FROM INFOWARE TO INFOWAR

JOSEPH F. TRAUB[1]

[1]Supported in part by AFOSR and NSF

From Infoware to Infowar

At its first meeting on May 7 and 8, 1986, the Computer Science and Technology Board identified six critical national issues. I'll tell you about those six issues as they looked in 1986 and how they appear today from my 1996 vantage. Then I'll turn to a seventh issue which I did not want to raise publicly in 1986.

From its inception, CSTB deemed it important to look at both technical and policy issues. Looking at policy issues was fairly unusual for National Research Council Boards, at least in 1986.

Therefore, at that first meeting we heard senior federal officials give their views of the critical national issues. The officials included: Congressman Don Fuqua, chairman, U.S. House of Representatives Committee on Science and Technology; John McTague, acting science advisor to President Reagan; Gordon Bell, assistant director, computer and information science and engineering, National Science Foundation; Robert C. Duncan, director, Defense Advance Research Projects Agency (DARPA); and Alvin Trivelpiece, director of research, U.S. Department of Energy.

I'll discuss the six critical areas from May 1986. When I speak about them from my 1996 vantage, I'm giving only my own view; I've not had the benefit of discussing these opinions with the Board.

Our number one concern in May 1986 was Competitiveness. How can the U.S. best ensure the continued leadership of its computer science and technology enterprise in the face of intensified global competition?

Competitiveness was certainly a big issue in 1986. Indeed, the opening sentences of the NRC press release announcing the Board were these: "U.S. leadership in computer research and manufacturing has been seriously eroded. The National Research Council has established a computer science and technology board to advise federal agencies and private firms on ways to strengthen U.S. international competitiveness in this field and to ensure that the full promise of this area is realized." We were deeply concerned about our competitive position, particularly vis-a- vis the Japanese in areas such as chips, AI, and software. For example, we had heard that software from Japanese factories had unusually few errors.

Today, we must remain vigilant regarding our competitive position. The economic and national security stakes are higher than ever. But certainly our worst fears of 1986 were not realized. For example, according to William Spencer, President of Sematech, in the mid-80s we were losing 3 to 4% of market share per year. Today the United States and Japan each have about 40% of market share while the rest of the world has 20% of the 150 billion dollar semiconductor market. American companies are booming in software, semiconductors, internet-related infoware, and above all, in producing content. We must maintain and leverage those positions in an economy which is increasingly international.

The second item on our list was Talent. How can the gap be closed between the small number of U.S. citizens graduating with Ph.D. degrees in computer science and computer engineering, and the large demand for graduates with these skills? How can high school graduates be taught to deal with the computers and high technology they must use on the job in fields that range from the military to banking?

I'll divide that into two parts: Ph.D. production and K-12 education. We've succeeded in building Ph.D. production from some 200 a year to about a thousand a year in computer science and engineering. In the 90s there has been concern about overproduction of Ph.D.s in at least some specialties as universities and research laboratories downsize and as the field matures. I'm not convinced the country needs a thousand Ph.D.s a year in computer science and engineering. I've seen the pain in physics and mathematics since about 1970; can we learn from history? Incidentally, after a quarter of a century and due to a number of circumstances, the crunch in physics and mathematics seems worse than ever.

Since most of these Ph.D.s will not be appointed to faculty positions in the top research universities, questions have also been raised about possible changes in the Ph.D. program to produce people better suited to positions in industry and colleges.

Problems in K to 12 education seem more serious and overwhelming than ever.

There is a widespread feeling, which I certainly share, that Americans do not get the education required for an informed populace in a democracy. They do not get an education which will enable them to fill many service sector jobs. They will not be able to function in our high technology armed forces. They are not adequately prepared in analytic and writing skills to do well in the universities.

If we believe that educated people will be the key resource in the 21st century, we have much to be concerned about. Bruce Alberts, the President of the National Academy of Sciences, has identified K to 12 education as the most important problem of his presidency.

The third item on the 1986 list was scope and support. What will the nature of computer science and technology be in the 1990s? How can its health and vitality be sustained during a period of uncertainty and stringency in federal research and development budgets?

I'll divide this one into two parts also, beginning with nature and scope. It is typical of NRC boards to do a study on the nature of their fields. Some of these studies have become classics, such as the Bromley Report for Physics, and the Pimentel Report for chemistry. These set the standard to which other studies could aspire. Since we were the new kids on the block, CSTB decided that beginning with a report on the nature of the field would be self-serving. We wanted to first build a record of reports dealing with critical national issues.

Computing the Future, our study of the scope and direction of computer science and technology was published in 1992. The committee was chaired by Juris Hartmanis. Following the precedent set by Allan Bromley, I expect Juris to be named the President's Science Advisor in 2001.

Recall that the other half of this bullet asked How can the field's health and vitality be sustained during a period of uncertainty and stringency in federal research and development budgets?

OH, MY PROPHETIC SOUL!

Since there are people in this audience who have been grappling with this issue during a period of uncertainty and stringency, I won't pursue it here.

