.S. Department of State - November 2003 Volume 8, Number 3

From the Editors

Each day brings new examples of how information and communication technology (ICT) is reshaping the lives of people around the world. To one degree or another, the digital revolution has arrived in just about every corner of the globe. In recognition of this, representatives of the world's nations will gather in Geneva this December for the World Summit on the Information Society to discuss how access to ICT might be achieved for all people.

On the Internet and the World Wide Web, people are governing, learning, communicating, debating, "politicking", shopping, and experimenting—conducting all kinds of interactions in ways only made possible by ICT. The Internet has brought into being a virtual world that, like the universe itself, is expanding every moment, full of promise, hope, and not a little mystery. But challenges remain if it is to achieve its full promise. The United States, in partnership with other governments, international organizations, and citizens of many countries, is committed to assisting people around the globe to meet these challenges so that this virtual world becomes a helpful and productive part of their everyday lives.

Among the articles in this edition of Global Issues, senior U.S. government officials outline priorities for Internet development and discuss U.S. assistance programs to help develop ICT skills, training, and access in developing countries. A U.S. lawmaker describes how the Internet can help create a more open and transparent society, and a scholar reviews efforts to bring the Internet into elementary and secondary schools. Finally, private sector experts explore the problems and challenges of protecting computers and the information they contain.

We hope that by considering the variety of issues and concerns presented in this journal, readers will gain a greater understanding of and appreciation for the digital revolution and their potential role in it.

global issues
An Electronic Journal of the U.S. Department of State
November 2003 Volume 8, Number 3

Table of Contents

The Evolving Internet

❑ FOCUS

❑ COMMENTARY

❑ ADDITIONAL RESOURCES

Global Issues

An Electronic Journal of the U.S. Department of State

ejglobal@pd.state.gov

Editor	William Peters
Managing Editor	Charlene Porter
Text Editor	Jim Fuller
Internet Editor	Tim Brown
Contributing Editors	Jenifer Bochner
	Cynthia LaCovey
	Vicki Silverman
	Gerri Williams
Reference and Research	Lynne Scheib
	Joan Taylor
Art Director	Chloe Ellis

Publisher	Judith S. Siegel
Executive Editor	Guy E. Olson
Production Manager	Christian Larson
Assistant Production Manager	Sylvia Scott
Editorial Board:	George Clack
	Kathleen R. Davis

The Bureau of International Information Programs of the U.S. Department of State provides products and services that explain U.S. policies, society, and values to foreign audiences. The Bureau publishes five electronic journals that examine major issues facing the United States and the international community. The journals—*Economic Perspectives, Global Issues, Issues of Democracy, U.S. Foreign Policy Agenda, and U.S. Society and Values*—provide statements of U.S. policy together with analysis, commentary, and background information in their respective thematic areas.

All issues appear in English, French, Portuguese, and Spanish language versions, and selected issues also appear in Arabic and Russian. English-language issues appear at approximately a one-month interval. Translated versions normally follow the English original by two to four weeks.

The opinions expressed in the journals do not necessarily reflect the views or policies of the U.S. government. The U.S. Department of State assumes no responsibility for the content and continued accessibility of Internet sites linked to herein; such responsibility resides solely with the publishers of those sites. Articles may be reproduced and translated outside the United States unless the articles carry explicit copyright restrictions on such use. Potential users of credited photos are obliged to clear such use with said source.

Current or back issues of the journals, and the roster of upcoming journals, can be found on the Bureau of International Information Programs' International Home Page on the World Wide Web at http://usinfo.state.gov/journals/journals.htm. They are available in several electronic formats to facilitate viewing online, transferring, downloading, and printing

Comments are welcome at your local U.S. Embassy or at the editorial offices:

Editor, Global Issues & Communications
Bureau of International Information Programs
IIP/T/GIC
U.S. Department of State
301 4th Street, S.W.
Washington, DC 20547
United States of America
E-mail: (ejglobal@pd.state.gov)

The Digital Dimension of Development: A Strategic Approach

By Ambassador David A. Gross
Coordinator for International Communications and Information Policy
U.S. Department of State

A top U.S. diplomat says the freedom to innovate, create, and share ideas is critical to development. He describes how the U.S. government is utilizing information and communications technology to achieve development goals.

"In the new century, growth will be based on information and opportunity. Information drives markets, ensures a rapid reaction to health crises like SARS, and brings new entrepreneurial opportunities to societies....The keys to prosperity in an information economy are education, individual creativity, and an environment of political and economic freedom. An environment of economic and political freedom is the sina qua non for the kind of progress we are talking about."

Secretary of State Colin L.Powell
Before the World Economic Forum
June 22, 2003

Over the past decade, breathtaking advances in information and communications technology (ICT) have changed the way we live, learn, and do business.

Whether it is responding more rapidly to health crises like SARS (severe acute respiratory syndrome), delivering education to the underserved, increasing government transparency, or creating new forms of commerce, technology is transforming our world.

ICT has become the new tool for achieving economic and social development. In fact, a growing global consensus has emerged in recent years that information-based technologies are fundamental to meeting basic development objectives.

The future prosperity and well being of all nations, including the United States, now depend in part on our ability to access and use these new tools effectively.

> “Our overriding vision for the information society is one that expands political and economic freedom by offering our citizens the opportunities to access and utilize information to better their lives.”
>
> Ambassador David A. Gross

For much of the world, however, that remains an elusive goal. The number of Internet users in the world today exceeds 500 million but some 40 percent of that number live in the United States. Over the past 10 years, global telephone penetration rates have doubled, but there are still more telephone landlines in New York City's borough of Manhattan than in all of Africa. On the other hand, technology is dramatically changing things almost everywhere—for example, there are now many more wireless phones in Africa than traditional landline phones.

World Summit on the Information Society

The upcoming United Nations World Summit on the Information Society (WSIS), scheduled for December 10-12 in Geneva, will focus precisely on these challenges.

The summit, the latest in a series of U.N. summits focused on development, will be attended by more than 50 heads of state and government from around the world. A second phase of the summit will be held in Tunis, November 16-18, 2005. Leaders from business, civil society, and international organizations are contributing to preparations for both phases.

The summit's mission is to outline a clear vision and a concrete plan for putting ICT into the service of development.

What considerations should guide the Summit's work?

Development begins with freedom. The freedom to innovate, the freedom to create, and the freedom to share ideas with people around the world are the foundation of a global, inclusive information society. Our overriding vision for the information society is one that expands political and economic freedom by offering our citizens the opportunities to access and utilize information to better their lives.

More specifically, we believe success in making freedom possible and crafting an ICT-for-development agenda depends on three fundamental building blocks.

A Strategic Approach

First, we believe countries should focus on creating a domestic policy environment that encourages privatization, competition, and liberalization, and that protects intellectual property.

Private investment is by far the largest source of funds for the development, deployment, maintenance, and modernization of the world’s communications and information networks and facilities. Public policies that do not actively invite such investment simply delay development.

Around the world, there are encouraging signs that rules favoring competition are paying big dividends. In Uganda, for example, a price war broke out last year in the country's competitive telecommunications sector. Costs per minute for telephone calls tumbled and some firms scrapped fees. The result has been more opportunities for entrepreneurs and cheaper rates for all users.

Second, it is critical to build human capacity. Users must have the ability to effectively use ICT tools. Without adequate education and training, infrastructure investments will yield little.

Teachers, school children, health professionals, citizens, and business people must have the knowledge needed to take full advantage of distance learning, e-healthcare, e-government, and e-business applications.

To be used effectively, ICT tools also must be adapted to local needs. Local content that reflects local culture and is in the language of the users' choosing is vital to sustaining the effective use of ICT. The U.S. government believes such content should be widely available.

At the same time, content restrictions must be avoided. Uncensored print and broadcast media provide independent and objective information and offer a vehicle for citizens to openly and freely express their opinions and ideas.

Artificial barriers that unnecessarily restrict the free flow of information and news are the enemies of innovation, retard the creation of knowledge, and inhibit the exchange of ideas that are necessary for people to improve their lives.

The realization of the many "digital opportunities" that ICT tools make possible depends on access to information. Electronic government, for example, can increase government transparency, accountability, and accessibility and lead to better development decisions as long as governments are prepared to share information with their citizens.

Third, users must be able to use ICT with confidence if the economic and social benefits of these technologies are to be achieved. Network security ICT tools and networks can never be made invulnerable to attack. But countries can protect their ICT infrastructure by adopting effective, substantive, and procedural laws.

Companies, consumers, and citizens can contribute as well by raising awareness and implementing widely recognized network security guidelines compiled by the United States and its partners in the Organization for Economic Cooperation and Development. Together we can create a global culture of network security that protects all users, no matter where they live.

In addition to creating the right policy environment, building human capacity, and protecting networks, governments also must avoid erecting new hurdles that will undermine efforts to harness ICT to development goals.

Whether it is weakening intellectual property protections, limiting press freedoms, or injecting governments unnecessarily into the technical management of the Internet, such misguided steps can quickly reduce choice, stifle innovation and democracy, and raise costs.

Partnerships for Development

The U.S. government's involvement in WSIS is only one aspect of our commitment to using ICT to foster development. Over the years, many of our assistance programs have incorporated ICT to achieve economic and social goals.

The Digital Freedom Initiative (DFI) is one of the leading examples of the U.S. government's (USG's) commitment to using the latest tools to achieve longstanding development goals. The program builds on previous USG initiatives, including the Leland Initiative, which was launched in 1996, and the Internet for Economic Development, which was launched in 1999.

The DFI promotes the use of ICT by entrepreneurs and small businesses in developing countries and leverages existing infrastructure to improve access to local, regional, and global markets. It also assists countries in creating a pro-competition policy and regulatory environment that will help entrepreneurship blossom.

The pilot program was announced in March 2003 at a White House ceremony and was first launched in Senegal. At the October 20-21 Asia-Pacific Economic Cooperation (APEC) leaders meeting in Bangkok, President Bush announced that Peru and Indonesia would join the program.

Over the next five years as many as a dozen countries may be invited to join the initiative.

The U.S. government advances ICT-for-development through numerous other programs. These include:

- Literally hundreds of individual U.S. Agency for International Development projects that use ICT to address health, education, and capacity issues;

- State Department-sponsored "e-logistics" workshops that provide practical real-world advice to developing country business owners, especially small and middle size enterprises eager to improve productivity and expand into new markets;

- Regulatory and technical training programs sponsored by the U.S. Telecommunications Training Institute, which, over the past 20 years, has graduated more than 6,200 ICT professionals from 163 developing countries; and

- A $30 million Internet Access and Training Program (IATP) that develops Internet skills and computer knowledge among diverse populations in Eurasia while promoting the free flow of information and ideas.

Whether it is these programs, a new initiative to promote the spread of wireless technologies, or efforts to raise awareness about the value of "electronic government," all our ICT-for-development programs rest on the building blocks outlined above.

We believe that these building blocks can help all countries achieve their digital progress and prosperity agendas, thereby helping the children and generations to come.

E-Government: The Next American Revolution

By U.S. Representative Tom Davis
Chairman, House Government Reform Committee

A member of the U.S. Congress explains how information technologies can help government better serve citizens.

Electronic government can reinvent the way citizens and businesses interact with the government. As an elected representative of the people of Virginia and a congressional leader in information technologies, I share this belief with the Bush administration and many of my colleagues in the U.S. Congress.

E-government is not just a theory or concept; it's already a reality, and destined to expand. Given time and resources, e-government really can revolutionize Americans' relationship with their government.

We often talk about how e-government can make governments more efficient and less costly, and certainly that's an important part of the equation. Just as important, however, are the ways in which e-government can better serve our citizenry. Americans see the benefits of e-government going beyond its capability to provide better or more cost-efficient services. They regard it as a way for citizens to become better informed and more involved in government.

Online government services provide information on lawmakers voting records, and the ability for constituents to offer comments on legislation or monitor hearings over the Internet. E-government gives citizens the ability to access online student loan applications. It can spare the public long waits in line to register a car or renew a license.

The Internet has made communicating with my constituents easier and faster. In recent years the amount of correspondence I've received on any and all issues has increased exponentially, due mostly to e-mail letters. I've installed a software program in my offices that allows me to quickly sort these messages and respond in a timely manner. This is a win-win scenario. I'm better able to gauge where my constituents stand on important issues, and I'm able to respond to them more quickly than traditional mail service permits.

Legislative initiatives in which I'm involved are described on Web sites supported by my congressional office and the House Government Reform Committee, which I chair. On these Web pages, I'm able to inform the public in "real time" about what we're voting on, what we're investigating, and what services are available. Constituents can turn to my Web sites for routine information about when the House of Representatives might vote on a bill of interest, or for information that can help in an emergency, such as a recent hurricane that struck my district and the entire mid-Atlantic region.

Constituents can also go online to join hearings that are held before the Government Reform Committee. When top administration officials come before my panel testifying about homeland security, emergency preparedness, or Internet vulnerabilities, the public can view the hearing in a Webcast just as if they'd made the trip to Washington. This all represents good government at its best.

Yet while the potential benefits of e-government are plentiful, the remaining challenges are profound. While the federal government is certainly making progress, in too many areas we're still moving at "old economy" speed.

Most government entities have Web sites, and more and more constituents are communicating with their representatives via e-mail. Governments are moving to the Internet for basic transactions, online procurement, and information dissemination. Despite these positive trends, federal, state, and local governments are still in the early stages of recognizing the real potential of e-government.

There is still much work to be done. We need to find new and innovative ways to make services more user friendly. The Web-savvy citizen of the 21st century is accustomed to the standard of service provided by commercial Web sites, and will accept nothing less from government sites.

> "Yet while the potential benefits of e-government are plentiful, the remaining challenges are profound."
>
> Tom Davis

We need more effective leadership and management. We need to develop a stronger "citizen-as-customer" focus. We need more reliable software and hardware. We need more sophisticated technical expertise.

The federal government has created more than 20,000 Web sites, so information can be hard to find. Some information remains difficult to locate because some agencies remain focused on posting their priorities rather than the services their customers demand.

We need to better assuage concerns about security, privacy, and access. By more than two-to-one, Americans say they want to proceed slowly rather than quickly in implementing e-government because of concerns about security, privacy, and access. Americans view e-government through the same lens with which they view the Internet: very positive, but not entirely trusting.

