Remarks of Dr. G. A. Keyworth, II
Distinguished Fellow
Hudson Institute
to
The Open Source Solutions
Symposium on
National Security and National Competitiveness:

Washington, D. C.
December 1, 1992

"Government, as a Customer
in the
Digital Age"

One of the priviledges of speaking early in a three day symposium is that it presents an opportunity to try to set the stage for what will follow. Let me seize that opportunity by offering my conclusions first, then following with the rationale.

We're here at this Symposium to talk, and to think, about America's future physical and economic security, all at a time when the pace of change seems overwhelming. Some of you, like me, believe that the long debate over the importance of open source intelligence

must now, finally, come to a head. Some, also like me, believe that our national security and our national competitiveness are somehow linked. Some will see government assuming a leadership role in that linkage, where others will wonder if it can even adapt. But I doubt that any of you question government's need to change.

In pondering just how government should change, however, my own experience, inside and outside of government, leads me to conclude that government can no more assume the lead in strengthening our economic competitiveness than it did, say, in leading the personal computing revolution. What it can do is encourage healthy progress, and one way is by being a good customer. By "good," I mean, above all, enlightened. And enlightenment requires broad understanding, of the kind of change that is underway and of the forces that are driving that change.

To highlight that, let me resort to a bit of stock-taking, not from a historian's vantage, which I can't, nor from a scientist's, which I won't, but rather more as a signal-to-noise processor.

To me, one overarching word desribes the phenomena that are driving many of the changes in our world--and that word is "distributed." We call what happened in computing, with the mighty, centralized mainframe made obsolete by hordes of lowly PCs, "distributed computing." The post cold-war environment is one of "distributed threats" replacing the massive "Evil Empire." And the economic situation that has us so restless is one where corporate giants, like IBM and its mainframes, are fragmenting, and upstart nations, like PCs, look like increasingly powerful competitors. It seems like chaos, but this is in fact the transition to the "digital age," the technical manifestation of the long-awaited post-industrial economy that had to come. With this transition, the traditional barriers-to-entry that supported all centralized power, whether at IBM or in the Soviet Union, are gradually diminished.

In this analogy, I caution you not to dwell on the causal relationships, because those are high-noise issues. Instead, look to the strong signals which indicate that, in fact, America as a whole is faring quite well in this transition, arguably leading the pack. We adapted to distributed computing, putting it to work in countless ways

to create a more productive service sector, better manufacturing, and more jobs. There are nearly 80 million PCs in use in America today, far more than in the rest of the world combined. And, in spite of widespread concern to the contrary, we gained worldwide market share in computing over the last decade, both in hardware and software, all because of the speed with which we adapted.

It is American resolve, in large measure, that brought down the Evil Empire and made communism an anachronism, except for some residual holdouts in Cuba and in a few of our better universities. And, in this post cold-war period, in contrast to those after World Wars I and II, the resolve to keep America a global power remains.

In converting from a centralized industrial economy to a distributed information economy, we've progressed farther than any other nation and borne up rather well, whether in terms of employment, per-capita income, or GNP. Assuredly it has been a wrenching upheaval, but the signs are that the American wealth generating machine is adapting as well to the digital age as it did to the industrial age. And, in the conversion from a superpower-dominated

world to one of more distributed powers, our citizens, if not our government, are committed.

But it is doubt over the government's ability to adapt to this new era of digital information that has brought us together here. The point of my stock-taking preamble has been to deny that we are in decline, and to define the nature of the real challenges we must confront if we are to replace that doubt with optimism.

I've repeatedly used the word "digital" to describe this new environment we find ourselves in. Let's examine the appropriateness of using such a seemingly narrow, technical term to describe such an encompassing change, from centralized to distributed institutions. My central premise is that the importance of information to a nation's welfare is not new; what is new is the fundamental difference between the value of information that is stored, moved, and used in analog form versus that in digital form.

Each form of analog information requires its own means of storage, such as newspapers, tapes, or books; its own means of transmission, such as delivery boys, FM or VHF broadcast, or mail;

and its own means for use, whether record player, telephone or TV. In short, analog information is difficult to store, expensive to move, and awkward to use. Furthermore, because it is so inherently limited in bandwidth, it makes maximum use of audio, voice and printed word, and less of visual imagery. Yet the truly remarkable process of human vision can accomodate information rates up to 1000 times greater than our ears can. The use, and therefore value, of analog information is inherently limited.

In contrast, digital information can be stored, moved and used by common means. "Common" need not imply unique, such as a single point of data storage, or fiber-optic cable, or high-resolution display. Instead, it means transparent, where the appearance is one of easy access to and use of information. And the technology to make digital information available with nearly unlimited bandwidth is, for all practical purposes, available.

So far, I've touched but briefly on this Symposium's title--National Security and National Competitiveness. Some may see Open Source Solutions as an odd host, but I see its ascendancy as simply an

inevitable result of the digital age. The reasons are twofold: One is that, with more information openly available and in open circulation, the supply is simply richer; The other is that, with such ease of access to information, the price of protecting information is so high that classification becomes a handicap, just as so many of those barriers-to-entry that were characteristic of our industrial economy have become handicaps. In short, the fact that our National Security and our National Competitiveness will depend, increasingly, upon our ability to gather and disseminate open source intelligence is more a condition than an issue.

I've claimed that increasingly distributed power centers, whether nations or computers, is a characteristic of the digital age. I've also claimed that information is becoming both more valuable and more available, also natural to the digital age. Neither of these observations is new or startling. Let me now turn to the more debatable issue of what the government can do to maintain our national security and improve our economic competitiveness.