Item 4 on the 1986 list was Supercomputers. How can the power of supercomputers be exploited to promote scientific and technological advances, and how can U.S leadership in this area be maintained?

Supercomputers continue to have economic and symbolic importance. At the time that I write this paper a major battle is underway as to whether the National Center for Atmospheric Research will purchase an American or Japanese supercomputer. The contract is valued at $13 to $35 million; the amount of interest must be due to more than just the money directly involved.

A teraflop computer will soon be installed at Sandia Laboratories. Faster, more powerful machines are needed to assure the safety and effectiveness of nuclear weapons with zero testing, for aircraft design, for molecular dynamics in biology, and for cosmological computations.

The federal government's interest in supercomputers has evolved since 1986. A program plan for High Performance Computing was published by OSTP in 1989. The High Performance Computing Act of 1991 authorized a five year program in High Performance computing and communications (HPCCI). In 1995 a CSTB study chaired by Fred Brooks and Ivan Sutherland responded to a congressional request for assessment of HPCCI with a study called "Evolving the High-Performance Computing and Communications Initiative to Support the Nation's Information Infrastructure." Although high performance continues to be extremely important, there is less focus on supercomputers since the parallel processing paradigm has been accepted, and higher performance has become pervasive.

Item 5 was Software. What can be done to promote the economical production of reliable software, which represents a major portion of the cost and effort in the design and use of new computer systems?

I was looking through my CSTB files and found the following note from 1987:

"Sam Fuller says Bill Gates has really thought about software; he’d be a good person to talk to the Board." Quite so, Sam.

In April 1988, CSTB met at Stanford, rather than here in Washington. Ed Feigenbaum arranged for John Young, the President and CEO of Hewlett-Packard to host a breakfast at the company where leaders of Silicon Valley companies could tell us what national issues most affected them. Side note: Attending the meeting was the chairman of Hambrecht and Quist, one Bill Perry.

I was struck at the consensus among the industrial executives. The two most important issues were identified as K - 12 education, and software. The former was because they were concerned about finding good employees. The latter was because they saw the economical production of reliable software as a crucial problem for their businesses. This meeting underscored the Board’s concern about software.

The final item on the initial list was Infrastructure. What are the important underlying capabilities such as national networks and electronic libraries, that are needed to support the healthy evolution of computing? How can they be provided in a timely and effective fashion and integrated into daily activities to enhance national productivity?

The first two studies we published were "Toward a National Research Network" in July 1988 and "The National Challenge in Computer Science and Technology" in September 1988.

The "National Challenge" was unique in that the study was done by the Board rather than by a committee specifically appointed for the purpose. Since it was a Board report, we were all equally involved. However, Mike Dertouzos was far more equally involved than the rest of us!

The "National Challenge" presented two recommendations, and I’d like to read the first in its entirety.

"Enhanced, nationwide computer networking should be seen as essential to maximizing the benefits in productivity and competitiveness that are created by computers. Networking will facilitate the application and delivery of diverse advances in computer science and technology to the benefit of all segments of society. The board envisions an enhanced national information networking capability, and it has already begun to examine a host of related questions about how physically to improve data networking infrastructure; associated costs, impacts, and benefits; and the roles of industry, government, and other interested parties." Seems rather prescient from the vantage of 1996.

During the last ten years, infrastructure certainly became prominent in the Board's portfolio. Indeed, the CSTB was initially the abbreviation for Computer Science and Technology Board. After the Board was asked by Frank Press, then the President of NAS and Chairman of the NRC, to add telecommunications to our responsibilities, Marjory Blumenthal and I decided to rename it the Computer Science and Telecommunications Board to preserve the abbreviation.

The Board's list of critical issues in 1996 can be ascertained by looking at the list of current and future initiatives listed in the new brochure. You might want to compose your own list of the six most critical national issues in computing and telecommunications in 1996.

There was a seventh topic on my mind. Starting in 1985, I noticed various ways in which our information infrastructure was vulnerable to electronic or physical attack. I imagined myself to be a terrorist or an enemy country, and targeted aspects of what we would today call the national information infrastructure. I didn't go public with this concern because I feared it would do more harm than good.

There is now considerable attention being paid to our vulnerability, especially by the Department of Defense and there has been much media attention. However, I have strong concerns and feel now is the time to express them. My focus will be on the civilian infrastructure, although it is sometimes difficult to separate military from civilian in this domain.

It is just because we are the most advanced country in the world when it comes to our use of information technologies that we are the most vulnerable. I'll give you one illustration.

Financial security is obviously very important to us as a people. We have two primary types of assets: real estate and what I'll call virtual estate. I'll confine my comments to virtual estate.

The virtual estate consists of bank accounts, equities, CDs pension accounts, etc. As you all know, it's a virtual estate because it's recorded in electrons. If you were a terrorist and wanted to do a great deal of damage to American institutions and individuals, a natural target would be the virtual estate. Although there are electronic backups and paper trails, I'm not convinced that the virtual estate is secure.

