Title

Secrets or Shields to Share? New Dilemmas for Dual Use Technology Development and the Quest for Military and Commercial Advantage in the Digital Age

Author

Stowsky, Jay

Publication Date

2003-02-21

Secrets to Shield or Share?

New Dilemmas for Dual Use Technology Development and the Quest for Military and Commercial Advantage in the Digital Age

by Jay Stowsky

BRIE Working Paper 151

Draft: Not for Distribution

Secrets to Shield or Share? New Dilemmas for Dual Use Technology Development and the Quest for Military and Commercial Advantage in the Digital Age

1. Introduction

For a brief period in the early 1990's the U.S. Department of Defense pursued an R&D policy that was explicitly "dual-use," funding projects aimed at simultaneously developing both military and civilian applications of the same underlying technologies.[1] The policy emerged from more than a decade of bipartisan agitation in Congress and segments of the military-industrial establishment, spurred by a shared belief that more advanced technologies now "spun on" from civilian to military applications than "spun off" in the other direction (US Department of Defense, Office of the Undersecretary for Acquisition, 1987; Gansler, 1989; Alic et al., 1992; Stowsky 1992, 1999). With the end of the Cold War and mushrooming budget deficits constraining defense spending, Pentagon planners saw dual-use development as a strategy for improving efficiency and lowering costs as well as enhancing quality by enabling the construction of sophisticated weapons systems off a more integrated civil-military technology base (US Congress, Office of Technology Assessment, 1995; US Department of Defense, 1995).

The dual-use experiment was short-lived, at least in its most conspicuous incarnation, the Technology Reinvestment Project (TRP) and the associated National Flat Panel Display Initiative. Objections to industrial policy led the newly Republican-led Congress to kill the programs early in 1995, constraining the Pentagon to develop only military-specific applications of new technologies that had no apparent civilian use and so would not compete to attract simultaneous investment in the commercial sector. This did not mean the end of dual-use development, per se, of course, as the Pentagon continued to contract with companies to develop military versions of technologies the companies were also exploring commercially; but such projects were now to be conducted with more explicit attention to keeping the two paths of development separate (Stowsky, 1996, 1999).

This remained the state of affairs until the terrorist attacks on New York and Washington D.C. in the fall of 2001, when attention turned swiftly to strengthening domestic security and protecting the American population and critical infrastructures against newly-apparent terrorist threats. Suddenly a wide range of emergent technologies and technologies already under development for commercial use in the private sector were being considered for lead roles in the war against terror. Technology policy makers were confronted immediately with two vexing dilemmas. First, how could they justify the enormous economic cost of investments in protective and preventive technological systems that in many cases would never be used? Terrorist attacks, as spectacularly

[1] When scholars assess technology policy retrospectively, they typically define the term "dual use" to mean, as Cowan and Foray (1995, p. 851) describe it, all those technologies "developed and used both by the military and space sectors on the one hand and by the civilian sector on the other." Molas-Gallart (1997, p. 370) is correct to note, however, that the eventual use by either sector of a technology initially developed for use by the other may be unexpected, and that a technology can be defined as dual-use "when it has current *or potential* military and civilian applications (emphasis added)." This is the definition of dual use that policy makers should bear in mind when designing technology development strategies prospectively and so is the definition I adopt here. See Reppy (1999) for a history of the dual use concept.

devastating as they can be, are likely to affect only one or a few population centers at a time; the impact on the rest of the population is great, but it is mostly psychological and economic. It is not possible to protect everyone at once, nor is everyone equally at risk. And those facilities and population centers judged to be most at risk might never, in fact, be hit. Thus the high costs of investment in technological systems for domestic security can become politically precarious, as taxpayers and their representatives begin to ask who and what is being protected, who and what is not, and why. Policy makers understand that the most straightforward way to justify the costs of such technology investments politically is to sponsor the development of technologies that can be put to dual use – technologies useful for military/security purposes that can also produce demonstrable social or economic benefits. For instance, a system of software, sensors, and surveillance equipment for detecting and containing a terrorist-spawned smallpox epidemic presumably can be used as well as part of new systems to detect more routine – and more routinely fatal – outbreaks of food poisoning or the flu.