In doing so it would be wise to separate national security from competitivesss. Recognizing the semantic argument that national security, in the broader sense, includes a healthy economy, that linkage is nevertheless fraught with pitfalls. While it has often been proposed, naively I suggest, that we use our intelligence means to improve the competitive position of U.S. industry, it has just as often been dismissed, either because it's not practical or because it's not supportable. And, although that argument may be reopened again, it will remain a largely blind alley.

Our citizens support their armed forces, including the intelligence services, to ensure their physical security, not to ensure an upper hand in trade. Even when competition for trade is not played on a level field, they don't see the Pentagon, or Langley, as the logical point of recourse. Nor is that likely to change.

What our citizens do expect is that their physical security is maintained by a technologically advanced military, and that the massive market for advanced technology which that military represents should be a source of competitive advantage. And, for

many years it was. But, for decades that advantage has been eroding. There are many reasons, but many of them are encompassed in the perception that the government has become a poor, not financially, but unenlightened customer.

If we can focus over the next few days on how government can become a better customer, then we may give some new substance to the otherwise hollow debates over industrial competitiveness and industry-government partnerships.

I've emphasized repeatedly that a better customer means a better informed customer. Above all, that means a customer living in the digital age, not one living in the analog industrial age with all of the attendant ramifications of centralization, barriers to entry, and protection of information.

Viewing the government as a customer, what are its needs? For its principal mission of ensuring physical security, the government needs information more than it ever has. Not only have the threats become more numerous and dispersed, requiring a broader base of information to assess those threats, but the means to deal with them

has become a process of risk versus benefit analysis, multilateral cooperation, and precise targetting. Even in Desert Storm, post-conflict analysis gave rise to a new buzz word, "synoptic," referring to the nead for broader-scale and better integrated intelligence. As weapons have become increasingly more precise, as well as longer-range, lack of targetting has become the missing-link. More and more of the information required is openly available, which is one reason why the Defense Mapping Agency is beginning to look more like the National Reconnaissance Office than a cartography center. Another step in the direction of progress is that, here in an unclassified setting, I am now permitted to speak those words--NRO or National Reconnaissance Office.

Whether for targetting, battle-damage-assessment, or decision support, timely information is becoming the long pole in the force multiplier tent. If what I said earlier about America being the nation that adapted most quickly to distributed computing is true, then this trend in the force multiplier should be to our advantage. And I'm sure it is. But I'm equally sure that it can be a source of even more advantage. The trends are in the right direction, but there is a gap

between the pace of our defense and intelligence communities' adaptation to the digital age and the population's as a whole.

That gap can only widen as the next stage of distributed computing enters, which is connected computing. Some of you may wonder why I even refer to that as "the next stage." I'm looking beyond corporate and local area networks to widespread digital connectivity, to the essential infrastructure of the digital age.

The routine use of digital information came with the PC. Mass storage is coming rapidly, as compression technology and gigabyte disks proliferate, with much more on the near horizon. Fiber-optic for bandwidth, and wireless for ubiquity, are emerging as the dominant trends in digital connectivity, although copper is by no means dead. The message here is that the tools to store and use digital information already pervade our society, far more widely than in the government, and connecting them is underway. That has already led to major structural changes in our economy, changes that still await much of the government.

For a customer to adapt to changing technology, he must see a need. That's happening, albeit in a somewhat haphazard way. In our competitive marketplace, the customer learns much faster than in the restrictive way government evolves. But, even in government, the climate is changing. It's leaders are more familiar with digital technology than their predecessors, as the sight of President-elect Clinton with his AST Notebook proclaims. The public, via The Congress, is less tolerant of inefficiencies. To me, this spells opportunity.

There is an opportunity here for the government in general, and for the defense and intelligence communities in particular. It would require accelerating the trend toward closer integration of defense and intelligence. It would require special emphasis on the movement of information, in addition to its acquisition, organization, and presentation. It would require coming to grips with classification. And it would require a renewed emphasis upon the "R" in R&D, permitting government to rejoin the vanguard of information technology. None of these would be unwelcome in The Congress, and the inevitable risks could be managed if the advantages were forthcoming.

Although done in some corners, it would be necessary to learn more widely how our commercial sector uses information to competitive advantage--even through benchmarking, and how they intend to expand that as digital connectivity becomes more pervasive. It would be necessary for the government to forego its fascination with the symbolic value it places on the relic supercomputers. Most of all, it would be necessary for the government to replace its obsession with limiting information to distributing information. And, ultimately, if the government is to draw upon our national strengths, it will be necessary to develop the kind of supplier-customer relationships that pervade the fastest moving parts of our economy--those who have already adapted to distributed computing and joined the digital age.

This kind of partnership is designed to enhance our physical security, not to confuse the missions of our defense and intelligence establishments with some kind of role in ensuring economic competitiveness. Both the U.S. military and the U.S. economy are the world's best. Working together, with the government as an enlightened customer, they can both be strengthened in this time of pervasive technical and economic challenge.

FIRST INTERNATIONAL SYMPOSIUM: NATIONAL SECURITY & NATIONAL COMPETITIVENESS: OPEN SOURCE SOLUTIONS Proceedings, Volume II - Link Page

Previous	Utilization of Open Source Information to Create Intelligence in a Commercial Environment
Next	Teaching the Giant to Dance: Contradictions and Opportunities in Open Source Exploitation within the Intelligence Community

Return to Electronic Index Page