The high degree of interdependence and interconnectivity between information systems, both internally and externally, exposes the vulnerability of the federal government's computer networks to both benign and destructive disruptions. This factor is important to understanding how we devise a comprehensive and flexible strategy for coordinating, implementing, and maintaining information security practices throughout the federal government as the rising threat of electronic terrorism emerges.

Finally, the government has a moral obligation to address digital divide issues so that computers and Internet access are not available only to those who can afford these technologies and the opportunities they provide to reach out to government and the world. I want ALL of my constituents to be able to contact me via e-mail, not just the ones with a personal computer in their homes. Creativity in this regard will be vital. We should consider, for example, whether we can post computer kiosks in our grocery stores or shopping malls to create equal access and opportunity to take advantage of the ease and convenience of obtaining government services online.

Indeed, with the advent of lightning-speed communications enabled by the Internet, the networked world is creating new demands on government services from consumers—demands that require immediate response. With the ability for citizens to e-mail and communicate with federal agencies directly, Congress and the administration must efficiently manage the federal government by providing the resources to make sure the government can deal with new demands.

As we continue to move forward, we must ensure that our government is utilizing the latest technologies to improve operational efficiencies, ensure confidentiality and privacy of information, and streamline the delivery of services. I think if we use technology to our advantage, it will prove to be the best vehicle we have for the creation and maintenance of good government.

The opinions expressed in this article are those of the author and do not necessarily reflect U.S. government policy.

Bringing Africa Online

By Lane Smith
Coordinator, Leland Initiative
U.S. Agency for International Development

Since 1996, the U.S. Agency for International Development has been working closely with African leaders and the private sector to bring Internet connectivity to Africa, through a program celebrating a U.S. Congressman who had dedicated his career to, and lost his life while, promoting development among countries on the continent.

The U.S. Agency for International Development (USAID) has been working for seven years to help African leaders bring information and communication technology (ICT) to their countries and to teach their citizens how to use it. USAID programs, based in partnerships with local-level institutions and private-sector donors, have provided an estimated 2 million Africans with Internet access, a number that is growing daily.

That figure represents a significant proportion of the total 8.9 million Africans now online.[1] Thanks to these pioneering efforts, an ICT success story is emerging, showcasing the positive results that can be achieved when African policy-makers and entrepreneurs are brought together with the best technology and know-how that the United States can offer.

These achievements have been accomplished under a program we call the Leland Initiative. It is named for Mickey Leland, a U.S. Congressman from the state of Texas who died in a plane crash while on a famine relief mission to Ethiopia in 1989. Throughout his career, Congressman Leland fought to bring the benefits of development to the people of Africa. The Leland Initiative was launched in June 1996 to help bring the information revolution to Africa in tribute to Congressman Leland's dedication and commitment to people everywhere.

In the mid-1990s, only a handful of countries in Africa had Internet access. This usually was limited to slow and expensive e-mail service in the capital city. Today, all 44 sub-Saharan African countries have access that, in most cases, extends to cities and regions far beyond the capital. Hundreds of Internet service providers (ISPs) have sprung up, and thousands of cybercafes offer fee-paying customers access to computers connected to the Internet. The

Leland Initiative established the principal Internet gateway and national connection for 10 of those countries.[2] In 16 additional countries,[3] the Leland Initiative and the local USAID missions have delivered access to major institutions such as universities, parliaments and private sector groups. In all countries, citizens experience the impact of Leland in the form of a more vibrant market, better access, and lower prices.

The accomplishments of this initiative must be measured in more than technology and access, however. Courageous African leaders saw the Leland Initiative as an opportunity to change government monopolies in telephone services, the traditional but discredited approach. African and U.S. private sector entities responded vigorously and rapidly to the opportunities that these policies created. With the groundwork laid by the Leland Initiative, private companies have invested capital, established businesses, built infrastructure, and aggressively pursued new business opportunities.

The Leland Principles

The Leland Initiative was conceived to work in several substantive areas that we've called the three "P's," which stand for **p**olicies, **p**ipes, and **p**eople.

In the policy area, USAID established one important principle with the 1996 launch of the Leland Initiative. We would only work with those countries willing to adopt modern, Internet-friendly communication policies based on low prices, the introduction of competition, and the free flow of information. Leland experts offered to help African telecommunications leaders reach out to the private sector to implement these policies.

"Pipes" mean the hardware, the communication technologies that link people to ISPs, ISPs to the national gateways, and these, in turn, to the worldwide Internet backbone. The Leland Initiative experts installed state-of-the-art telecommunications equipment to national capitals and trained phone company staff in its use. Leland experts also provided technology to link private Internet services businesses to this equipment and devised models for getting connections out to underserved areas and the secondary cities.

Helping people build the skills and knowledge base of an information industry was the third objective of the Leland Initiative. We intended to help individuals and institutions apply the powerful information and communication tools of the Internet to achieve social and economic development and improve the lives of African citizens.

Ten nations joined the Leland Initiative on these terms in 1996. In partnership with the U.S.-based telecommunications corporation AT&T, USAID showed government regulators in these first-round countries how to set affordable wholesale prices for Internet circuits that would still yield a healthy rate of return on the investments that their governments had made for the circuits. AT&T's involvement helped national phone company officials—accustomed to monopolistic telecommunications policies—view the private sector as a partner, rather than as an opponent to be controlled. In each country, Leland arranged meetings among the stakeholders—government officials, telephone company officers, private entrepreneurs, university and school leaders, NGOs and the like. Through these meetings, Leland helped the parties hammer out transparent—and minimal—licensing procedures. In each Leland country, multiple companies responded to these opportunities to enter the Internet business, ready to invest an average of $40,000 each to participate.

When the policies were in place, USAID turned to the U.S. technology sector, using firms in Utah, California, Virginia, Maryland, and elsewhere to design modern satellite-based Internet gateways to bring efficient high speed Internet into the national phone companies. We introduced both wired and wireless technologies to link these gateways to the new ISPs and to give them telephone lines over which customers could access the Internet. New wireless technologies continue to be provided to underserved neighborhoods and people; cybercafes and neighborhood access centers are now a major growth point for the Internet.

The initial 10 countries that signed on to the terms of the Leland Initiative made rapid progress in their telecommunications sectors, progress that was noted by neighboring governments. Countries that had spurned participation upon the initial offering in 1996 saw that their policies of high prices and state and private monopolies were not achieving the results obtained by nations that had adopted Internet-friendly policies. In the late 1990s, these initial holdouts began to sign agreements to pursue policy reform, to lower prices, and to allow marketplace competition.

Increasing Skills

Proper hardware and sufficient access are only of value when people know how to use information technologies to improve their lives and their communities. Recognizing this, USAID embarked on a major effort to increase the capacity of African people and institutions to use information resources in education, business, agriculture, and democracy building.

The Leland Initiative has trained thousands of individuals in strategic use of the vast international information resources that the Internet provides. These people represent every sector of society—government, business, nongovernment organizations (NGOs), education, and health care. They apply these skills today to invigorate economic activity, increase human potential, spur development, and create more civic participation and greater transparency in government.

The Internet-based development activities that are products of the Leland Initiative are varied:

- . Partnerships between African and U.S. schools strengthen in-country capacity to use the Internet in the educational process, and foster on-going relationships.

- . Education officials are uniting disparate universities in Kenya, Uganda, Rwanda, South Africa, Mali, and Guinea into national networks, the fundamental building block of the rapidly globalizing educational world.

- . Private sector trade and investment activities are strengthening the ability of business associations to use the Internet.

- . Internet-based networks of democracy stakeholders from the executive, legislative and judicial branches are increasing transparency, promoting democracy and building better governments.

The business sector provides some of the most tangible evidence of the progress made in these areas. We provided equipment and training to help small-business owners develop their skills and identify strategic information resources. Within six months, all the companies involved in the project had increased their revenue by 60 percent. Many of the enterprises were able to find better sources for raw materials and equipment through the Internet, thus reducing their operating expenses and increasing their competitiveness.

Another success story was in the formation of a women's business network. With membership from Ghana, Kenya, Uganda, South Africa, and the United States, the Women's Business Network promotes use of the Internet in developing trade relationships, expanding access to critical market information, and establishing e-business linkages between African and U.S. companies. More than 140 African businesswomen created their own, self-reliant U.S.-Africa Women's Business Alliance. Forty businesswomen have set up Web sites to better market their products and services, or have begun advertising their goods over existing sites.

In KwaZulu Natal Province in South Africa, Leland Initiative experts helped the Black Farmers Union set up Internet information centers. Internet access at these centers allows more than 1,200 farmers to use banking services online, and thus avoid a 128-kilometer roundtrip to the closest urban area served by financial institutions. They also have real-time access to information on the price and availability of key agriculture inputs such as fertilizer and seed, rather than conducting transactions through costly and inefficient middlemen.

The Future

The results and the lessons derived from USAID's seven-year experience with the Leland Initiative have become the basis for the information technology component of the Global Development Alliance, the U.S. Government's business model for sustainable development through partnerships among governments, nongovernmental organizations, businesses, and educational institutions. Public-private efforts are underway to achieve a variety of goals that will strengthen the role of ICTs in Africa. USAID has engaged partners from government, education, and the private sector to develop improved education and training programs to produce an African cadre of skilled ICT professionals and experienced regulators. U.S. universities, corporations, and NGOs are providing expertise, software, and equipment to strengthen poorly resourced African universities.

These partnerships work toward helping Africans meet one of the key challenges of the 21st century –stimulating economic and social development. Distance learning, telemedicine, e-commerce, and e-government all hold great promise for African and American interests alike. The Leland Initiative has already introduced millions of Africans to the advantages that information technologies can provide in enhancing the quality of life and building better societies. It is our challenge now to continue this work and expand our efforts to the millions more who still have not entered the digital age.

A number of institutional Web sites supported by the Leland Initiative demonstrate its achievements. They are available at: www.nettelafrica.org, www.kenet.org, www.ncc.gov.ng, www.makerere.ac.ug

[1] International Telecommunications Union Statistics at a Glance, October 2003. http://www.itu.int/ITU-D/ict/statistics/at_glance/Internet02.pdf

[2] Cote d'Ivoire, Benin, Eritrea, Guinea, Guinea-Bissau, Madagascar, Mali, Malawi, Mozambique, Rwanda.

[3] Chad, Democratic Republic of the Congo, Ethiopia, Ghana, Namibia, Niger, Nigeria, Lesotho, Liberia, Senegal, South Africa, Swaziland, Tanzania, Uganda, Zambia, Zimbabwe

Connecting with Eurasia

By Barry Ballow
Director, Office of Academic Exchange Programs
Bureau of Educational and Cultural Affairs
U.S. Department of State

The U.S. government is promoting Internet skills and computer knowledge among diverse populations in Eurasia.

For decades the U.S. State Department has been sponsoring educational and cultural exchange programs for citizens around the world to promote mutual understanding. The department has always tried in one way or another to maintain links with alumni of these programs. For alumni in Eurasia, that effort moved into cyberspace in a formal and comprehensive way in 1995 with establishment of a network of public access Internet sites throughout the region.

The program that established the network offers, in addition to mere Internet access, Web site design, training, and distance learning, and it encourages Internet-based activities between alumni, the general public, and counterparts in the United States. The program has built a network of professionals in the 12 countries of Eurasia who communicate daily, sharing lesson plans, engaging in community service projects, and connecting citizens of those countries with U.S.-based resources and counterparts.

Background and History

The State Department's Bureau of Educational and Cultural Affairs *(http://exchanges.state.gov)* created the program in 1995, calling it the Internet Access and Training Program (IATP). Two organizations share management responsibilities for the program—Project Harmony in Russia *(http://www.projectharmony.org)* and the International Research and Exchanges Board (IREX) in Belarus, Moldova, and Ukraine, and in the Caucasus and Central Asian countries *(http://www.irex.org).*

The main goals of the IATP are to expand knowledge and use of the Internet in order to foster the free flow of information and ideas across national borders; to provide Internet access to exchange-program alumni as well as targeted members of the general public; and to provide training in using the Internet and accessing the resources on the World Wide Web.

So far, the Bureau of Educational and Cultural Affairs has spent nearly $30 million on IATP in Eurasia, and the results have been profound. IATP has counted more than 2,500,000 users, supported development of more than 6,000 Web sites, and provided training for more than 210,000 individuals. In addition, IATP has 79 open access centers in 54 regions of Russia, and a total of 140 sites in Belarus, Moldova, Ukraine, and the Caucus and Central Asian countries.

The Russian Experience

Under Project Harmony's guidance, the IATP program in Russia has focused on enabling local citizens to participate in the global Internet community. Emphasis has been placed on fostering civic leadership, harnessing Internet technology, and facilitating cross-cultural learning.

IATP has 79 centers across the country, of which 41 are based at regional libraries, 22 at universities, and 16 at other facilities. Each host institution provides an educational coordinator and a technical specialist. All partners provide fully remodeled office space and furniture, and they cover monthly Internet connection, staff salary, utilities, and security costs. A key goal for the centers is to be self-sustaining once U.S. government support ends.

Center staff recruit exchange program alumni to participate in Web design courses and thematic training, and they encourage them to teach classes for the general public. All centers are open for a minimum of 20 hours a week for alumni and general public Internet access, and they offer an additional 20 hours of training for such diverse groups as non-government organization (NGO) workers, women's organizations, individuals with disabilities, and orphans. Four centers are dedicated to exchange-program alumni and persons with disabilities. Many program participants engage in community service work and many also have acquired sufficient Web design skills necessary to gain fruitful employment.

The U.S. Embassy in Moscow cooperates closely with Project Harmony to administer the American Corners program in Russia. American Corners, launched more than three years ago at the initiative of former U.S. Ambassador to Russia James Collins, is a scaled down, high-tech version of American cultural and educational centers in other parts of the world. A large portion of their collections are on CD-ROM.

The embassy has even taken this concept a step further, creating a U.S. Virtual Consulates Program. Virtual consulates, offering visa information and forms via an embassy-produced Web site, are available at IATP centers in several regions of Russia.

This year, IATP added several new elements. One, done in partnership with the World Bank Institute, is the Virtual Learning Environment (VLE), which gives alumni access to more than 25 distance learning courses. The VLE, available to all IATP centers free of charge, provides courses on a range of topics, among them public speaking, NGO management, resume writing, leadership, managing a board of directors, geometry, and database development. Each online course is limited to 25 students and is always facilitated by a professional instructor. During each course, an assistant is selected to study the notes and techniques of the instructor so that he or she can lead the course in the future.

