RICE UNIVERSITY'S BAKER INSTITUTE | 20 YEARS 1993–2013

2013 POLICY RECOMMENDATIONS FOR THE OBAMA ADMINISTRATION

Christopher Bronk, Ph.D.
Fellow in Information Technology Policy

Information Technology Policy: Action Items for the Next Four Years

by Christopher Bronk, Ph.D.

Overview

In his bid for re-election in 1996, President Bill Clinton clearly identified the need to build a bridge to the next century, largely through investment in information technology (IT). Today, the U.S. innovation economy is generally synonymous with activity undertaken in California's Silicon Valley—an innovation center that is the envy of the world. The policy prescriptions in this paper largely ask how IT may confront the broad array of problems faced by the country. Eight recommendations are made on the themes of computation and jobs, cyberespionage, the militarization of cyberspace, resilient and intelligent infrastructures, digital diplomacy, and fostering innovation. This report is a very high-level overview of IT policy issues, but one that embraces the idea that highly detailed and nuanced policy directions are needed in national security, energy, health care, education, and foreign policy. The United States remains the global leader in computing, and it should be the administration's goal to enact public policy that preserves this leadership position for as long as possible.

- **Recommendation 1:** Through its national counterintelligence mandate, the administration must develop deeper collaborations with industry in the protection of key intellectual property and systems against efforts to purloin data via cyber means.
- **Recommendation 2:** The administration should reconsider its policy of offensive cyberattacks as covert action, as well as produce clear, public doctrine on U.S. intent regarding the use of force in cyberspace and guidance on U.S. options for response in the event of a cyberattack producing kinetic outcomes against the nation or its interests.
- **Recommendation 3:** The administration should embrace collective security strategies of cyberdefense with its allies and move to restore U.S. national leadership in the multi-stakeholder governance effort that manages the evolution and growth of cyberspace.
- **Recommendation 4:** Invest in further research on distributed electricity generation, resilient electricity delivery, and, where necessary, increased security for the distribution system for electricity designed to protect U.S. economic output.
- **Recommendation 5:** Work with critical infrastructure stakeholders to develop resilient architectures and systems, which have as core design components broad redundancy and capacity to withstand disruption by physical and cyber means.

- **Recommendation 6:** Work to protect a highly inclusive set of Internet governance activities that embraces technologists, industry, and members of civil society rather than shifting Internet governance entirely to an agency falling under the umbrella of the United Nations.
- **Recommendation 7:** Continue to embrace Internet-based technologies in fostering dialogue with the more than 2 billion Internet users on the planet, allowing for maximum responsibility for those foreign affairs professionals engaged in those communications.
- **Recommendation 8:** Continue, wherever possible, to preserve research funding outlays for both basic and applied science in computing, as this contributes to national competitiveness through innovation.

Background

Four years ago, interest in information technologies as a major issue for policy remained comparatively low on the Washington agenda. Moreover, most recommendations on IT policy made to the Obama transition team were focused on government management issues, such as the creation of federal chief intelligence officer and chief technology officer positions, and also as part of the broader agenda of science and technology policy. At the beginning of the second Obama administration, recommendations must acknowledge the fundamental shift in how IT is shaping economics, geopolitics, and virtually all aspects of public policy. IT mattered a great deal in 2008; in 2012, IT matters a great deal more.

This paper divides IT issues between those that would seem to fall primarily in the area of domestic policy and those landing in foreign affairs. There is one significant caveat, however, that must be addressed, and that is the enormous degree of global interconnectivity between the United States and virtually every country on the planet. The pace of dissemination for information technologies is simply staggering. We are approaching a point at which the number of mobile phones on the planet equals the number of people on it. Furthermore, more than a billion of those phones provide some degree of connectivity to the Internet. And that number—one billion—is also the number of subscribers to the Facebook social network. If it were a country, Facebook would be the world's third largest after China and India. Never before has commerce, news, and culture moved so far so fast.

The fundamental problems and prospects for the United States in the next four years can no doubt produce a long list. Slow job growth, rising federal debt, and ongoing military operations loom large as issues for the U.S. government. However, when we look for strengths in the United States, the IT sector stands as a significant driver of economic growth fueled by innovation. But IT is not only a catalyst for economic growth and productivity, it is also restructuring our entire economy, from entertainment to health care to our foreign policy and national security. More than ever before, IT is embedded in our policy issues and the prescriptions we craft for them.