This raises a second vexing dilemma -- the perennial dual use dilemma -- but with a new twist. The traditional dilemma can be posed as follows: Does U.S. military involvement in the development of advanced technology necessarily hurt the prospects for commercialization of that technology by U.S.-based firms, and does that in turn make the technology more expensive, more unnecessarily complex, and less reliably accessible for military use, thus actually undermining national security instead of enhancing it? I shall argue here that the answer to this traditional question is no, or yes, depending on a set of consistently identifiable variables. The new twist to this question is created by a combination of three developments of the last quarter of the 20th century: (1) the private sector now most often leads the public sector in the development of new technology; (2) the United States no longer dominates technology development across a range of potential dual-use applications; and (3) many of the most useful technologies for fighting terrorism – but also for helping groups to wage it – can be constituted and disseminated electronically, enabling their rapid and widespread dissemination via the Internet or other easily portable media (e.g., CD-ROM). So a new complication is added to the perennial dilemma of dual use: Can the U.S. military involve research universities and leading commercial producers (some of them foreign-based) in the development of critical dual-use technologies for military use and still deny terrorist adversaries ready access to those technologies, without impeding the free flow of scientific and technical information that is so essential to innovation and successful commercialization?

This question is especially vexing in an environment where the availability of these technologies commercially or for free can place them in the hands of terrorist groups long before complex government procurement procedures place them in the hands of military and law enforcement officials. So, not surprisingly, the first response of the U.S. military/security establishment to the new dual use question has been to answer no – to acknowledge that university researchers and commercial firms are inescapably involved in the development of dual-use technology for waging the war on terror, but to insist that they must be subject to stricter controls on who their research and development partners are, where and whether they can discuss their work and their findings, and which dual use technologies can be made available for export. I shall argue here that, in most cases, this

answer is wrong. In the digital age, the best way to pursue security by developing dual-use technology is not to shield information about the technology, but to share it. To do otherwise risks not only the prospect that U.S.-based firms will be unable to sustain and assume positions of technological and commercial leadership in these sectors, but also that the United States and its allies will be rendered less secure.

I develop my argument as follows. In the next section, I briefly address the original dual use dilemma and show how military involvement in dual use technology development can either promote or impede the commercialization of new technology by U.S.-based firms. I identify a specific set of characteristics of military involvement whose importance to commercial outcomes became evident in the 1950s and 1960s, the golden period of commercial spin offs from military sponsored projects, and that continued to operate as the Pentagon designed its first intentionally dual-use development efforts in the late 1970s and 1980s. In the subsequent sections I argue that this set of predictive characteristics has remained consistent over time, and I demonstrate this by detailing the cases of four technologies with military roots that became commercially important in the 1990s and that are now subject to renewed military scrutiny due to their apparent relevance to homeland defense.

I argue in the concluding sections, however, that the three developments I previously identified as presaging new complications for dual use policy – the shift of technological leadership from the military to the commercial sector, the decline of technological dominance by U.S.-based firms, and the emergence of critical dual-use technologies that can be constituted and thus easily disseminated electronically – require countervailing changes in the strategies defense technology policy makers use to manage flows of information about the potential applications and performance attributes of dual-use technology. Those strategies have often included secret-shielding mechanisms such as export and publication controls and citizenship restrictions on the participants who are eligible to engage in government-sponsored research. I argue here that the relative efficacy of these information-channeling strategies for promoting commercial innovation while preserving secrecy for security purposes relates to specific characteristics of the socio-technical networks that effectuate dual use technology development. The dawn of the digital age, the passage of technology leadership from the military to the commercial sector, and from the United States to a set of advanced industrial and newly industrializing countries that merely includes the United States, irreparably alters the configurations of these development networks and the military's position within them. This changes the relative efficacy of shielding versus sharing secrets as a strategy for maintaining technological superiority over adversaries, whether in the marketplace or on the battlefield.

2. Contrasting Commercial Outcomes of Military Investments in Dual-Use Technology

Disagreements over the economic impact of military involvement in U.S. technology development are nothing new (Tirman, 1984; Stowsky 1986a; Hooks, 1991; Markusen and Yudken, 1992; Cowan and Foray, 1995; Molas-Gallart, 1997; Reppy, 1999). But this

has always been a curiously disengaged debate, something more like a side-by-side press conference held by two politicians, with each candidate reciting only the facts that support her own arguments and ignoring the facts that support her opponent. There is a large, ideologically diverse literature claiming to show that military involvement in the development of advanced technology damages and depletes the civilian economy, by favoring development of technologies that are too specialized and expensive to attract commercial investment (Kaldor, 1981; Lichtenberg, 1989; Alic et al., 1992). There is an equally large and diverse literature claiming to show that military involvement in technology development has been a primary engine of technological innovation and economic growth, by sponsoring early research, paying premium prices and providing technically-sophisticated launch and demonstration markets for new processes and products (Tilton, 1971; DeLauer, 1984; Misa, 1985; Flamm, 1988; Mowery and Rosenberg, 1991). If one chooses to abandon this false intellectual coherence to evaluate historical examples of both outcomes – instances of military involvement that promoted technology commercialization and instances where commercialization was impeded – one is forced to acknowledge that military involvement in technological development is not inherently good or bad with respect to its effects on commercial performance. The contrasting effects depend on certain contrasting characteristics of the military's involvement.