IATP conducts outreach to the smaller republics of Russia. For instance, a project conducted in the Republic of Mari El led to creation of an extensive educational network there as well as a team of information technology specialists. Alumni of the Teachers for Excellence in Education (TEA) and Partners in Education (PiE) exchange programs are implementing a similar effort in the Republic of Kalmykia, for which the republic's ministry of education is providing substantial financial support. Similar projects have been implemented in the Samara and Irkutsk regions.

IATP offers all alumni 50 megabytes of computer server space to develop their own Web sites and e-mail services. Not surprisingly, the State Department relies principally on e-mail to keep in touch with alumni and inform them of U.S. government assistance programs.

IATP in the other Eurasian Countries

IREX administers more than 140 IATP centers across Belarus, Moldova, and Ukraine as well as the countries of the Caucasus and Central Asia in close cooperation with U.S. embassies there.

IATP provides computer workstations, a server, a printer, a scanner, related cabling, and power backup systems for each center. IATP also provides a site administrator who often works with partner institution personnel to administer the site. The partners commonly cover costs for the center's room, renovations, utilities, and security. In some cases, partner institutions contribute computer equipment.

The centers offer the Step-by-Step Training Program to members of targeted organizations such as community groups, educational institutions, libraries, and NGOs after identifying their needs. Through this program, schools have acquired computer hardware and begun doing their own training, and newspaper associations have worked with IATP to create e-mail networks to share news stories and photographs.

In Tajikistan, the Step-by-Step Training Program has already resulted in the first Web site dedicated to combating tuberculosis. The Web site is currently filling up with information about the specifics of the disease and its reach in Tajikistan, and it serves as a forum for Tajik doctors dealing with the illness.

In Spitak, Armenia IATP is using the Step-by-Step Program with children, teaching them to use the Windows and Linux operating systems to create personal Web sites. The children of Spitak now maintain an online newspaper and a Web radio station, participate in Web-design groups, and create their own animations. Some of these children even assist IATP trainers throughout the region. Spitak can now boast a cadre of young people with highly marketable and practical technology skills.

The IATP Mobile Training Program is closely aligned with the Step-by-Step Training Program. As the name implies, the Mobile Program takes training on the road to organizations that have their own computers, providing users with training targeted to their organization's particular needs, such as the creation of a mailing list.

IATP is the largest Internet development program in the region, and all of its sites have a standard look and feel. Key to this standardization is early training for IATP center staff, both in computer and Internet basics as well as in specialized areas such as library science.

In many cities, councils of exchange-program alumni work with community groups to identify training needs, advertise the services of IATP sites, and raise awareness through special workshops on such subjects as trafficking in persons, HIV/AIDS, and culture and life in the United States. Alumni can often contribute specialized knowledge about specific academic or professional fields they studied in the United States. For example, members of an alumni council in Ferghana, Uzbekistan recently taught computer skills to more than 60 professionals who work in the fields of natural sciences and community organizing.

In eight short years, IATP has established a dynamic and growing network of computer and Internet users in Eurasia, linking them with each other and with their counterparts in the United States and around the world. Jobs have been created, knowledge acquired, associations established, and mutual understanding promoted—all testimony to the power and effect of cooperative engagement in an environment of open and free communications.

A New Way of Governing in the Digital Age

By Charlene Porter
Managing Editor of *The Evolving Internet*

Information technologies and Internet transactions are changing the relationship between governments and their citizens.

The Internet delivery of government information and services, e-government, has been a fact of online life since 1996. In the fast-moving pace of digital technology, several evolutionary cycles in e-government have developed in that time. Now e-government is on the brink of a new era when it could work to transform government's service delivery and interaction with citizens, according to a number of surveys and experts. In so doing, e-government could also change the traditional structures of government and citizens' perceptions of them.

In the United States, the federal government, as the largest single government entity, is at the forefront of this transition. The federal portal FirstGov.gov offers an entry point to the full range of government services, programs, and agencies, and it does so in a user-friendly manner that has been widely praised by independent evaluating organizations and information technology specialists.

State, city, and county governments have also moved rapidly over the past several years to establish an Internet presence. All 50 U.S. states have established an online presence. The International City/County Management Association (ICMA), a professional organization comprising local government managers and administrators, conducted a survey in 2002 of local governments with populations in excess of 2,500, finding that 75 percent have put a Web site online.

The quality and quantity of the information and services provided online by all these different government entities range across a wide spectrum, the result of thousands of individual decisions made in city halls, council chambers, and state houses across the country. Recognition of that divergent quality and usability brings on the next stage in e-gov's evolution—the challenge to identify the best practices of online service delivery and the best methods to use advanced information technologies to deliver the greatest payoff for governments and the citizens they serve.

If governments can rise to that challenge, they stand to transform the belief held by publics of practically all cultures and political systems—that government is inefficient, slow, and unresponsive. "The evolution of electronic government represents a bold new way of doing the state's business to provide a government that serves its citizens and businesses productively and more efficiently," according to a study conducted by the National Governor's Association (NGA).

The Council for Excellence in Government is an independent Washington-based organization closely monitoring the pace and progress of government online. Council Vice President for E-government David McClure said in an interview with *Global Issues* that online service delivery has already begun to highlight what's been wrong with the old methods. "The inefficiencies of the existing processes are already starting to show themselves. The Internet erases a lot of that inefficiency," McClure said.

The Council for Excellence in Government and private sector underwriter Accenture released a poll assessing perceptions of e-government by citizens in April 2003. E-government services received high marks, according to the more than 1,000 citizens surveyed by Hart-Teeter Research. More than 60 percent who were Internet users expressed interest in conducting basic transactions with government online—services such as filing a change of address, renewing a driver's license, or obtaining a birth certificate or marriage license.

Of those online users who had already accessed such services, 67 percent said that dealing with the government was easier and more convenient because of the online service, and 74 percent said that the benefits of e-government will likely grow in the years to come and improve government operations overall.

"They don't have to go stand in line to get a driver's license renewal," McClure said. "They don't have to write a letter; they can interact with the government via e-mail....It's convenient."

Evolving Internet Facts

- Half of all Americans and three-quarters of American Internet users already have used a government Web site to find information or conduct transactions.

- When asked to name the most important potential benefit of e-government, 28 percent of Americans cite greater government accountability to its citizens, 19 percent say greater efficiency and cost-effectiveness, 18 percent say more access to public information, and 13 percent say more convenient government services.

Source: Hart Teeter/Council for Excellence in Government

The Evolutionary Stages

McClure's study of the movement of governments online since the late 1990s has allowed him to identify several stages in the process. Governments large and small, local and national, go through much the same developmental process, he said, in the United States and in other nations. The first stage is bringing a Web site online and establishing a presence, which usually offers little more than basic information. Next a government will develop an interaction with citizens and create a channel for an online exchange of information. Then the agency will advance to the transaction phase—allowing users to reserve a campsite at a public park, renew a driver's license, pay a business license fee, etc.

The phase now beginning in many governments, McClure said, is transformation, “figuring out how can you make the best use of this dynamic interaction you now have with people—citizens and businesses—so that you can redesign everything in your process behind it to make it much more efficient.”

One of the progressive trends in governments' online services is to provide information in a thematic fashion, rather than in a bureaucratic fashion dictated by the structure of the government agencies that are the custodians of that information. On the federal level, for instance, a wide array of agencies maintain public lands that offer recreational activities. Now, online users can explore all those opportunities at Recreation.gov without having to know which government agency has jurisdiction over what.

The state of Massachusetts has established a thematic online clearinghouse for businesses attempting to start an enterprise in the state. MassMeansBusiness.com is an Internet portal that consolidates information from state agencies, municipalities, and private sector firms who are all hoping to encourage new business and improve economic development in Massachusetts. The portal consolidates information resources for a potential business investor in a way never previously achieved.

Projects such as these represent the new trends, but not the entire reality. General characterizations about the state of e-government are impossible to make because of the uniquely localized ways it is developing. Teams of technocrats, bureaucrats, and elected officials in governmental entities everywhere are working to combine their ideas, resources, and priorities in the design and maintenance of online government services. Their independent actions form a mosaic from which a full picture is yet to emerge.

Citizens themselves are getting more opportunities to contribute to the design of their online services. McClure says municipalities in increasing numbers are surveying citizens about the types of services they want to see online. When cities take that step, McClure said their online products get higher approval ratings from citizens. “[The cities] rate higher, they're delivering focused services. They're not trying to do everything. It makes a huge difference,” McClure said.

There's another bonus that emerges from this approach, according to the Council for Excellence in Government survey. People who reported successful online interactions with government like government more. “Their trust in government, their acceptance of government goes up tremendously,” McClure said.

The Obstacles

Ensuring privacy and security in transactions between government and online citizens is a high priority for both the people who use the services and for the people who provide them. A survey of government information technology specialists found that 80 percent of respondents identified the protection of confidential and sensitive information as a critical priority for their agency. The study, conducted by Lightspeed Systems—an information technologies (IT) company—also found that a majority of these technology specialists reported they do not have solutions to these problems.

“When gone unrecognized, IT issues such as privacy protection, system intrusion, offensive e-mail, and spam considerably drain IT resources at government agencies, costing these institutions a tremendous amount of time and money,” Lightspeed President Rob McCarthy told *Government Technology* magazine in October. “And the survey indicates not many agencies have solutions in place.”

Despite the positive reviews of e-government services that emerged from the Council for Excellence in Government survey, 46 percent of participants expressed strong concerns that their online interaction with government could compromise their privacy, or the security of personal information.

McClure said the findings reflect the high standards that the public holds for government's obligation to protect the privacy of citizens. “All it takes is one incident, and trust in government would slide 20 (percentage) points and everything would be pulled offline.”

The expectation of privacy varies from one nation to the next, however, and some nations—notably Canada, the United Kingdom, and Singapore—have moved ahead of the United States in the types of online transactions they offer involving the collection of private information. The Council for Excellence in Government survey finds that citizens in other countries have fewer concerns about privacy than Americans do and are more accepting of government compilation of personal information that could occur through online transactions.

Ensuring that all citizens receive an equal level of service from government is a concern about e-government identified in a report prepared by a task force organized by the ICMA. Even while governments move online, they are still providing services in person, on the telephone, and through traditional mail. The ICMA report finds that governments will be challenged to provide an equal level of service through all those channels.

“Simply because someone e-mails rather than mails a complex request does not mean, in practice, the issue should be rectified any faster,” said the task force report.

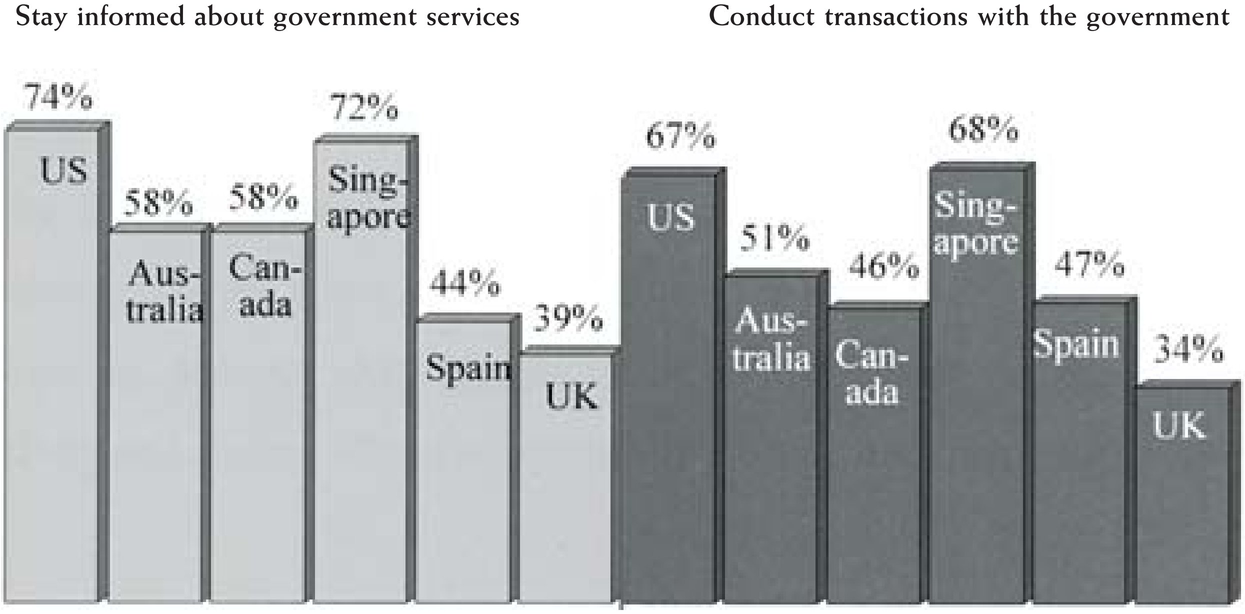
Access and equity of service delivery are noted as problems in a study conducted by the Taubman Center for Public Policy at Brown University and released in September 2003. A review of government Web sites maintained by the 70 largest U.S. cities concluded that only 20 percent of them comply with an international Web standard for disability access, and only 13 percent comply with a standard outlined in U.S. law.

“Government Web sites need to do much more to make themselves accessible to all Americans,” said Taubman Director Darrell M. West in a press release announcing the September findings. “Web sites maintained by city agencies are flunking basic disability access standards for the visually and hearing-impaired.”

There’s also a language barrier online, Taubman found. Only 13 percent of the city government sites surveyed offered any form of foreign language translation. A second Taubman study surveying state and federal government sites found a higher level of online multilinguality. Sharing a border with Mexico and home to a significant Hispanic population, the state of Texas was

International E-gov Users Agree Information And Transactions Easier

E-gov makes it easier and more convenient to:



Source: Hart Teeter/Council for Excellence in Government named by Taubman as the national leader in this area with 55 percent of its Web pages offered in a second language *(http://www.texas.gov/home.jsp?language=esp)*

The federal government took an important step toward overcoming the online language barrier in October with introduction of a Spanish language version of FirstGov.gov. WWW.espanol.gov will serve 28 million Spanish speakers in the United States, according to the General Services Administration (GSA), the agency that oversees federal online offerings.

“President Bush, through his e-gov initiative, challenged the government to employ the latest in technology to create a more efficient, citizen-centered, federal government," said GSA Administrator Stephen A. Perry, announcing the launch of the Spanish site. "FirstGov en Español is yet another example of making it easier for the public to interact with federal government agencies," he said.