Then there are the electrons in the foreign exchange markets. According to the Bank for International Settlement, turnover in this market is 1.2 trillion dollars a day. This, of course, overwhelmingly dominates the value of goods moved around the world. Furthermore, an amount of money which equals the annual GNP of the United States moves through the foreign exchange markets in not much over a week. And it's all electrons!

This is international, but a successful attack could have major domestic consequences; the line between international and domestic attack fades. This fading of distinctions is characteristic; we'll see more examples later.

Our virtual estate is just an example of a potential target. Others include the power grid, the air traffic control system, and the communications system.

I see the protection of information assets as a national security issue, though this view is not shared universally. In November 1993 I was one of seven civilians who participated in a seminar convened by Andrew Marshall, Director, Net Assessment, in the Office of the Secretary of Defense. Marshall is a highly respected and influential pioneer in what is sometimes called Revolutionary Military Affairs (RMA). Mr. Marshall organized the meeting because he believed that the world stands on the threshold of new information technologies that would have a profound effect on the U.S. military establishment. Participating on the military side was a group of general officers from all the services.

I argued that there was a history of the military defending transportation assets, such as rail lines, harbors, rivers, and airports during wartime. Should the armed services consider protecting the national information infrastructure? Such a mission poses many questions and its own risks. It is made even more complicated by the blurring between wartime and peacetime which has already begun and will only increase.

There was a surprising split among the participants. A number of the civilians, myself included, felt that the protection of civilian information assets might fall within the parameters of national security, while the military believed that responsibility belongs in the realm of private industry and the police.

Military uses of infowar (IW), both defensive and offensive, are clearly the responsibility of the DOD. In January 1995, the Secretary of Defense established the IW Executive Board to facilitate "the development and achievement of national information warfare goals". I recommend a 1996 RAND report, "Strategic Information Warfare" to learn more. See also a Fall 1995 report, "Warfare in the Information Age," published in Issues in Science and Technology.

I want to focus here on protection of civilian assets. Unfortunately it is difficult to separate civilian from military assets. An enemy might attack the U.S.A. exactly by attacking the civilian infrastructure. This is just an example of a more general tendency. In his book, The Transformation of War, Martin van Creveld argues that the low intensity conflicts which have become the norm since World War II will become far more prevalent and will spread to developed countries instead of being confined primarily to the Third World. He writes "As the spread of low-intensity conflict causes trinitarian structures to come tumbling down, strategy will focus on obliterating the existing line between those who fight and those who watch, pay, and suffer." By trinitarian structures he means the division between the state, the military, and the people.

Here are two specific examples of the difficulty in separating military from civilian assets. Approximately 95% of all military communications are routed through commercial lines. We buy most of the chips used in military systems from commercial vendors, many of whom are located in foreign countries.

Why might infowar be the weapon of choice of foreign or domestic terrorists, and of foreign countries, small and large? Here's a partial list:

* We are the only current superpower. As the Gulf War showed, it's foolish to challenge us in conventional war.

* Since we have the most advanced NII, it is the most vulnerable to attack. (Of course, this would give us an advantage in offensive IW.)

* Price of entry in IW is low.

* The learning curve is very steep.

* It might be difficult to detect who attacked us, or even if there was malicious intent.

Who should be in charge of protecting the civilian infrastructure against attack? I believe there needs to be strong government leadership and that it should be in the executive branch. Should the lead role be played by an existing entity, a combination of existing entities properly coordinated, or a government structure created for this purpose? This is an exceptionally complex and important issue which I won't pursue here.

It has been argued that the NII will acquire at least partial immunity due to repeated attacks, analogous to a biological organism. It has also been argued that the problem can be left to the private sector. While I believe that the private sector has a very important role to play, I'm not convinced it can do this on its own. Coordination between the government and private sectors will be another difficult and important area.

Protecting ourselves against infowar may require a careful balancing of our desire for liberty and privacy with our wish for security. As the Clipper Chip illustrates, the conflicting demands of privacy, commerce, and security can generate strong tensions. It's a particularly difficult issue for democracies, far more difficult than for countries that don't value privacy or liberty.

How imminent is a serious IW attack? How much time do we have to prepare? Unlike most conventional warfare, where there is a visible build-up of forces, an IW attack may come without warning. While we should think carefully about how to meet the threat, I believe time is of the essence.

I suggest that no issue is more important to the nation than the defense of our national information infrastructure.

ACKNOWLEDGEMENT

I am grateful to Marjory Blumenthal for her perceptive comments on a draft of this paper.

BIBLIOGRAPHY

Berkowitz, B., "Warfare in the Information Age," Issues in Science and Technology, pp. 59-66, Fall, 1995, National Academy of Sciences, Washington, D. C.

Molander, R. C., Riddile, A. S., Wilson, P. A., Strategic Information Warfare, National Defense Research Institute, RAND, Santa Monica, CA, 1996.

van Crevald, M., The Transformation of War, The Free Press, New York, N.Y., 1991.