TECHNOLOGY FOR PREVENTING TERRORISM
Enhancing Technological Innovation/Government Subsidization & Acquisition
Public-Private Sector Bridge

E. Floyd Kvamme
Partner Emeritus
Kleiner, Perkins, Caufield & Byers

We are at War. And, while our conference and panel topic doesn't use the word, WAR, I seriously doubt that we would be here today discussing this topic had the events of September 11, not happened and had the President subsequently not declared a "war on terrorism". But, to most of us, it doesn't seem like wartime – not that I have vivid recollections personally of our last declared war – World War II. But, from the movies and discussions with parents, those of my generation know there was a wartime mobilization. I even recall, as a young boy, living in the Sunset District of San Francisco how the ocean facing side of the street lamps were painted black as well as the top hemisphere of those same lamps, so that at night as one looked toward the city from the Great Highway at Ocean Beach, it looked like there was nothing there. There were "black-out" drills when all lights in the house had to be off and only the small "Scotty" radio in our kitchen could be on as we listened to hear when the "all clear" would be sounded. My father's work changed from being a carpenter working on new homes in the sand dunes of the western part of San Francisco to working at the Port of Oakland on Army facilities. We were at War and everybody knew it. Part of the reason everyone knew it was that the draft had scooped up members of many families in the community. Everyone knew of young men who had been called into service or of women who had volunteered for wartime jobs. The hope was that the death tolls of this war wouldn't be like those of the previous war, World War I, when thousands died in single days of conflict in places like Gallipoli that were hardly known to those in the West. Part of the reason, I'm sure, that everyone knew we were at war was that war, such as fought in World War I was a field and naval combat exercise fighting for territory held by the enemy. World War II turned out to be different because a relatively new technology that had played a minor role in World War I was turning out to give the allies an advantage – air power. The enemy had airplanes, as well, but our mobilization that turned auto factories into fighter plane factories soon enabled us to win the battle for the air, and, in the end airpower played a decisive role in winning the war. Not only our airpower but also our anti-airpower helped. Radar was in its infancy early in the conflict but developed rapidly as the war progressed giving us another advantage against the enemy; even radio played a role in aiding troop movements. In a sense, I believe it could be argued that electronics as an instrument of war came of age in World War II. And, while historians who are far more knowledgeable in the use of technological tools in the winning of wars, may argue the point, World War II must certainly be classified as the first time technology – the technology of airpower, radar and radio electronics, and, let's not forget, nuclear power – changed warfare.

In my college classes at Berkeley as an undergraduate engineer, many of my fellow students were war veterans – primarily from the Korean conflict – but some with WW II experience. Many choose to enter the program in Electrical Engineering in which I was involved because of their exposure to electronics in battle situations. On graduation, many in the class who had stood in the streets at dusk to see the Sputnik orbiting overhear went on to aerospace companies to help

build the next generation of fighting machine as the Cold War was in full bloom. Advanced fighter planes, better radar systems, smarter tanks and artillery were all in development in addition to the race to space. We had been beaten in launching a first orbiting satellite; we weren't going to lose the race to the moon. These were heady times for techies working at the Lockheeds, the Martins, the Littons, the Hughes, the Space Technology Labs and the myriad of other aerospace companies involved with government contracts to win not only the space race but the continuing race to having superior weaponry. Mil/Aero, as it was called in the early days of the semiconductor business was big – roughly 40% of revenues was derived from serving these markets. Except for products aimed at Consumer Electronics – principally television – virtually all new products were produced with a mil/aero customer in mind and, as products came off the production line, the screening for the top performing units was done to meet the demanding requirements of these mil/aero customers.