The Future

Governments large and small increase their online presence day-by-day, even as they struggle to determine what services citizens want, how they might be provided, and how they might be funded. Even amidst this swirl of immediate activity, a picture of what the future might look like is taking shape in the vision of some analysts.

The ICMA task force found “(E-)government services help to ‘democratize’ local government in a positive way. Web site resources boost transparency, increase access to policymaking, and increase accountability from government leaders.”

That positive outlook must be balanced against another possible outcome, according to the ICMA report. “(T)he rate at which information is received can also pose a hazard if it abbreviates the democratic thought process.”

The prospect of increased transparency in government is one foreseen by many of the Internet futurists who watch the trends in e-government. A study released jointly in May 2003 by the Federation of Government Information Processing Councils and the GSA finds, “The use of e-gov can be an important tool of democratic governance, facilitating the transparent, two-way open communication that makes government-of-the-people possible.”

Government jurisdictions throughout the United States and around the world are at many different points along the evolutionary e-government timeline. But authorities watching the trends seem to agree that advanced information technologies and their users have the momentum to compel more openness and transparency from governments large and small.

Charlene Porter is the managing editor of this journal and writes on communications issues for the Office of International Information Programs, U.S. Department of State.

This article is based on a survey of current opinions, and does not necessarily reflect U.S. government policy.

Staying Safe in Cyberspace

By Lawrence R. Rogers
Senior Member of the Technical Staff
Software Engineering Institute, Carnegie Mellon University

A computer security specialist offers instruction and guidance on how to prevent intruders and infected software from getting into your home computer system.

The Internet is a great communications and research tool as well as a source of entertainment for millions of people around the world. It is also a security risk. Malicious computer programs have been used to attack computer systems hooked up to the worldwide Internet, damaging computer programs and gaining access to confidential information. News reports of these attacks have brought to the world new meanings for old words such as "virus," "worm," "infection," and "crash"—part of a frightening vocabulary that can intimidate those just beginning to use this new technology. What does it all mean and how can those less experienced Internet travelers navigate the hazards more safely?

Computer security has its similarities to the precautions most people take to secure their home, family, property, and person in an uncertain and sometimes dangerous world. Locking the doors at night, avoiding dangerous neighborhoods, and keeping an eye on one's wallet have their corollaries in sensible computer use.

The Threats

Your home computer is a popular target for intruders, because they want what you may have stored there: credit card numbers, bank account information, personal background information, and anything else they can find. With such information, intruders can take your money, even steal your identity. But it is not just money-related information they may be after. Intruders also want your computer's resources, meaning your hard disk space, your fast processor, and your Internet connection. They use these resources to attack other computers on the Internet. In fact, the more computers an intruder uses, the harder it is for law enforcement investigators to figure out where the attack is coming from. If intruders can't be found, they can't be stopped, and they can't be prosecuted.

Intruders go after home computers because typically they are easy targets. When connected to high-speed Internet connections that are always turned on, these computers are all the more easy for intruders to find and attack.

How do intruders break into your computer? In some cases, they send you e-mail with a virus. Reading that e-mail activates the virus, creating an opening that lets intruders see what is inside your computer. In other cases, they take advantage of a flaw or weakness in one of your computer's programs—a vulnerability—to gain access. Once inside, they often install new programs that let them continue to use your computer—even after you have plugged the holes they used to get into your computer in the first place. These so-called backdoors are usually cleverly disguised to blend in with the other programs running on your computer.

So, think of your computer as you would your house or your apartment. For example, you know that if you have a loud conversation, someone next door can probably hear you. You probably routinely lock the doors and close the windows when you leave, and you don't give the keys to just anyone. If a stranger shows up at the door, you don't invite him inside until you have made some discriminating judgments about his intentions. If you're approached by a salesperson, you don't start handing him money until you've decided whether he's legitimate and his product or service is reliable and desirable. These are the same kinds of judgments that you must make when browsing the World Wide Web on the Internet and deciding whether the information you encounter and the messages you receive are helpful or harmful.

E-mail Security

Electronic mail—e-mail for short—is one of the biggest threats to your home computer. By understanding how e-mail works, and by taking precautions in how you go about reading and writing messages, you can reduce this security threat.

When you exchange e-mail with someone, the messages sent between you and that person pass through several computers before they reach their destinations. Think of this conversation as taking place in an Internet "room," a very, very big room. Anyone, or, more accurately, any program, along the conversation path can probably understand what is being said, because most Internet conversations are not concealed or hidden in any way. Consequently, others may be listening in, capturing what you send, and using it for their own benefit.

E-mail-borne viruses and worms often arrive in attractive, enticing packages, much like the printed advertisements we receive via traditional mail designed to sell us something. By all appearances, an infected e-mail message appears to be something we want to read from someone we know, not a malicious virus or worm poised to destroy our data, exploit our hard drive, and hijack our computer's processing power.

There are steps you can take to help you decide what to do with every e-mail message with an attachment that you receive. You should only read a message that passes all of these tests:

1. The Know test: Is the e-mail from someone that you know?

2. The Received test: Have you received e-mail from this sender before?

3. The Expect test: Were you expecting e-mail with an attachment from this sender?

4. The Sense test: Do the subject line describing the contents of the e-mail message and the name of the attachment both make sense? For example, would you expect the sender—let's say your mother—to send you an e-mail message with the curious, possibly mystifying subject line "Here you have, ;o)" that contains a message with an attachment—let's say “AnnaKournikova.jpg.vbs?” A message like that probably wouldn't make sense. You know your mother doesn't follow world tennis, and probably doesn't know who Kournikova is. In fact, it could be an instance of the so-called Anna Kournikova worm that began infecting computers around the world with malicious code in February 2001, and

reading it would damage your system.

5. The Virus test: Is this e-mail infected? To determine this, you need to install and run an anti-virus program.

Preventing Viruses

It's helpful to think about viruses in the same way that you think about that stranger who has come knocking at the door. It is your responsibility to profile or evaluate anyone who enters your living space. Anti-virus programs do much the same thing. These programs look at the contents of each file, searching for specific patterns that match a profile—called a virus signature—of something known to be harmful. For each file that matches a signature, the anti-virus program typically provides several options on how to respond, such as removing the offending patterns or destroying the file.

Viruses can reach your computer in many ways—through floppy disks, CD-ROMs, e-mail, Web sites, and downloaded files. All need to be checked for viruses each time you use them. In other words, when you insert a floppy disk into the drive, check it for viruses. When you receive e-mail, check it for viruses using the tests described above. When you download a file from the Internet, check it for viruses before using it. Your anti-virus program may let you specify all of these as sources to check each time you encounter or use them. Your anti-virus program may also do this automatically.

You often have the chance to react to viruses when they've been discovered on your home computer. Depending upon the specific characteristics of the virus, you might be able to clean the infected file. Or you might be forced to destroy the file and load a new copy from your backups or original distribution media. Your options depend upon your choice of anti-virus program and the virus that's been detected.

Patching

Sometimes a would-be intruder may attempt to enter your home through a broken window. Software programs that you run on your computer can also have "broken windows," and cyberspace intruders are constantly searching to exploit such openings.

A Brief Glossary

Excerpted from the Webopedia Dictionary Online for Computer and Internet Terms

Download: To copy data (usually an entire file) from a main source to a peripheral device. The term is often used to describe the process of copying a file from an online service or bulletin board service to one's own computer.

Intruder: An adversary who is conducting or has conducted an intrusion or attack against a victim host, site, network, or organization.

Trojan Horse: A destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer.

Virus: A program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves.

Vulnerability: A feature or combination of features of a system that allows an adversary—the intruder—to place the system—your home computer—in a state that is both contrary to the desires of the people responsible for the system—you—and increases the risk of undesirable behavior in or of the system.

Worm: A program or algorithm that replicates itself over a computer network and usually performs malicious actions, such as using up the computer's resources and possibly shutting the system down.

A comprehensive glossary of Internet terms is available at http://www.webopedia.com/

Just as you would repair the broken window to secure your home, you must fix the vulnerabilities in programs running on your computer. Most vendors provide patches, sometimes free of charge on their Web sites, for this purpose. When you purchase programs, it's a good idea to see if and how the vendor supplies patches. Just as appliance vendors often sell extended warranties for their products, some software vendors may also sell support for theirs. Vendors send notices to product owners when a safety-related problem has been discovered. Registering your purchase through the warranty card or online gives the vendor the information they need to contact you if there is a recall or a software fix.

Program vendors also provide a service allowing you to receive patch notices via e-mail. Through this type of service, you can learn about problems with your computer before intruders have the chance to exploit them. Consult the vendor's Web site to see how to get e-mail notices about patches. Some programs include features that automatically contact the vendor's Web sites to look for patches. These automatic updates tell you when patches are available, and they download and even install them.

While the patching process is getting easier, even to the point of automation, it is not yet foolproof. In some cases, installing a patch can cause another seemingly unrelated program to break. The challenge is to do as much homework as you can to learn what a patch is supposed to do and what problems it might cause once you've installed it.

Evolving Internet Facts

CERT/CC defines a security incident as the act of violating an explicit or implied security policy related to the laws, rules, and practices for managing and protecting computer systems.

Number of security incidents reported:

1988:	6
1992:	773
1996:	2,573
2000:	21,756
2003:	114,855 (January-September only)

Source: CERT/CC Statistics 1988-2003

Conclusion

Today's Internet evolved from a 1960s project that was designed to allow scientists and researchers to share ideas and resources via computer technology. The element of trust was key to the endeavor, shaping many of the practices, procedures, and technologies that are still in place today. As the Internet has become a global forum for communications and commerce, relying principally on trust has proven to be inadequate. Today's users must treat the Internet with the same wariness and caution they would carry into any unknown environment. While the Internet superhighway still has many potholes, sharp bends, and occasional accidents, today's users can safely journey through those hazards when they apply the types of cautions they already know and use in everyday life.

The Software Engineering Institute is a federally funded research and development center and the home of the CERT® Coordination Center, a center of Internet security expertise. A more detailed explanation of all the issues discussed here is available at http://www.cert.org/homeusers/

A CERT representative describes the global damage done by viruses this year in the Additional Resources Section of this publication.

The opinions expressed in this article are those of the author and do not necessarily reflect the views or policies of the U.S. government.

Bridging the Digital Divide

By Teresa Peters
Executive Director
Bridges.org

Installing computers and connections in underdeveloped communities is only part of what is needed to put information and communications technology to use for socio-ecoomic development. An understanding of grassroots realities, pooling of resources, and a favorable regulatory system are among the many elements necessary in an effective approach to the digital divide.

Information and communications technology (ICT) is a key weapon in the war against world poverty. When used effectively, it offers huge potential to empower people in developing countries and disadvantaged communities to overcome development obstacles, address the most important social problems they face, and strengthen communities, democratic institutions, a free press, and local economies. Yet a digital divide separates those who can access and use ICT to gain these benefits, and those who do not have access to technology or cannot use it for one reason or another. There are a wide range of projects underway aimed at bringing ICT to people in developing countries. But in order for ICT to have a *real impact* on people's lives, it is crucial that development efforts go beyond computers and connections to ensure that people have *real access* to ICT so they can use it effectively to improve their lives.

The digital divide between countries is usually measured in terms of the number of telephones, computers, and Internet users. Between groups of people within countries, it is usually measured in terms of race, gender, age, disability, location, and income. It is difficult to gain an overall understanding of the digital divide, the proposed solutions, and what is having a real impact, when there are multiple definitions of the problem, conflicting views on whether it is getting better or worse, and various opinions on the key factors affecting it.

Bridges.org. is an international non-profit organization based in Cape Town, South Africa. The organization promotes policies and laws that foster widespread ICT use, and works at the grassroots level to help people understand ICT and its practical utility. Bridges.org has seen that the digital divide is growing around the world, despite the fact that all countries and all groups within countries, even the poorest, are increasing their access to and use of ICT. This is because people in ICT "have" countries and groups are increasing their access and use at an exponential rate. At the same time, ICT "have-nots" are increasingly excluded from jobs, participation in government processes, and public discourse on the issues that affect their lives, leaving them politically and economically powerless. Countries and communities face the threat of being left further behind if they do not address the growing digital divides. However, the infusion of ICT can intensify existing disparities. ICT alone is not enough to solve long-standing imbalances and can make inequalities worse if not applied wisely.

The digital divide is a complex problem, presenting both practical and policy challenges. It is also apparent that solutions that work in developed countries cannot simply be transplanted to developing country environments: solutions must be based on an understanding of local needs and conditions.

What is being done?

Governments, businesses, individuals, and organizations have studied the issues at stake in the digital divide and drafted a range of valuable reports—from statistical analyses to in-depth case studies. Most offer recommendations for tackling the problems, usually suggesting specific ground level initiatives and policy reforms. Many also cover the wider issues that impact on digital divides, such as e-commerce, information society, and international trade. Major international initiatives, such as the G-8's Digital Opportunity Task Force (DOT Force) and the World Summit on Information Society (WSIS), bring together leaders and decision-makers from around the world for a consultation process to determine the key factors and how to address them. Several organizations have undertaken "e-readiness" assessments to determine a country's readiness to integrate technology and e-commerce and establish a benchmark for regional comparison and public and private sector planning. Unfortunately, there is significant duplication of effort in these studies and recommendations, and too few of the suggestions are followed up in practice. There is a lot of talk, but not enough action.

Numerous on-the-ground initiatives are working to provide technology access and help put technology to use in underserved populations. There are an enormous number of efforts, ranging from projects that create public centers where poor people can use telephones and computers, to those that incorporate ICT in healthcare, to programs using innovative technology in small business applications. These efforts are driven by organizations that range from the smallest NGO working in remote areas—such as SchoolNet, Namibia's efforts to put computers in rural schools—to the largest multinational corporations, such as Hewlett Packard's $1 billion "E-Inclusion" initiative to promote hardware innovations suitable for developing country environments. Many initiatives address specific aspects of the range of issues, but too often they neglect related factors that limit their success. For example, too many community access projects providing computers and connections in rural locations do not become self-sustaining because local people do not use their services—often they have failed to address the role of the center in the local economy or the need for locally relevant content. There is a need for a holistic approach to cover the range of issues to create effective and sustainable uses for technology that are integrated into local society.