Computation and Jobs

In a meeting with the late Steve Jobs, founder of Apple Inc., President Barack Obama asked how or when Apple could bring manufacturing positions back to the United States from its overseas operations, primarily in China. "Those jobs aren't coming back, Mr. President," he is reputed to have answered. But those jobs may not be staying in China forever, either. Foxconn, the manufacturing subcontractor for Apple's iPad and iPhone production lines, is already investigating how it can replace its workers with robots. We have witnessed how technological change renders entire categories of work obsolete. This is often summarized as the creative destruction identified by economist Joseph Schumpeter, although with the sunny prognostication that new jobs will be created.

Today, the United States' future economic well-being hinges upon the creation of new jobs. However, we are left to wonder what new sorts of work will emerge from our time, an era of increasingly smart machines. Erik Brynjolfsson and Andrew McAfee noted last year that "technological progress is accelerating innovation even as it leaves many types of workers behind." Innovation from Silicon Valley continues to produce enormous wealth: Consider the startup Instagram, which went from an idea to a $1 billion acquisition within 18 months of its founding, and which employed fewer than 20 people when it was bought. No doubt, American entrepreneurs are still coming up with incredible innovations, but those innovations are not leading to new areas of substantial employment. We have a society that must increasingly wonder what jobs may be performed by algorithms and, therefore, replaced by computers.

While there is no prescription for government offered here, the issue of computing and how it is impacting the employment picture deserves mention nonetheless. The 1990s U.S. economic boom was in some part a byproduct of the Internet and IT finding their place in American business, nearly a decade after economist Robert Solow opined, "You can see the computer age everywhere but in the productivity statistics." Today, big data is ubiquitous, but we are left to wonder where it will create jobs for American workers.

Cyberespionage

The economic prosperity of the United States is linked to its capacity to protect intellectual property (IP) theft by cyber means. Gen. Keith Alexander, chief of the National Security Agency, has labeled efforts by foreign entities to purloin proprietary information of U.S. firms "the greatest transfer of wealth in history." Foreign intelligence services and companies are able to utilize cyberspace and the digitally interconnected topography of the contemporary global corporation to gain access to sensitive communications, documentation, and research and development (R&D) products. The target of industrial espionage is not only the CEO or his administrative assistant, but also their smart phones and email accounts.

The simple answer to this problem is that U.S. firms need to think much more comprehensively in their cyber counterintelligence capabilities. Beyond developing their own intrinsic capacity to thwart cyberespionage, countermeasures need to become far more of a team effort, and not one solely aimed at producing technological countermeasures. We suggest the following:

> **Recommendation 1: The administration, through its national counterintelligence mandate, must develop deeper collaborations with industry in the protection of key intellectual property and systems against efforts to purloin data via cyber means. This will require the sharing of intelligence, dedication of R&D resources, and protection of corporate data from public disclosure.**

The Militarization of Cyberspace

While cyberespionage is a significant obstacle to U.S. economic development, the possibility of cyberconflict looms more real with each new piece of sophisticated malware detected by computer security labs in Moscow, Atlanta, or Cambridge. The United States has been reluctant to clearly state its military objectives and concerns in cyberspace, which it has labeled a distinct military domain standing on par with land, sea, air, and space. This is understandable, as cyberspace allows the Department of Defense (DoD) to mount synchronized military operations across vast distances with minimal delay or friction. The Internet is likely the most important system of systems ever created by the DoD in pursuit of its national security missions and mandates.

The emergence of the Stuxnet malware and information regarding cyberattacks against the nuclear enrichment infrastructure of Iran indicate that the United States has likely crossed the Rubicon into the use of clandestine cyberattacks to produce kinetic results (i.e., damage to enrichment centrifuges). What the U.S. and its allies will likely face now is cyberattacks designed to damage their economic and geopolitical interests. Foreshadowing this problem was the significant outage of computer systems at Saudi Aramco in August 2012. If undertaken by the U.S. government, was Stuxnet worth it? Time will tell, but before Stuxnet, we only hypothesized about cyberattacks with physical impacts—something that is now a distinct possibility.