In Stowsky (1986, 1992) I compared two cases of military-sponsored technology development, integrated circuits and computer numerically controlled machine tools, to represent characteristic patterns of military involvement and commercial outcomes in the 1950s and 1960s. The integrated circuit case showed how military involvement sometimes facilitated the successful commercialization of new technology by U.S.-based producers (see also Tilton, 1971; Utterback and Murray, 1977; Braun and MacDonald, 1978; Borrus, Millstein and Zysman, 1983; Steinmueller, 1986; Borrus, 1988). When military-sponsored R&D projects aimed to advance the general technological state of the art, encouraged competitive product development and the creation of efficient, general-use production technologies, paid premium prices and/or provided outlets for volume production that enabled manufacturers to realize learning economies and economies of scale over long production runs; when they occurred before the trajectory of commercial development and uses had been defined and confirmed by private investment, and when they permitted information about technological advances to diffuse to potential civilian users and to producers outside the project who were targeting commercial applications, the military's intercession in the development of new technologies helped U.S. firms to achieve technological leadership and capture market share.

When, as in the case of numerically-controlled machine tools, military-sponsored R&D aimed, instead, at the development of a military-specific product application, relied on sole-source suppliers and/or cost-plus contracts with a small set of specialized defense suppliers, and financed the creation and use of expensive, specialized production equipment to manufacture unique items in small batches; when the projects involved technologies whose commercial applications were already well-established and confirmed by a pattern of private investment and use, and when the effect of all this was to create technologies that could not diffuse easily (or at all) to the commercial sector, the

military's involvement proved either detrimental to the performance of U.S. companies in markets for the technology's commercial applications or simply irrelevant (see also Noble, 1984; DiFilippo, 1986; Collis, 1988).

Because the potentially detrimental effects on U.S. companies of military sponsored technology development were not evident in sectors like machine tools until U.S. firms were blindsided by the mass-market friendly offerings of their Japanese and German competitors in the 1970s and 1980s, policy makers typically accepted the notion that military attention was mainly a source of significant competitive advantage to the American industry. This was the firmly held belief in Europe, where such involvement was viewed as a thinly guised industrial policy by a country that was otherwise loudly opposed to such endeavors. By 1980, however, more U.S. industry and defense analysts were coming to the view that military technology had become overly specialized and expensive and that many commercial technologies, now being produced in high volumes with technically sophisticated performance attributes, were increasingly leading military applications in complexity, quality and cost (Defense Science Board Task Force, 1980; Air Force Systems Command, 1980; US Congress, House Armed Services Committee, 1980; Gansler, 1980). The U.S. Department of Defense responded with a series of R&D efforts that were explicitly dual use, geared toward involving efficient commercial producers in the production of military applications and speeding the insertion of state-of-the-art technologies, many of which were now entirely commercial in origin, into the next generation of weapons systems. In Stowsky (1986, 1992) I showed why two of these efforts – the Very High Speed Integrated Circuit (VHSIC) project and the Strategic Computing Initiative – were going to fail (see also US Department of Defense, 1982; Bruekner and Borrus; 1984; Fong, 1986; Steinmueller, 1986; Yoshino and Fong, 1986; Pollack, 1989). Because both projects funded development only of military-specific applications of the technologies that the commercial firms would not otherwise have developed themselves, these projects replicated the project characteristics that had failed to foster commercial advances (or worse, distracted companies from pursuing them) in cases such as numerically-controlled machine tools. In the end, as predicted, little of interest to commercial users emerged from either effort, and the rate of insertion of state-of-the-art commercial technology into weapons systems quickened hardly at all.

But revolutionary changes, both technological and political, were about to shift the context for dual use technology development. In one sense, ironically, all this change produced only more of the same: The characteristics of military projects that led to successful commercial spin-offs in the 1950's and 1960's continued to produce successful spin-offs in the 1990's; projects with the characteristics that created impediments or proved irrelevant to commercial development in earlier decades threatened to do so again thirty years later, though irrelevance as an outcome was more likely now because military markets for high-tech products were typically so much smaller as a proportion of overall consumer demand. The curious thing was that now not only did the military's most direct efforts to promote U.S.-based commercial development of dual-use technology (flat panel displays) fall short, and not only did a technology promoted primarily by military and NASA-trained engineers and defense contractors (intelligent transportation systems) fail to take hold in the civilian sector. The

curious thing is that both these outcomes occurred even as a technology in which the Pentagon had invested solely for its own purposes (the Internet) burst forth to virtually transform the commercial landscape, while a key dual use technology whose further commercial development the military/security establishment tried actively to suppress (strong encryption software) became one of the most ubiquitous commercial products of the decade. I examine these cases in detail in the next two sections.