What more is needed? Real Access

Providing access to technology is critical, but it must be about more than just physical access. Computers and connections are insufficient if the technology is not used effectively because it is not affordable; people do not understand how to put it to use; people are discouraged from using it; or the local economy cannot sustain its use. ICT projects will only be widely successful in developing countries when all of the other components necessary for the effective integration of ICT into society are in place. Bridges.org calls this *real access* to ICT, and its work looks at twelve interrelated factors that determine whether ICT can be effectively used by people:

- **Physical access**: Is technology available and accessible to people and organizations?

> "The issues at stake in international and domestic digital divides are huge, and organizations should cooperate to tackle problems collaboratively."
>
> Teresa Peters

- **Appropriate technology**: Is the available technology appropriate to local needs and conditions? What is the appropriate technology according to how people need and want to put technology to use?

- **Affordability**: Is technology affordable for people to use?

- **Capacity**: Do people have the training and skills necessary for effective technology use? Do they understand how to use technology and its potential uses?

- **Relevant content**: Is locally relevant content available, especially in terms of language?

- **Integration**: Is technology use a burden to peoples' lives, or is it integrated into daily routines?

- **Socio-cultural factors**: Are people limited in their use of technology based on gender, race, or other socio-cultural factors?

- **Trust**: Do people have confidence in technology and understand the implications of the technology they use, for instance in terms of privacy, security, or cybercrime?

- **Legal and regulatory framework**: Do laws and regulations limit technology use? Are changes needed to create an environment that fosters its use?

- **Local economic environment**: Is there a local economic environment favorable to technology use? Is technology part of local economic development? What is needed to make it a part?

- **Macro-economic environment**: Is technology use limited by the macro-economic environment in the country or region, for example, in terms of deregulation, investment, and labor issues?

- **Political will**: Is there political will in government to do what is needed to enable the integration of technology throughout society, and public support for government decision-making?

Overall, a pooling of resources and experiences is needed. Dealing with the digital divide is beyond the scope of any single initiative. While it is important for organ-izations doing community ICT projects to meet the needs of their clients as comprehensively as possible, the issues at stake in international and domestic digital divides are huge, and organizations should cooperate to tackle problems collaboratively. Private sector programs and philanthropic efforts are vital too, although there is room for improvement.

For-profit programs are successfully expanding access to technology to increasingly larger groups, but often fail to adequately address the needs of the poorest countries, and the poor citizens within countries. In isolation they can exacerbate divisions within countries since privileged groups are more able to afford and use the technology. Donations and philanthropic programs have demonstrated the useful application of technology among underserved populations, but in many cases they have failed to produce sustainable, widely replicable models. The digital divide is not a new problem. We should learn from previous experience in fields such as economic development, technology transfer, and sustainable development. Many of these ongoing programs have an impact on the digital divide, and coordination will benefit everyone.

Getting government policy right is also critical

Governments can play a fundamental role in creating an environment that will foster technology use and encourage investment in ICT infrastructure, development, and a skilled workforce. Government action is also important in spreading the benefits of technology throughout society, and governments have the power and mandate to balance the needs of their citizens for long-term economic growth and social prosperity. However, translating a vision into practical steps that fit the local context is not a simple matter. Leaders need to have a realistic appreciation for what ICT can—and cannot— do for their countries and communities, and they must lead effectively and bolster public confidence in the path they take.

A range of projects are underway in developing countries to integrate ICT in a number of critical areas, including education, healthcare, government, trade, and small business support. However, these projects frequently encounter obstacles that directly or indirectly relate to the country's policy environment. Examples include projects that rely on technology or infrastructure use that may be limited by current laws or regulations, such as laws that control or ban the use of satellite, wireless, or Voice over Internet Protocol (VoIP) technologies. There are ICT projects that may be hindered by a general law or regulation, such as fiscal or customs policies that limit cross-border trade in computing technologies. A significant problem is projects working in a particular area, such as healthcare, where current laws or regulations impede ICT use, such as privacy and data protection laws governing the handling of electronic health data.

Many national leaders have embraced ICT and are ready to promote a legal and regulatory environment that will enable its widespread use. But often at the working level, government officials do not understand the implications of existing policies that may hinder ICT use, nor the changes they need to make to create a more favorable environment. Although the development aid industry generates a tremendous volume of reports, advice, and analyses aimed at helping developing countries in the policy area, developing country governments frequently say that such recommendations do not show sufficient understanding of local needs and conditions.

Some governments have subscribed to e-strategies promulgated by outsiders, but at a practical level they lack the political will to drive change because they do not enjoy widespread public support for an ICT-focused approach. Often this is because government officials fail to engage stakeholders in framing the e-strategies, so they do not have public buy-in for their long-term plans. In some cases the government has partnered with the country's business and civil society sectors to promote ICT-enabled development at the ground level, but the various stakeholder groups lack the experience and resources to give effective input.

To cross the digital divide and put ICT to effective use to improve people's lives, countries and communities must be "e-ready" in terms of infrastructure, access, training, and a legal and regulatory framework that will foster ICT use. If the digital divide is to be narrowed, these issues must be addressed in a coherent, achievable strategy that is tailored to meet local needs.

The opinions expressed in this article are those of the author and do not necessarily reflect the views or policies of the U.S. government.

Evolving Internet Facts

Continent	Users (k)	Users per10k inhabitants	PCs per 100 inhabitants
Africa	8,941.7	111.25	1.26
Americas	207,579.8	2,441.76	28.98
Asia	211,392.8	584.75	4.43
Europe	167,883.4	2,099.69	21.14
Oceania	10,571.4	3,333.60	42.29
World	606,369.1	994.01	9.87

(K=1,000)

Source: Global Internet Access by Continent, 2002, International Telecommunications Union

Bringing the Internet to Schools Effectively

By Janet Ward Schofield
Professor of Psychology and Senior Scientist
Learning Research & Development Center
University of Pittsburgh

Installation of computers and Internet access in schools must be preceded by careful consideration of how to best use and support the technology.

Internet access is spreading rapidly in primary and secondary schools around the world. Virtually 100 percent of schools are connected to the Internet in countries such as the United States, Australia, Finland, Canada, and Great Britain. The Internet is also fast becoming widely available in schools from Scandinavia to Israel to Korea.

Almost daily, countries are making decisions with major educational and financial consequences about whether to connect schools to the Internet, what kind of connections to use, and to whom to permit access. Unfortunately, education officials do not always give sufficient thought to the adoption of Internet and other computer-based technologies in schools. Sometimes computer technology is acquired as a symbol of modernity rather than for carefully planned educational purposes. Furthermore, since the Internet is generally seen as a desirable resource, pressures mount on schools to broaden access in classrooms before plans have been formulated for its effective use there.

This article will briefly discuss four issues that should be considered in making decisions about Internet access in primary and secondary schools: its cost relative to alternatives; the need for substantial technical and pedagogical support; the alignment of school, Internet, and community norms; and the alignment of schools' goals and the Internet's educational potential. Much of this discussion is based on a five-year study of Internet use in a large urban school district in the United States. The Internet version of this article provides full footnotes and documentation at www.usinfo.gov/journals/itgic/1103/ijge/gj09.htm

In addition, the views and experiences of scholars and educators from around the world have also influenced this paper. Some of the issues mentioned, like cost, are obvious. Others are more subtle, but are nonetheless likely to have a strong impact on how Internet access influences educational processes and outcomes.

Cost relative to alternatives

Bringing the Internet to schools is not cheap. Providing Internet access for students in the United States took an initial investment of roughly $110 billion and entails continuing costs of nearly $30 billion a year. Indeed, the U.S. government has spent more than $7 billion just on subsidies for Internet connections in schools since 1997. India has announced plans to spend the equivalent of roughly $2.5 billion to bring e-learning to 600,000 schools during the next four years. Costs are especially high when schools must purchase computers with sufficient power to navigate the Internet and when all students are provided with a personal, Internet-ready laptop computer, as is done in some programs in the United States.

Internet service will also increase on-going school operating costs. For example, technical innovations often make perfectly usable computers close to obsolete with regard to Internet use in five to seven years because older computers cannot interact well with evolving network requirements and resources. Furthermore, maintenance and technical support for Internet use is also a continuing expense.

Given the substantial cost of obtaining Internet access and supporting its effective use, a question arises about whether the expenditures necessary to bring widespread Internet access to all classrooms would be more productively devoted to other things, such as additional teachers, especially in countries where labor is relatively inexpensive in contrast to the cost of computer hardware and connectivity. Also, given rapid technological change, careful consideration of anticipated technological developments and their impact on cost and capabilities is important before spending large amounts on Internet access.

Need for substantial technological and pedagogical support

Frequently, those bringing computers to schools spend too much on hardware and connectivity and too little on activities necessary for effective computer use, such as professional development and support for teachers. Countries in which large investments have been made to bring the Internet to schools have increasingly begun to recognize the importance of setting aside substantial funds for professional development and on-going technical support. Nonetheless, finding the right balance between expenditures on hardware, software, and support is a difficult problem that has not been solved. Lack of adequately developed information technology skills among teachers impedes the use of information and communication technology in many countries.

To use the Internet effectively, educators typically must increase their technical skills and their knowledge about the Internet. They also have to develop a vision of how it can contribute productively to their work. These are not simple tasks. Resources increasingly are being developed to aid educators in these regards, though their availability varies from language to language. Finally, many teachers may not have the time or the

Evolving Internet Facts

- In fall 2002, 99 percent of public schools in the United States had some basic access to the Internet, contrasted with 35 percent in 1994 when the National Center for Education Statistics first started estimating Internet access in schools.

- U.S. public schools have made consistent progress in expanding Internet access in instructional rooms (i.e., classrooms, computer, and other labs, library/media centers) from 3 percent in 1994 to 77 percent in 2000 and 92 percent in 2002.

- In 2002, the ratio of students to instructional computers with Internet access in public schools was 4.8 to 1, an improvement from the 12.1 to 1 ratio in 1998, when it was first measured.

Source: “Internet Access in U.S. Public Schools, Fall 2002,” released October 2003, National Center for Education Statistics (NCES), U.S. Department of Education.

inclination to make use of these resources, making it crucial that there be readily available professional development activities and on-going support for them.

Alignment of school, Internet, and community norms

The Internet can connect students to information and people around the world. It allows students to take courses not offered in their schools, to interact with experts unavailable in their communities, to find new audiences for their work, and to participate in collaborative projects that they could never undertake locally. For example, in one Internet project students interacted with members of a scientific expedition in Antarctica. In another, students in many communities in the United States worked collaboratively with scientists to collect and analyze data on acid rain, with students in distant schools contributing data from their own region. However, connection to the outside world may also expose students to content that is unacceptable within their communities and to individuals whose ideas or behavior may also be deemed unacceptable by teachers and parents.

Norms, values, and behaviors vary markedly from culture to culture. When Internet content is inconsistent with local mores, educators sometimes curtail Internet use in schools. Indeed, use can be so circumscribed as to undermine a substantial portion of the Internet's potential educational value. For example, in one school teachers allowed high school students to visit only pre-approved Web sites, due to fears that they might encounter inappropriate material. This practice dramatically reduced the resources these students could access and impeded development of certain kinds of Internet-related skills.

Strategies have been developed to help deal with incompatibilities between local norms and values and those accessible via the Internet. Acceptable use policies often specify the kinds of materials that students are permitted to seek out. In addition, filters can be used to try to block materials considered inappropriate, although they also inadvertently block some unobjectionable and potentially useful material. Online and other educational resources may also help students learn how to avoid danger or exploitation by individuals they may encounter on the Internet. For example, numerous organizations have developed Web sites that provide students with Internet safety tips. Two are *www.NetSmartz.org and www.CyberSmart.org.* However, such resources are more readily available in English and other world languages than in the languages of many countries now connecting schools to the Internet. Where clashes between local norms and those of the Internet are serious and widespread, and where community influence over schooling is strong, Internet use may be curtailed and/or highly controlled, thus limiting its potential value for education.

Alignment of school goals and the Internet's educational potential

Merely placing computers in schools does not guarantee effective use. Use depends on factors such as the extent to which teachers believe the technology helps them reach valued goals and the ease with which use fits into everyday classroom practice. For example, teachers who place very high priority on their students learning new information and ideas make more use of the World Wide Web than do those who place more emphasis on students' mastery of basic skills.

Whether the Internet fosters skills and experiences that are emphasized by existing tests is also likely to strongly influence the degree to which it is used in schools. Use of many kinds of computer applications can facilitate student achievement. Indeed, a recent comprehensive analysis of studies conducted between 1994 and 2000 on the effectiveness of educational software concluded that its use in schools is associated with gains in reading and mathematics achievement. But, the Internet is so new that strong evidence about its effectiveness in fostering various academic outcomes is not readily available, although many teachers do highly value its use in their work.

One of the great advantages of the Internet is that it can help students pursue their own individual interests. However, in many countries, national or regional exams play an important role in determining the futures and reputations of individual students and educational institutions. Such exams typically presuppose a common set of knowledge and skills that are tested. If the Internet leads to more diverse and individualized learning for students, such learning seems unlikely to raise scores on standardized examinations. This may well discourage teachers and educational institutions from taking maximum advantage of what the Internet has to offer.

Conclusion

Many potential educational benefits can flow from Internet use in primary and secondary schools. The Internet can help teachers obtain and share information easily, develop their skills in many fields, and communicate with other educators as well as with the community their school serves. For students, it can provide a potentially invaluable means of gathering information as well as of communicating and collaborating with those outside of their schools and communities.

Thus, although Internet use in primary and secondary schools holds great potential, important questions remain regarding the financial trade-offs that are necessary to bring about high levels of classroom access, how best to realize its educational potential, and how to measure its effectiveness.

Work on which this essay is based was funded by Contract No. RED-9253452 with the National Science Foundation and Grant No. 199800209 from the Spencer Foundation.

The opinions expressed in this article are those of the author and do not necessarily reflect the views or policies of the U.S. government.

The Frontiers Ahead

A Dialogue on the Progress and Promise of the Internet

Lee Rainie, Director, Pew Internet & American Life Project
George Sadowsky, Executive Director, Global Internet Policy Initiative

Two authorities discuss how Internet technologies have reshaped our lives, and how they will continue to do so in the future.

Online space is a new world created by human hands, ingenuity, and imagination. It grows larger every hour of every day, and as it does, it becomes more and more a reflection of the real world of everyday life and human interaction. The traveler in online space may find it enlightening, beautiful, charitable, and wise. But the journey can also take one to places where vulgarity, ignorance, and dishonesty exist as they do in the physical world.