By the end of the sixties, the bloom started to come off of the mil/aero rose, computers were coming out of their glass houses with remote terminals springing up on desks in the front office as well as on the manufacturing floor. Handheld calculators, watches and clocks were becoming big semiconductor markets. Video games were in their infancy. Within ten years, Bill Perry, then worrying about R&D from within the Defense Department had to sponsor a special new program – the Very High Speed Integrated Circuit or VHSIC program – to try to re-interest semiconductor companies in defense needs. Bill is here at Stanford now; you can ask him, but my observation is that he had a tough time selling the concept. At National Semiconductor, we went along with the program but built a whole new facility near Tucson, Arizona, to do the work so as not to "contaminate" our commercial product lines. The eighties and the ninety only served to widen the gap between those technologies that were aimed at the burgeoning commercial markets and those aimed at military or aerospace applications. While I don't have the numbers, semiconductor procurements for products specifically manufactured for mil/aero applications by the year 2000 were probably well under 1% of the market. Furthermore, whereas the mil/aero market led the way in pushing back the frontiers of new technology for their applications in the '60s, it was the Internet, the cell phone, the DVD player, the PDA, and the personal computer and other commercial and consumer items that governed developments in the last decade. On the software side, the same could be said. Database applications for e-commerce, CRM (customer relationship management) software, data mining capability to analyze the gigabytes of data coming from point of sale systems were at the cutting edge of software development. Business application such as business intelligence, planning, managing software in addition to the plethora of package for consumer games dominated the software companies. In related fields, lasers were for optical communications in cable and telecommunications and bar-code scanning, Global positioning satellite systems were sold to consumers for their hunting expeditions into the wild or for mapping or keeping track of the fleet of trucks for delivery companies. Defense applications were not the focus of but a few of the nation's venture capital firms. Then came 9/11!

Whoa! What were we thinking? We are vulnerable. Many of those who perished in the towers were known to members of the venture and investment banking finance community that had worked with the technology entrepreneurs to build this world of instant communications, instant information, and instant wealth. What can we do to lessen this vulnerability? It is unacceptable.

Our session heading suggests three areas for us to consider. First, **Enhancing Technological Innovation.** The immediate question might be, "Is that really necessary?" We have plenty of technological innovation. We are enhancing it every day and have been for most of the last thirty years. Silicon circuits have kept apace with Moore's Law by dutifully doubling in complexity (or transistor count) every eighteen months or so, lasers have found their way into everything from simple pointing devices to the most sophisticated communications systems where dense wave division multiplexing (DWDM) technology transmits more information in a few seconds than was transmitted in an entire year back in the sixties. Display technology has brought us low cost, thin liquid crystal displays that are almost lifelike in the spectrum of color they offer while being thin and light so that our notebook PCs nowadays almost look anorexic. Sensors that will be (or have been) described at another session in today's conference have made dramatic leaps forward such that the monitoring of chemical processes to automobile engine emissions is now commonplace in industry and consumer products. It just doesn't seem that enhancing technological innovation is an appropriate way to look at the issue of using technology to prevent terrorism. But, something has changed. Company CEOs who hadn't considered the government market as interesting want to "help". They want to know where the capability of their company may help keep another 9/11 from happening on their watch. They realize that there is plenty of current day technology. It just must be aimed at the terrorism problem. That is the first challenge. Further, our technology is not only plentiful, it is also almost ubiquitous and, thus, also available to our enemy in this war. That is a further challenge. Detecting bio and chemical warfare will require the sensors and computing capability that we have designed for other applications. Data mining software and products designed to track the buying habits of major customers can be turned into products for tracking the movements of suspected terrorists. There are privacy rights issues with many of the possible products – but the technology exists. Technology has already shown its capability in the field of battle in Afghanistan – look at the precision with few errors of the bombing raids. We're told of unmanned drone aircraft aiming firepower at targets highlighted by land based laser pointers carried to the point of attack on horseback – what a blend of war, new and old. Bottom line, this first area is the easy one except for certain biological threats where much more research may be necessary. Our technology is already very enhanced and advanced; it now needs to be applied to the specific kinds of problems we face and I sense that industry is prepared to be supportive. But, technology keeps moving, so continued research is a continuing necessity. Here, government continues to play a leading role that is actually increasing. Back in the early '60s many large corporations maintained large research centers that attracted graduating technologists primarily with their advanced degrees. In the past forty years most of those private research institutions have either withered away or their role has changed such that today, much of the nation's research (as differentiated from development) takes place in the 155 or so research universities and in government labs and is sponsored in large part by government entities. This year the research budget at the federal level exceeded $100 Billion. Of course defense garners a large piece of that budget (almost half) and the National Institutes of Health are awarded about a quarter of the dollars. These are large sums of money by any measure and should help the United States maintain its lead in technology development. Again, however, the challenge as we consider terrorism is to channel the appropriate amount of that research budget into such programs. Efforts at DARPA and other advanced research agencies will, of course, continue to move the technological developments forward in very specific application areas but, generally speaking, my worry is not that America is short on technology, but rather that we have been

moving for many years in a direction that favors the commercial development of technology and not a defense or war response direction. Thus, while we have this unique moment where there is interest in being part of the solution on the part of technology enterprises, the requirements must be defined so as to be tackled efficiently by commercial suppliers.