> **Recommendation 2: The administration should reconsider its policy of offensive cyberattacks as covert action, as well as produce clear, public doctrine on U.S. intent regarding the use of force in cyberspace and guidance on U.S. options for response in the event of a cyberattack producing kinetic outcomes against the nation or its interests.**

> **Recommendation 3: The administration should embrace collective security strategies of cyberdefense with its allies and move to restore U.S. national leadership in the multi-stakeholder governance effort that manages the evolution and growth of cyberspace.**

Resilient and Intelligent Infrastructures

Discussion on cybersecurity issues frequently comingles with consideration of how components of the national critical infrastructure may be vulnerable to cyberattack. How systems delivering electricity, fuel, and water are modernized by employing networked computing resources is of concern, no doubt, but there are deeper questions of how current U.S. infrastructure is able to cope with evolving needs, rising population, and the digital economy. This discussion typically rises to the top of the agenda when disruption occurs.

Perhaps most worrisome today is a disruption to electricity delivery. The Electric Power Research Institute Inc. estimates that power disturbances across all business sectors cost between $104 and $164 billion per year, a figure roughly equal to the total gross domestic product of Slovakia.[1] Hurricane Sandy is only the most recent massive storm to disrupt electrical service to millions. Without electricity, the digital economy screeches to a grinding halt. SmartGrid technologies aim to build resilience into electrical distribution; however, response to massive outages produced by natural phenomena remains excruciatingly slow for affected customers. Attention is required to better protect the electrical distribution system from weather-related, usage-based, and cyber-related disruption. Dedication of significant resources to develop damage-avoidance safeguards and more rapid repair for the electricity grid would be a wise investment.

> **Recommendation 4: The administration should invest in further research on distributed electricity generation, resilient electricity delivery, and, where necessary, increased security for the distribution system for electricity designed to protect U.S. economic output.**

> **Recommendation 5: The administration should work with critical infrastructure stakeholders to develop resilient architectures and systems, which have as core design components broad redundancy and capacity to withstand disruption by physical and cyber means.**

Digital Diplomacy

One of the enduring images of the Arab Spring remains a banner from Tahrir Square that reads, "We Want Internet." Under the direction of Secretary Hillary Clinton, the State Department has incorporated many of the latest Silicon Valley innovations—Facebook, Twitter, and Google's YouTube chief among them—to facilitate global outreach. Social media has allowed U.S. diplomats to engage with foreign publics on a personal level, despite the increasingly fortified physical presence of overseas diplomatic missions.

Beyond this engagement there is the entire issue of how the Internet should be managed. The United States will be increasingly dogged by efforts to shift the governance of cyberspace from the multi-stakeholder arrangement undertaken by the Internet Corporation for Assigned Names and Numbers, the Internet Engineering Task Force, and the Internet Governance Forum. The government should resist such change and be wary

of information security issues (which focus on information content) forwarded by Russia, China, and other states desiring a greater degree of ideological insulation.

Recommendation 6: The administration should work to protect a highly inclusive set of Internet governance activities that embraces technologists, industry, and members of civil society rather than shifting Internet governance entirely to an agency falling under the umbrella of the United Nations.

Recommendation 7: The administration should continue to embrace Internet-based technologies in fostering dialogue with the more than 2 billion Internet users on the planet, allowing for maximum responsibility for those foreign affairs professionals engaged in those communications.

Fostering Innovation

This set of guidelines began with the sounding of a caution regarding the manner in which computational innovation is changing the landscape of work. Despite this concern, however, the U.S. government should continue to invest in computational research, from basic research that stands as the foundational pillars of the discipline to applied research aimed at servicing inquiry in other disciplines.

The United States still holds the lead in design and production of a sizable set of computing technologies, including the fundamentally important microprocessor sector. Ensuring that leadership requires continued government funding in mathematics, electrical engineering, and computer science. In addition, computational research is increasingly relevant in interdisciplinary projects, such as bioinformatics and high-performance computing for energy. While it no doubt sounds self-serving of a university-based research think tank to advocate for research funding in academia, such research is the basis for U.S. leadership in high-technology sectors and, thus, economic strength.

Recommendation 8: The administration should continue, wherever possible, to preserve research funding outlays for both basic and applied science in computing, as this contributes to national competitiveness through innovation.

References

1. Electric Power Research Institute, *Estimating the Costs and Benefits of the Smart Grid: A Preliminary Estimate of the Investment Requirements and the Resultant Benefits of a Fully Functioning Smart Grid* (Palo Alto, CA: Electric Power Research Institute, 2011).

Christopher Bronk, Ph.D., is the Baker Institute fellow in information technology policy. He previously served as a career diplomat with the United States Department of State on assignments both overseas and in Washington, D.C.