Global Issues Managing Editor Charlene Porter discussed these contradictions and the state of the Internet with two professionals in the field. Lee Rainie is the director of the Pew Internet & American Life Project, a research organization studying how the American public is adapting online. George Sadowsky is the executive director of the Global Internet Policy Initiative, a group working to assist foreign governments in taking advantage of the Internet's benefits.

Question: The "evolving internet" mirrors an image frequently used to illustrate the course of human evolution. The first primates come down from the trees, begin an upright stride across the plains, and progress through several stages of development to become Homo sapiens. Compare our evolution in use of the Internet to that image. Where would you place us today on that developmental path?

Sadowsky: I think we're still swinging from the trees. The metaphor is a very good one. Many people seem to think that the Internet sprang full-blown from I don't know what anatomical part of some god or goddess. In fact, the development of information technology generally has been going on for hundreds of years. The Internet, although it is only about 40 years old now, relies on a lot of technical developments that came from previous technologies.

We haven't seen anything yet, even though we've seen an enormous amount of development from the beginning of computers in the 1950s to something now which appears like magic to most people. We can get information from anywhere in the globe—almost instantaneously. We have communication with so many people almost anywhere in the world. So many services are being layered on this magical transport device. Still, I think we're going to see a lot more, we just don't know what it is yet, but it will come.

> "You can communicate with more people in more ways, form more bonds, and learn more things using the Internet."
>
> Lee Rainie

Rainie: I actually would place us in the metaphor at a different place, but endorse a lot of what George was saying. I think that we're standing erect now. We have our basic civilian clothes on, and we're sizing up the materials for the jumpsuit that we will wear in the spaceship. We haven't picked out all the material yet, and we're still experimenting with what we want, but we now are seeing the possibilities that will exist in the not very distant future—computing that will be everywhere, access that will be everywhere, communication that can take place from anywhere to anywhere.

Q: Access anywhere, anytime, but to anyone? Surveys now show about 600 million people using the Internet worldwide out of a global population of more than six billion. As users in the developed world become ever more sophisticated in their use of the technologies, billions more don't know them at all. Does that mean the digital divide is narrowing or widening?

Rainie: I think for the short term it might widen. The people who have access are privileged in a way that people who do not have access are not.

There are five basic things that you get with the Internet that make life better for you. You can take better care of yourself. You can learn more than you used to. You can become a much better economic agent, both as a consumer and a producer. You can become a better citizen, so your power in the world grows. And finally, you become a better social agent. You can communicate with more people in more ways, form more bonds, and learn more things using the Internet.

The pace is accelerating along those five dimensions. People who do not have access are going to be left behind for the short term. There are bigger problems in their lives, though, than lack of access to communications technologies. Medical conditions are poor. The basic economic conditions are poor. Once those aspects of their lives improve, then it makes sense to worry about giving them access to information technologies.

The other thing that's easy to see in the future is that we won't depend on wires nearly as much as we do now, and the devices we use to access the Internet will be simpler.

Sadowsky: All new technologies diffuse from the time when they are introduced to the time when they have essentially saturated whatever population they are going to saturate. I think if you want to compare the diffusion of the Internet in the world, you should compare it with a few other things. The fastest diffusing technology I think was the television set. We went from the first commercial networks in the early 1950s, through the 1960s and 1970s when television was widely established throughout the world. So I don't think we should take the Internet to task for not diffusing fast enough. It's going as fast as it can.

In many countries, although not all, the private sector is the fundamental motivating force that helps that diffusion go as fast as possible.

Q: The digital divide will be a major issue on the table at the upcoming World Summit on the Information Society (WSIS) to be held in December in Geneva under the sanction of the U.N. General Assembly. What are your expectations for the summit?

Sadowsky: I think it will end with substantial agreement on platitudes, and very little actual results. That observation would apply to both the Geneva summit this year and the Tunis summit in April of 2005.

Everybody expects a lot from information technology, and information technology can bring a lot to the table, but the summit has strayed very much into the socio-political dimension, and it's trying to use information technology as a focus to solve many, many different problems.

There are also some fundamental disagreements among the countries. I read some of the accounts of the latest PrepCom (Preparatory Committee of the WSIS, held September 15-26), and the disagreements are in the area of who is going to pay for it, who is going to control it, and what kind of information is going to be allowed to circulate. Those are very fundamental divisions that exist today among the cultures.

The money issue isn't much of a division, there just isn't enough of it, and people have different priorities.

So I think the initial results will be euphoria followed by not very much of anything.

Rainie: One of the big tensions that will emerge in Geneva centers on whether access to this technology is an entitlement—an essential privilege of the human condition. No other technology has ever been discussed in that way. This speaks to the power of the Internet. We know that access to information, and better access to people, can make life better. The question is: To what degree is access to the Internet a right? That leads to discussion about who pays for it, and who gets to control the product.

It would be nice if there could be some consensus in Geneva about where we're going, the essential conditions under which the Internet is going to function. Then, we could leave it to each individual culture to decide how much government control there should be, how much should be left to the private sector, to what degree educators should be involved, to what degree there should be credibility screeners for information, etc.

Q: Let's turn to e-government, the effort by governmental entities large and small to interact with their publics online and to offer information and services to them. Some experts say that governmental entities will only truly progress in this endeavor if they are able to transcend the problems that citizens have typically complained about – slowness, inefficiency, excessive bureaucracy. How do you gentlemen assess the rate of progress in this arena of online activity?

Rainie: Clearly, a lot of people who run government agencies are having new kinds of conversations about what business they are in, whom they are trying to serve, and who are their masters? Those are good questions to be asking. In many respects, the issue isn't whether we should move government information and services online, but how we should do it that best suits the needs of our citizens.

One of the biggest arguments in information policy in the United States is to what degree should government disseminate information in an environment where bad guys might learn useful things. Americans are all for transparency and all for maximum disclosure until the word "terrorist" enters the conversation. Then they are ready to pull back and say, "No, I'm ready to leave questions about what information to release to the people who run my government. Let them determine what seems safest."

Sadowsky: I agree with that. I tend to work more in developing countries, and what I see are the initial steps—sometimes timid, sometimes brash, sometimes knowing what's happening, and sometimes not—toward implementing initial e-government functions. One of the problems we have in many governments—and to some extent in the U.S. government too—is that there are vested interests opposed to transparency. That's terribly important to try to understand and work around. One of the hopes for improving the democratic climate in developing-country governments is that e-government functions can be instituted and can lead to greater understanding among people about how their governments work, and greater interaction between citizens and members of their government.

I understand in Britain there is a service that allows any person in the country to e-mail their parliamentarian and have a pretty good chance of getting a response. That happens in the United

States when people write the President and the letters are shuffled around and finally a response is given. But the immediacy that the Internet creates, the ability to have direct contact with people in government, is terribly important, I think, for opening up governments and making people feel they have a part in the governmental process.

Q: Everything you've said is premised in the notion that government wants to respond to citizens. There are certainly any number of governments in the world that don't care to be responsive. Can these technologies force them toward greater responsiveness?

Rainie: I think that's inevitable. It won't be the case that every ministry will produce all the information all the citizens want. But the Internet gives new power and new voice to gadflies, whistleblowers, and people inside the agencies who are anxious to disclose what they know.

All the force is toward disclosure, openness, and responsiveness, but these policy issues are going to be argued over a long period.

Sadowsky: These are very enabling and exciting technologies. In the case of governments that are not particularly friendly toward the Internet in terms of implementing e-government applications, there are other considerations. A government doesn't look at the Internet just to provide e-government. Typically what I've observed in my work in the developing world is that governments will look at the Internet as a way to get on the global e-commerce train, and that train is leaving the station. That message is being broadcast and governments are listening. To the extent that e-commerce provides the motivation, the Internet is going to invade that country, and eventually the kinds of uses that are made of it in terms of enabling business relations suggest that governments are going to make good use of it also.

Vinton Cerf, one of the fathers of the Internet, said, "The Internet has never retreated." In fact, it doesn't. Once it gets in, it's going to spread. It will play out in different ways in different countries, but the Internet is going to increase its presence and there will be pressure on government to revolutionize the way it deals with its citizens.

Q: Internet surveys show that some of the Web sites receiving the greatest traffic are involved with unsavory and mundane activities—pornography, gambling, the sale of diet pills. Do those findings temper your optimism about people using the technology to become better citizens, improve their societies, and make a better world?

Sadowsky: That is a very important issue right now. I would argue that all technologies are neutral and their value depends on what use is made of them. I was just reading a book about the development of the atomic bomb, and the hope at the time of the Second World War that the bomb could be forgotten and nuclear power plants would eliminate our dependence on fossil fuels. Well, we can see what happened with that.

With the Internet, I think there's more hope that the positive side will win, and the miscreants who are flooding our networks with spam[1] will eventually lose. I don't know how that's going to happen.

We have to separate the pornography challenge from the spam challenge. I think spam is a major challenge and we're going to have to find out how to deal with that before our technology is reduced to something that is mundane and ineffective because of what is essentially a denial-of-service attack[2] by all the spammers of the world.

Evolving Internet Facts

- 25 percent of America's e-mail users say they are using e-mail less because of the electronic junk mail known as "spam."

- 75 percent of U.S. e-mail users are bothered that they can't stop the flow of spam, no matter what they do.

- 70 percent of U.S. e-mail users say spam has made being online unpleasant or annoying.

Source: "Spam: Hurting E-mail and Degrading the Internet Environment," by the Pew Internet & American Life Project, October, 2003

Rainie: The genius of the founding fathers and mothers of the Internet was to make it a system dependent on what happens at the ends of the system, not the center of the system. That means the online environment has the same good features and bad features of all human endeavors. It's going to be chaotic and ugly sometimes, uplifting and enlightening other times.

Everything that happens in the human condition is reflected in the online world. Online and offline, you've got predators, as well as people who help cure others. Online and offline, you've got hackers, as well as people who solve other people's problems. Online and offline, you've got people who commit fraud, as well as people who are good Samaritans.

Q: You both are professionally involved in the Internet, but certainly this technology has touched your personal lives as well. Give me an anecdote about how your own life has changed because of the Internet.

Sadowsky: I have been in this business a long time. I started with the Internet in 1986, and prior to that I was doing work in developing countries for the United Nations. One of the things that has radically changed is the ability for me to have a community of friends and colleagues that spans the world.

I was in Rwanda as a technical specialist for the United Nations in 1981. I was doing a debugging session on a computer we had bought to do the census. I had to ask the manufacturer of the computer a question, so I tried to make a telephone call from Kigali to Dayton, Ohio. Two weeks later, I gave up. There was no way I could do it, the communications were so poor. The telexes didn't go through, the intermediaries to forward the telexes weren't there. The radio-telephone wasn't working sometimes; it was only open two hours a day.

Now I communicate with every one of my friends in every capital of the world, instantaneously, without a problem, knowing the message will get through. I can work in this virtual community—as large or as small, as general or as specialized, as I want—to address what I want to do, and I do it with success. That opens up all kinds of possibilities in addition to making the world a much smaller and potentially friendlier and more understanding place.

This is going to happen to people generally, and maybe 20 years from now it won't be unusual for a child in school to have a "pen pal" in half the countries of the world.

Rainie: My network has changed dramatically, too. Many more people are in it, which adds some stress to my life. Many more people have a claim on my time and attention. I'm sitting here today because of the Internet. People at the State Department found me and my work through some kind of online search. Half the calls that come into our office, half the invitations that we get to talk to people about our research, come from people who have found us online. My network is growing daily.

The other dimension of my work life that is radically different is that it has ballooned. I work at home and do "home" stuff at work. I shop at work, I book my airline tickets at work, and I occasionally play games, but I also read my e-mail before I go to bed, and the first thing when I get up in the morning. I take my laptop on vacation with me to stay on top of my e-mail. I feel like I spend much more time "on the clock" than I used to.

A third thing that has changed in my life is my Sunday nights. I have teenage children, and they have very different school lives than I had. When you had a major school project in the past, you had to go to the library a couple days ahead of time to make sure you had all the research you needed for the project. Nowadays, I can't count how many Sunday night miracles we've had in my family when assignments were due on Monday, but none of the research had been done beforehand. The library has been closed for the whole day. Yet we can go online to find all the material we need to make sure the projects get done.

Q: Some skeptics out there are fearful that your teenagers and their peers are growing up with the belief that the sum total of human knowledge is on the Web. What are your concerns that a whole body of knowledge could be lost because the Internet generation lost the habit of going to the library and looking it up?

Sadowsky: It's definitely an issue. I would argue that probably less than 5 percent of the world's knowledge is online, although it's increasing rapidly and ultimately it's all going to be there.

With both published and online material, you have the similar problems of truth and reliability. Just because information appears in 12-point type doesn't make it true. What does it represent? Just as was true with books years ago, material online may carry more authority not because of the content but because of the form in which it is presented. That's a danger we're going to get over, just as we all learn how to tell fact from fancy and how to evaluate different opinions.

We'll learn to deal with these things. This is a technology that presents new challenges, and we'll learn to develop our abilities to determine the veracity of a source and stabilize a source so that we can be certain of the reliability of online information.

Rainie: You also have to recognize that the Internet is giving a new life to endangered human knowledge. The Internet is being used in wonderfully creative ways by local cultures to preserve their languages, their artifacts, and to keep their traditions going in ways that local institutions have abandoned.

Recently I heard about a medieval scholar who put an unbelievably rich database online from sources around the world. Think of the value of that kind of scholarship and that kind of archive for other people around the world. It only takes one person to put the Dead Sea Scrolls on line, and then every other person who's interested has access to it.

To think about the new possibilities for story telling and communicating is enormous. We haven't yet found our best ways to do storytelling online, but when we do, it will combine the great powers of text with the immediacy of images and do it in ways that are wholly new.

Sadowsky: This is a tool that enables individuals to do a lot of things that they otherwise wouldn't be able to do. The ability for curiosity to thrive has been given a totally new life by the Internet. One person in a developing country can use the Internet to educate himself or herself in ways that would have been totally impossible just 10 years ago. We certainly have enough problems in this world that we need the best minds applied to them. We need all the creativity we can get. As far as I can tell, intelligence is pretty evenly distributed around the world. We're not making as good use of the capabilities in the developing world. The Internet is a really strong tool for helping people to feed on the knowledge base and contribute to solving the world's problems.