Our second subtopic, **Government Subsidization & Acquisition,** gets at another aspect of the problem of preventing terrorism. Before 9/11, if an entrepreneur walked into my office and, I suspect, the offices of most Sand Hill Road venture firms with an interesting plan that had good technical hooks capable of keeping competitors at bay for some years through intellectual property protection, I'd be interested – of course – but my interest would be severely curtailed if the intended customer for the products of this technology were the government. Entrepreneurial endeavor and government procurement have not been considered compatible. Fortunately, it is my impression that this issue is being recognized at top government levels; whether changes will be seen down the line is not yet known. Government needs the capabilities now available to build systems that respond to threats. An interesting example of a government program that bears watching is the establishment by the CIA of In-Q-Tel. This small (by government standards) $30M fund is operating here in the Valley to co-invest with other venture partners in technologies that might have application to governmental projects. The fund will not be an exclusive founder of a startup but will seek to make the companies in which it is invested aware of markets for their products and technology that are parallel to their commercial applications. If this experiment is successful – and I am quite impressed with its leadership – we may see additional such venture arms seeking to offer funding and introductions to capabilities that will serve to address terrorist activities. Within the NIH, that, as mentioned earlier, now has a budget that is at its highest level ever, the principle activity is to improve the health of the country through the development of vaccines, biotechnology and other practical tools. But, many of the threats that now concern us are biotechnology or, at least, disease based. An interesting example is smallpox, a disease that has been eradicated. But, now, terrorists are feared to be threatening to reintroduce this plague on unsuspecting citizens of our country through infected martyrs for their cause. Proposals to examine such threats will undoubtedly require some of the NIH funds to address these threats. Outside of government, however, lies the largest opportunity for addressing terrorism. Again, the model of the '60s and the space race may be appropriate. Private industry is always looking for a market toward which to direct its development efforts. As government, perhaps through its Homeland Defense Office, specifies needs for capabilities, industry will respond if the market opportunity is clear and the acquisition criteria are seen to be profitable. Since much of what is needed may end up being a minor modification of products already produced for private enterprise many of the procurement procedures that burdened more application specific acquisitions could be done away with and a competitive market could be used as a barometer of whether government is spending its funds in the best interest of taxpayers. While government may have subsidized much of the research and development that went into a university program to develop a particular technology, it would seem that its primary role today will be to establish purchase requirements using the high level of technology already available to encourage private industry to respond more enthusiastically to government proposals.

Lastly, let me touch briefly on the last subtopic in our session title, **Public-Private Sector Bridge.** As already mentioned, the Federal government is spending over $100 Billion per annum on research. Much of this research is carried out in our research universities. Private enterprise can benefit mightily from this research as has been demonstrated in the development of much of

our nation's leading biotechnology capability. There are, of course, numerous other developments that have been commercialized including the Internet (from its 1968 beginnings), lasers and many of our communications capabilities. It could probably be argued, however, that many of these developments took too long to go from the research phase into general use in the economy. At PCAST (the President's Council of Advisors in Science and Technology), we currently have a panel that is studying the federal expenditures in science and technology and specifically looking for ways to expedite its availability to entrepreneurs and others to commercialize. Any steps in that direction could clearly benefit the economy but also address many of the terrorist's threats we now fear. This panel will also be looking at ways to ensure that our research dollars are spent efficiently. This is a huge task, but using this massive federal budget item effectively will help us build a yet stronger and more vibrant economy that will inevitably serve international markets as our technology products always have. This spreading of product capabilities has, in past decades, led to the creation of literally thousands of jobs in poorer economies. It is my firm conviction that few weapons to combat terrorists are more effective than full employment in a nation they are trying to control or destabilize. We cannot lose sight of the power of a vibrant private sector economy on combating terrorists. Lastly, technology, as already mentioned, will undoubtedly play a far greater role in this war than in any previous conflict; that already seems obvious. But, we must not forget that when in a war zone, and all of us should consider ourselves to be exactly that today here in Silicon Valley, personal vigilance will also be a deterrent. While we want to remain the open society that has made us strong and want to benefit from the advances in communications, health, and security that technology has played a role in providing, let's also commit to being alert to aberrant behavior so as to nip the 9/11 crowd that may be in our midst from using our technology against us.