[1] Spam is electronic junk mail, generally advertising. Spam can consume a significant amount of network bandwidth, and can potentially slow down or even crash network systems and even slow the World Wide Web.

[2] A denial-of-service (DoS) attack is an attack on a network that is designed to bring down the network by overloading it with useless traffic.

Lee Rainie and George Sadowsky participated in this discussion at the State Department's Bureau of International Information Programs in Washington, D.C.

The opinions expressed in this article are those of the interview subjects and do not necessarily reflect the views or policies of the U.S. government.

ADDITIONAL RESOURCES

The National Strategy to Secure Cyberspace

A White House Report

Cybersecurity is cited as a critical element of homeland security in a national strategy crafted by the Bush Administration.

In February 2003, the White House released The National Strategy to Secure Cyberspace, a 76-page document outlining a sustained, multi-faceted approach to safeguarding the nation's vital communications technologies. The strategy was developed after several years of intense consultations among thousands of individuals—officials at all levels of government, experts from the private sector, and other concerned citizens. The following excerpts reflect the course the United States pursuing to protect the complex, interconnected, computer-based systems vital to today's society.

Critical Priorities for Cyberspace Security

The National Strategy to Secure Cyberspace articulates five national priorities including:

I. A National Cyberspace Security Response System;

II. A National Cyberspace Security Threat and Vulnerability Reduction Program;

III. A National Cyberspace Security Awareness and Training Program;

IV. Securing Governments' Cyberspace; and

V. National Security and International Cyberspace Security Cooperation.

The first priority focuses on improving our response to cyber incidents and reducing the potential damage from such events. The second, third, and fourth priorities aim to reduce threats from, and our vulnerabilities to, cyber attacks. The fifth priority is to prevent cyber attacks that could impact national security assets and to improve the international management of and response to such attacks.

Priority I: A National Cyberspace Security Response System

Rapid identification, information exchange, and remediation can often mitigate the damage caused by malicious cyberspace activity. For those activities to be effective at a national level, the United States needs a partnership between government and industry to perform analyses, issue warnings, and coordinate response efforts. Privacy and civil liberties must be protected in the process. Because no cybersecurity plan can be impervious to concerted and intelligent attack, information systems must be able to operate while under attack and have the resilience to restore full operations quickly.

The National Strategy to Secure Cyberspace identifies eight major actions and initiatives for cyberspace security response:

1. Establish a public-private architecture for responding to national-level cyber incidents;

2. Provide for the development of tactical and strategic analysis of cyber attacks and vulnerability assessments;

3. Encourage the development of a private sector capability to share a synoptic view of the health of cyberspace;

4. Expand the Cyber Warning and Information Network to support the role of DHS in coordinating crisis management for cyberspace security;

5. Improve national incident management;

6. Coordinate processes for voluntary participation in the development of national public-private continuity and contingency plans;

7. Exercise cybersecurity continuity plans for federal systems; and

8. Improve and enhance public-private information sharing involving cyber attacks, threats, and vulnerabilities.

Priority II: A National Cyberspace Security Threat and Vulnerability Reduction Program

By exploiting vulnerabilities in our cyber systems, an organized attack may endanger the security of our Nation's critical infrastructures. The vulnerabilities that most threaten cyberspace occur in the information assets of critical infrastructure enterprises themselves and their external supporting structures, such as the mechanisms of the Internet. Lesser-secured sites on the interconnected network of networks also present potentially significant exposures to cyber attacks. Vulnerabilities result from weaknesses in technology and because of improper implementation and oversight of technological products.

The National Strategy to Secure Cyberspace identifies eight major actions and initiatives to reduce threats and related vulnerabilities:

1. Enhance law enforcement's capabilities for preventing and prosecuting cyberspace attacks;

2. Create a process for national vulnerability assessments to better understand the potential consequences of threats and vulnerabilities;

3. Secure the mechanisms of the Internet by improving protocols and routing;

4. Foster the use of trusted digital control systems/supervisory control and data acquisition systems;

5. Reduce and remediate software vulnerabilities;

6. Understand infrastructure interdependencies and improve the physical security of cyber systems and telecommunications;

7. Prioritize federal cybersecurity research and development agendas; and

8. Assess and secure emerging systems.

Priority III: A National Cyberspace Security Awareness Training Program

Many cyber vulnerabilities exist because of a lack of cybersecurity awareness on the part of computer users, systems administrators, technology developers, procurement officials, auditors, chief information officers (CIOs), chief executive officers, and corporate boards. Such awareness-based vulnerabilities present serious risks to critical infrastructures regardless of whether they exist within the infrastructure itself. A lack of trained personnel and the absence of widely accepted, multilevel certification programs for cybersecurity professionals complicate the task of addressing cyber vulnerabilities.

The National Strategy to Secure Cyberspace identifies four major actions and initiatives for awareness, education, and training:

1. Promote a comprehensive national awareness program to empower all Americans — businesses, the general workforce, and the general population—to secure their own parts of cyberspace;

2. Foster adequate training and education programs to support the Nation's cybersecurity needs;

3. Increase the efficiency of existing federal cybersecurity training programs; and

4. Promote private-sector support for well-coordinated, widely recognized professional cybersecurity certifications.

Priority IV: Securing Governments' Cyberspace

Although governments administer only a minority of the Nation's critical infrastructure computer systems, governments at all levels perform essential services in the agriculture, food, water, public health, emergency services, defense, social welfare, information and telecommunications, energy, transportation, banking and finance, chemicals, and postal and shipping sectors that depend upon cyberspace for their delivery. Governments can lead by example in cyberspace security, including fostering a marketplace for more secure technologies through their procurement.

The National Strategy to Secure Cyberspace identifies five major actions and initiatives for the securing of governments' cyberspace:

1. Continuously assess threats and vulnerabilities to federal cyber systems;

2. Authenticate and maintain authorized users of federal cyber systems;

3. Secure federal wireless local area networks;

4. Improve security in government outsourcing and procurement; and

5. Encourage state and local governments to consider establishing information technology security programs and participate in information sharing and analysis centers with similar governments.

Priority V: National Security and International Cyberspace Security Cooperation

America's cyberspace links the United States to the rest of the world. A network of networks spans the planet, allowing malicious actors on one continent to act on systems thousands of miles away. Cyber attacks cross borders at light speed, and discerning the source of malicious activity is difficult. America must be capable of safeguarding and defending its critical systems and networks. Enabling our ability to do so requires a system of international cooperation to facilitate information sharing, reduce vulnerabilities, and deter malicious actors.

The National Strategy to Secure Cyberspace identifies six major actions and initiatives to strengthen U.S. national security and international cooperation:

1. Strengthen cyber-related counterintelli gence efforts;

2. Improve capabilities for attack attribution and response;

3. Improve coordination for responding to cyber attacks within the U.S. national security community;

4. Work with industry and through international organizations to facilitate dialogue and partnerships among international public and private sectors focused on protecting information infrastructures and promoting a global "culture of security;"

5. Foster the establishment of national and international watch-and-warning networks to detect and prevent cyber attacks as they emerge; and

6. Encourage other nations to accede to the Council of Europe Convention on Cybercrime, or to ensure that their laws and procedures are at least as comprehensive.

The complete text of The National Strategy to Secure Cyberspace is available at www.whitehouse.gov/pcipb.

Attacks on the Internet in 2003

Congressional Testimony

Richard Pethia
Director, CERT Coordination Center

Disguised under ominous names like Blaster, Slammer, and Sobig.F, malicious computer code has brought more havoc to the Internet in 2003 than ever before. Releases of malicious code by unknown perpetrators have prompted heightened concern about the vulnerability of the Internet at the same time this worldwide system becomes ever more important to global communications and economics. The following document is an abridgment of testimony that CERT Coordination Center Director Richard Pethia presented to the U.S. Congress September 10 on the viruses and worms that have swept through the Internet in 2003 and actions needed to confront them.

The complete version of Mr. Pethia's testimony is available at http://www.cert.org/congressional_testimony/ Pethia-Testimony-9-10-2003/

The Internet is vulnerable to attack today, and will remain so in the foreseeable future.

Introduction

The CERT Coordination Center (CERT/CC) was formed in 1988 as a direct result of the first Internet worm. [The worm] was the first computer security incident to make headline news, serving as a wake-up call for network security. In response, the CERT/CC was established by the Defense Advanced Research Projects Agency at Carnegie Mellon University's Software Engineering Institute in Pittsburgh. Our mission is to serve as a focal point to help resolve computer security incidents and vulnerabilities, to help others establish incident response capabilities, and to raise awareness of computer security issues and help people understand the steps they need to take to better protect their systems. We activated the center in just two weeks, and we have worked hard to maintain our ability to react quickly. The CERT/CC staff has handled 260,000 incidents, cataloged and worked on resolutions to more than 11,000 computer vulnerabilities, and published hundreds of security alerts.

Today, with continued sponsorship from the Department of Defense and from the Department of Homeland Security, we continue our work and disseminate security information and warnings through multiple channels—a Web site (www.cert.org), an online vulnerability database, and an electronic mailing list of more than 161,000 addresses. We have relationships with major media outlets that help us distribute accurate information about major security events to the broad community. We also work with over 600 technology vendors to facilitate their response to product vulnerabilities and warn the community of vulnerabilities that require immediate attention.

The CERT/CC is now recognized by both government and industry as a neutral, authoritative source of data and expertise on information assurance. In addition to handling reports of computer security breaches and vulnerabilities in network-related technology, we identify and publish preventive security practices, conduct research, and provide training to system administrators, managers, and incident response teams.

Growing Risk from Worms and Viruses

Worms and viruses are in a more general category of programs called "malicious code." Both exploit weaknesses in computer software, replicating themselves and/or attaching themselves to other programs. They spread quickly and easily from system to system. By definition, worms are programs that spread with no human intervention after they are started. Viruses are programs that require some action on the part of the user, such as opening an e-mail attachment, before they spread....

Today, worms and viruses are causing damage more quickly than those created in the past and are spreading to the most vulnerable of all systems – the computer systems of home users. The Code Red worm spread around the world faster in 2001 than the so-called Morris worm moved through U.S. computers in 1988, and faster than the Melissa virus in 1999. With the Code Red worm, there were days between first identification and widespread damage. Just months later, the Nimda worm caused serious damage within an hour of the first report of infection. In January of this year, Slammer had significant impact in just minutes.

The figures ... show how quickly Slammer infected a significant number of computer systems. It shows that Blaster was slightly slower than Slammer, but still much faster than Code Red. After 24 hours, Blaster had infected 336,000 computers; Code Red infected 265,000; and Slammer had infected 55,000. Figure 2, "Comparing Blaster and Code Red in the First 18 Hours," shows the growth in the number of computers reached by the Blaster and Code Red worms in the first 18 hours. In both cases, 100,000 computers were infected in the first 3 to 5 hours. The fast exploitation limits the time security experts like those at the CERT/CC have to analyze the problem and warn the Internet community. Likewise, system administrators and users have little time to protect their systems.

After the initial surge of infections from the Blaster worm and subsequent patching, the impact reached a steady state of 30,000 computers in any given hour.... The Blaster worm is still active and continues to have impacts on computer systems across the globe.

Impact of Worms and Viruses

At best, worms and viruses can be inconvenient and costly to recover from. At worst, they can be devastating. Virus and worm attacks alone have resulted in millions of dollars of loss in just the last 12 months.

In the 2003 Computer Security Institute/Federal Bureau of Investigation Computer Crime and Security Survey (www.gocsi.com), viruses were the most cited form of attack (82 percent of respondents were affected), with an estimated cost of $27,382,340. The lowest reported cost to a victim was $40,000, and the highest was $6 million. The Australian Computer Crime and Security Survey found similar results, with 80 percent of respondents affected by viruses or worms. Of the victims, 57 percent reported financial losses, totaling $2,223,900. According to the Australian survey, one-third (33 percent) of the victims recovered in less than one day, and 30 percent recovered in one to seven days. The other 37 percent took more time, including two organizations that believe they might never recover.

So far, damages from the Blaster worm are estimated to be at least $525 million, and Sobig.F damages are estimated to be from $500 million to more than $1 billion (*Business Week,* the London-based mi2g at *www.mi2g.com,* among other reports in the media). The cost estimates include lost productivity, wasted hours, lost sales, and extra bandwidth costs. The *Economist* (August 23, 2003) estimated that Sobig.F was responsible for one of every 16 e-mail messages that crossed the Internet. In our own experience, Sobig.F has accounted for 87 percent of all e-mail to our cert@cert.org address since August 18. We have received more than 10,000 infected messages a day, or one message every 8.6 seconds.

Implications for the Future

The significance of our recent experience with Blaster and Sobig.F lies beyond their specific activity. Rather, the worms represent a larger problem with Internet security and forecast what we can expect in the future.

My most important message is that the Internet is not only vulnerable to attack today, but it will stay vulnerable to attack in the foreseeable future. This includes computers used by government organi zations at all levels and computers used at research laboratories, in schools, in business, and at home. They are vulnerable to problems that have already been discovered, sometimes years ago, and they are vulnerable to problems that will be discovered in the future.

The implications for federal, state, and local governments, and for critical infrastructure operators, are that their computer systems are vulnerable both to attack and to being used to further attacks on others. With more and more government and private sector organizations increasing their dependence on the Internet, our ability to carry on business reliably is at risk.

Reactive Solutions are Limited

For the past 15 years, we have relied heavily on the ability of the Internet community as a whole to react quickly enough to security attacks to ensure that damage is minimized and attacks are quickly defeated. Today, however, it is clear that reactive solutions alone are no longer adequate. To briefly summarize the factors:

- The Internet now connects over 171 million computers and continues to grow at a rapid pace. At any point in time, there are millions of connected computers that are vulnerable to one form of attack or another.

- Attack technology has now advanced to the point where it is easy for attackers to take advantage of these vulnerable machines and harness them together to launch high-powered attacks.

- Many attacks are now fully automated and spread with blinding speed across the entire Internet community, regardless of geographic or national boundaries.

- The attack technology has become increasingly complex and in some cases intentionally stealthy, thus increasing the time it takes to discover and analyze the attack mechanisms in order to produce antidotes.

- Internet users have become increasingly dependent on the Internet and now use it for many critical applications as well as online business transactions. Even relatively short interruptions in service cause significant economic loss and can jeopardize critical services.

These factors, taken together, indicate that we can expect many attacks to cause significant economic losses and service disruptions within even the best response times that we can realistically hope to achieve. Aggressive, coordinated, continually improving response will continue to be necessary, but we must also move quickly to put other solutions in place.

Recommended Actions—What Can System Operators Do?

Addressing the threat of worms and viruses is not easy. With approximately 4,000 vulnerabilities being discovered each year, system and network administrators are in a difficult situation....

In the face of this difficult situation, there are steps system operators and their organizations can take to help protect systems:

Adopt security practices. It is critical that organizations, large and small, adopt the use of effective information security risk assessments, management policies, and security practices. While there is often discussion and debate over which particular body of practices might be in some way "best," it is clear that descriptions of effective practices and policy templates are widely available from both government and private sources, including the CERT/CC....

Keep skills and knowledge current. System operators should attend courses that enhance their skills and knowledge.... They need to keep current with attack trends and with tools that help them protect their systems against the attacks. The security problem is dynamic and ever changing with new attacks and new vulnerabilities appearing daily.

Help educate the users of their systems. System operators must provide security awareness programs to raise users' awareness of security issues, improve their ability to recognize a problem, instruct them on what to do if they identify a problem, and increase their understanding of what they can do to protect their systems.

Recommended Actions—What Can Technology Vendors Do?

The steps available to system operators will help, but will only solve parts of the problem. Technology vendors are in a position to prevent the spread of worms and viruses more effectively. Although some companies have begun moving toward improvement in the security of their products, there is a long way to go. Software developers do not devote enough effort to applying lessons learned about the causes of vulnerabilities. The CERT/CC continues to see the same types of vulnerabilities in newer versions of products that were in earlier versions.

Additional vulnerabilities come from the difficulty of securely configuring operating systems and applications. These products are complex and often shipped to customers with security features disabled, forcing the technology user to go through the difficult and error-prone process of properly enabling the security features they need....

It is critical for technology vendors to produce products that are impervious to worms and viruses in the first place. In today's Internet environment, a security approach based on "user beware" is unacceptable....

Recommended Actions—What Can the Government Do?

The government can help by taking a multi-pronged approach. Actions that I believe should be investigated include the following:

Provide incentives for higher quality/more security products. To encourage product vendors to produce the needed higher quality products, we encourage the government to use its buying power to demand higher quality software. The government should consider upgrading its contracting processes to include "code integrity" clauses—clauses that hold vendors more accountable for defects, including security defects, in released products and provide incentives for vendors that supply low defect products and products that are highly resistant to viruses....

Information assurance research. It is critical to maintain a long-term view and invest in research toward systems and operational techniques that yield networks capable of surviving attacks while protecting sensitive data....

Thus, the government should support a research agenda that seeks new approaches to system security. These approaches should include design and implementation strategies, recovery tactics, strategies to resist attacks, survivability trade-off analysis, and the development of security architectures....

More technical specialists. Government identification and support of cyber-security centers of excellence and the provision of scholarships that support students working on degrees in these universities are steps in the right direction....

More awareness and training for Internet users. The combination of easy access and user-friendly interfaces have drawn users of all ages and from all walks of life to the Internet. As a result, many Internet users have little understanding of Internet technology or the security practices they should adopt. To encourage "safe computing," there are steps we believe the government could take:

- Support the development of educational material and programs about cyberspace for all users. There is a critical need for education and increased awareness of the security characteristics, threats, opportunities, and appropriate behavior in cyberspace....

- Support programs that provide early training in security practices and appropriate use. This training should be integrated into general education about computing....

The National Cyber Security Division (NCSD), formed by the Department of Homeland Security in June 2003, is a critical step towards implementation of these recommendations. The mission of NCSD and the design of the organization are well-aligned to successfully coordinate implementation of the recommendations that I have described here. However, implementing a "safer cyberspace" will require the NCSD and the entire federal government to work with state and local governments and the private sector to drive better software practices, higher awareness at all levels, increased research and development activities, and increased training for technical specialists.

Conclusion

Our dependence on interconnected computing systems is rapidly increasing, and even short-term disruptions from viruses and worms can have major consequences. Our current solutions are not keeping pace with the increased strength and speed of attacks, and our information infrastructures are at risk.... We can make significant progress by making changes in software design and development practices, increasing the number of trained system managers and administrators, improving the knowledge level of users, and increasing research into secure and survivable systems. Additional government support for research, development, and education in computer and network security would have a positive effect on the overall security of the Internet.

The opinions expressed in this article are those of the author and do not necessarily reflect the views or policies of the U.S. government.

Bibliography

Books and Documents

Barnett, Andy
LIBRARIES, COMMUNITY, AND TECHNOLOGY
McFarland & Company, 2002, 168 p.

Bimber, Bruce
THE INTERNET AND AMERICAN DEMOCRACY
Cambridge University Press, 2003, 284 p.

Castells, Manuel
THE INTERNET GALAXY: REFLECTIONS ON THE INTERNET, BUSINESS, AND SOCIETY
Oxford University Press, 2003, 304 p.

Cooper, Joel, and Kimberlee D. Weaver
GENDER AND COMPUTERS: UNDERSTANDING THE DIGITAL DIVIDE
Lawrence Erlbaum Associates, 2003, 176 p.

Franda, Marcus
LAUNCHING INTO CYBERSPACE: INTERNET DEVELOPMENT AND POLITICS IN FIVE WORLD REGIONS
Lynne Rienner Publishers, 2001, 297 p.

Mack, Raneta Lawson
THE DIGITAL DIVIDE: STANDING AT THE INTERSECTION OF RACE AND TECHNOLOGY
Carolina Academic Press, 2001, 191 p.

Marshall, Stewart, Wallace Taylor, and Xing Huo Yu, editors
CLOSING THE DIGITAL DIVIDE: TRANSFORMING REGIONAL ECONOMIES AND COMMUNITIES WITH INFORMATION TECHNOLOGY
Greenwood Publishing Group, 2003, 267 p.

Mossberger, Karen, Caroline J. Tolbert, and Mary Stansbury
VIRTUAL INEQUALITY: BEYOND THE DIGITAL DIVIDE
Georgetown University Press, 2003, 208 p.

National Academy of Engineering, Computer Science and Telecommunications Board
CRITICAL INFORMATION INFRASTRUCTURE PROTECTION AND THE LAW: AN OVERVIEW OF KEY ISSUES
National Academy Press, 2003, 104 p.
http://www.nap.edu/books/030908878X/html/

Norris, Pippa
DIGITAL DIVIDE?: CIVIC ENGAGEMENT, INFORMATION POVERTY, AND THE INTERNET WORLDWIDE
Cambridge University Press, 2001, 320 p.

Organisation for Economic Co-operation and Development
OECD GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS AND NETWORKS: TOWARDS A CULTURE OF SECURITY
OECD, 2002, 30 p.
http://www.oecd.org/document/42/0,2340,en_2649_33703_15582250_1_1_1_1,00.html

Organisation for Economic Co-operation and Development, Council
SEIZING THE BENEFITS OF ICT IN A DIGITAL ECONOMY
OECD, 2003, 28 p.
http://www.oecd.org/dataoecd/43/42/2507572.pdf

Servon, Lisa J.
BRIDGING THE DIGITAL DIVIDE: TECHNOLOGY, COMMUNITY, AND PUBLIC POLICY
Blackwell Publishing, 2002, 288 p.

Spooner, Tom
INTERNET USE BY REGION IN THE UNITED STATES
Pew Internet & American Life Project, 2003, 105 p.
http://www.pewtrusts.org/pdf/pew_internet_region_082803.pdf

U.S. Executive Office of the President
THE NATIONAL STRATEGY TO SECURE CYBERSPACE
U.S. Executive Office of the President, 2003, 60 p.
http://www.whitehouse.gov/pcipb/

Wallsten, Scott
REGULATION AND INTERNET USE IN DEVELOPING COUNTRIES
AEI-Brookings Joint Center for Regulatory Studies, 2003, 29 p.
http://aei.brookings.org/admin/pdffiles/phpvP.pdf

Warschauer, Mark
TECHNOLOGY AND SOCIAL INCLUSION: RETHINKING THE DIGITAL DIVIDE
MIT Press, 2003, 274 p.

Articles

Arunachalam, Subbiah
INFORMATION FOR RESEARCH IN DEVELOPING COUNTRIES: INFORMATION TECHNOLOGY – FRIEND OR FOE?
Bulletin of the American Society for Information Science & Technology, Vol. 29, No. 5, June/July 2003, pp. 16+

Berkowitz, Bruce and Robert W. Hahn
CYBERSECURITY: WHO'S WATCHING THE STORE?
Issues in Science and Technology, Vol. 19, No. 3, Spring 2003, pp. 55-62
http://www.nap.edu/issues/19.3/berkowitz.htm

Cerf, Vinton G.
MUSINGS ON THE INTERNET
Educause Review, Vol. 37, No. 5, September/October 2002, pp. 74-84
http://www.educause.edu/ir/library/pdf/erm0256.pdf

Chabrow, Eric
SYMANTEC VP NAMED FEDERAL CYBERSECURITY CHIEF
Information Week, No. 956, September 22, 2003, p. 30

Curry, Andrew
CAP, GOWN, MOUSE
Foreign Policy, No. 134, January/February 2003, pp. 102, 104

Dickey, Christopher, and others
TUNING IN, TURNING ON
Newsweek (Atlantic Edition), Volume 142, No. 8, August 25, 2003-September 1, 2003, pp. 46+

Hamm, Steve, and others
EPIDEMIC
Business Week, No. 3848, September 8, 2003, p. 28

Holden, Stephen H., and others
ELECTRONIC GOVERNMENT AT THE LOCAL LEVEL: PROGRESS TO DATE AND FUTURE ISSUES
Public Performance and Management Review, Vol. 26, No. 4, June 2003, pp. 325-344

Huang, Hai, and others
TRUST, THE INTERNET, AND THE DIGITAL DIVIDE
IBM Systems Journal, Vol. 42, No. 3, 2003, pp. 507-518
http://www.research.ibm.com/journal/sj/423/huang.pdf

James, Jeffrey
FREE SOFTWARE AND THE DIGITAL DIVIDE: OPPORTUNITIES AND CONSTRAINTS FOR DEVELOPING COUNTRIES
Journal of Information Science, Vol. 29, No. 1, 2003, pp. 25-35

Kalathil, Shanthi
DOT COM FOR DICTATORS
Foreign Policy, No. 135, March/April 2003, pp. 42-49

Kenny, Charles
DEVELOPMENT'S FALSE DIVIDE
Foreign Policy, No. 134, January/February 2003, pp. 76-77

Leslie, Mitch
PROJECT HELPS INTERNET HAVE-NOTS SEARCH THE WEB
Science, Vol. 301, No. 5633, August 1, 2003, p. 573

Lindsay, Beverly, and others
THE INTERNET: CREATING EQUITY THROUGH CONTINUOUS EDUCATION OR PERPETUATING A DIGITAL DIVIDE?
Comparative Education Review, Vol. 47, No. 1, February 2003, pp. 112-122
http://www.journals.uchicago.edu/CER/journal/issues/v47n1/470103/470103.web.pdf

Marshall, Patrick
CYBERSECURITY
CQ Researcher, Vol. 13, No. 33, September 26, 2003 (entire issue)

Murphy, Cait
THE HUNT FOR GLOBALIZATION THAT WORKS
Fortune (Europe), Vol. 146, No. 7, October 28, 2002, pp. 61-66

Steinberg, James
INFORMATION TECHNOLOGY & DEVELOPMENT: BEYOND 'EITHER/OR'
Brookings Review, Vol. 21, No. 2, Spring 2003, pp. 45-48
http://www.brookings.edu/press/review/spring2003/steinberg.htm

Sterling, Bruce
THE CYBERSECURITY INDUSTRIAL COMPLEX
Wired, Vol. 11, No. 1, January 2003, pg. 86
http://www.wired.com/wired/archive/11.01/view.html?pg=4

Swail, Watson Scott
HIGHER EDUCATION AND THE NEW DEMOGRAPHICS: QUESTIONS FOR POLICY
Change, Vol. 34, No. 4, July/August 2002, pp. 14-23

Warschauer, Mark
DEMYSTIFYING THE DIGITAL DIVIDE
Scientific American, Vol. 289, No. 2, August 2003, pp. 42-47

Selected Internet Resources

Aidworld Information Technologies
http://www.aidworld.org/hi/home.html

The Berkman Center for Internet & Society at Harvard Law School
http://cyber.law.harvard.edu/home/

Bridges.org
http://www.bridges.org

Center for Democracy and Technology
http://www.cdt.org/

Center for Digital Government
http://www.centerdigitalgov.com/

Center for Technology in Government
http://www.ctg.albany.edu/

CERT Coordination Center
http://www.cert.org

Computer Security Institute
www.gocsi.com

Digital Divide Network
http://www.digitaldividenetwork.org/

First Monday: Peer-Reviewed Journal on the Internet
http://firstmonday.org

Global Internet Policy Initiative
http://www.internetpolicy.net/

Institute for Security Technology Studies
http://www.ists.dartmouth.edu/

InterConnection
http://www.interconnection.org/

International Research and Exchanges Board
Internet Access and Training Program (IATP)
http://www.irex.org/programs/iatp/

Internet Security Alliance
http://www.isalliance.org/

Internet Society
http://www.isoc.org/

Internet Society
Internet Histories
http://www.isoc.org/internet/history/

National Science Foundation
Social and Economic Implications of Information Technology: A Bibliographic Database Pilot
http://srsweb.nsf.gov//it_site/index.htm

Organisation for Economic Co-Operation and Development
Information and Communication Technologies
http://www.oecd.org/topic/0,2686,en_2649_37409_1_1_1_1_37409,00.html

Process Control Systems Cyber Security (PCSCS) Forum
http://www.pcscs.org/

Professionals for Cyber Defense
http://www.uspcd.org/

Stanford Law School Center for Internet and Society
http://cyberlaw.stanford.edu/

U.S. Department of Homeland Security
Critical Infrastructure Assurance Office
http://www.ciao.gov/

World Resources Institute
Digital Dividend
http://www.digitaldividend.org/

global issues

.int http:// www. .com .org .edu .net .int http:// www. .com .org .ngo

The Evolving Internet

An Electronic Journal of the U.S. Department of State - November 2003 Volume 8, Number 3