3. Case Studies of Military Investment in Emergent Dual-Use Technologies[2]

Two technological systems with military roots and large potential applications to homeland security attracted broad commercial interest in the 1990's. Both systems – the Internet and the set of computer-integrated sensor, surveillance and tracking technologies known as "smart highways" or intelligent transportation systems (ITS) – began as outgrowths of military R&D. But while the internet evolved rapidly into a nearly ubiquitous civilian infrastructure ripe for widespread commercial exploitation, ITS struggled to achieve significant deployment, even in major traffic-choked metropolitan regions of the United States, save for one-off installations of systems devoted to highway on-ramp metering and electronic toll collection or on-board safety and road navigation systems affixed to luxury cars. The divergent outcomes can be traced in part to decisions made (or missed) when defense and defense-trained personnel still had effective control over development of the emerging technologies.

In the Internet case, the military provided the funding for the technology's development and mostly ceded jurisdiction over deployment to the civilian user-developers on whom the Pentagon depended for technical expertise. The demands of users employing the Internet to work on military projects facilitated the expansion of the user network beyond those users receiving direct military funding (including users outside the United States), and the Pentagon allowed civilian user experimentation and innovation to drive the trajectory of technological innovation. In the case of ITS, military demand for automated vehicles and a comprehensive integrated approach to the design of large transportation systems permeated the projects that defense-trained engineers launched from their new positions at the U.S. Department of Transportation. The technical experts they funded at research universities and the transportation divisions of defense aerospace firms shared their systems orientation to defining and solving the problems of traffic management, creating a closed socio-technical development network that hardly communicated with potential civilian end-users on the outside. Organizations that controlled access to the highways and vehicles where these systems would have to be deployed – state and local transportation authorities, automobile manufacturers -- were all but left out of the

---

[2] Cowan and Foray (1995) argue that the scope for military R&D to be of value to civilian users (or potential users) is greater when a technology is just emerging than when it is already mature and thus more standardized according to use. I agree, but add that the scope for military R&D to have a *detrimental* impact on the commercialization of a technology is also greater at the emergent stage. I do not agree with Cowan and Foray that process technologies necessarily possess more dual-use potential than product technologies; as Molas-Gallart (1997) argues, the product-process distinction is easily blurred in complex technological systems, and one can find examples of each where the scope for dual-use was large or small, depending on the relevant needs of military and civilian users.

development network. Consequently, their needs were not addressed or reflected in the U.S. ITS development trajectory, in contrast to the ITS developments underway simultaneously in Germany and Japan. ITS applications began to appear on the roads and highways of Europe and Asia in the 1990s, but technologies that emerged from the initial U.S. ITS projects were merely track tested and rarely actually deployed.

3.1. The Internet

It is widely believed that the Internet was created to achieve a specific military objective, the creation of a robust communications network that could continue to operate even if sections of it were obliterated in a nuclear attack. This characteristic did come to be a recognized and highly valued attribute of the network (Brand, 2001). But the initial goal was more prosaic. Administrators at the Pentagon's Defense Advanced Research Projects Agency (DARPA) wanted to save money on duplicative computer purchases, so they funded the development of a packet-switched, interactive computing network that might enable the agency's geographically dispersed contractors, located mostly at the nation's universities, to share expensive hardware, software and high-volume data (Abbate, 1999). This will no doubt come as a shock to any reader who happens to hold a faculty appointment at a major research university, but it's true: the idea of the internet, a convenient, anarchic, but increasingly responsive channel for efficient communication, was nurtured into existence by a bunch of government research administrators.

Because DARPA funded research at independent universities and companies, military projects to develop the technologies of computer networking involved civilians from the very start, mainly academic computer scientists. As the dominant source of funding for basic computer research in the United States (Flamm, 1988; Mowery and Simcoe, 2002), DARPA faced little resistance when it required all of its contract research sites to connect to the new computer network, the ARPANET, in 1969. DARPA thus created a unique socio-technical network of user-developers, funded by the government but based in private institutions where they were expected to pursue their search for innovative solutions wherever it led them.

DARPA depended in turn on the computer scientists' technical expertise, and this empowered the scientists to assert their own user preferences for the fledgling network. DARPA administrators had reasoned that interactive, networked computing would help the agency cut costs by creating a way for scientists to download heavily used data from remote servers (Abbate, 1999). The scientists, however, did not at first find this application especially useful. What they quickly found useful instead was their enhanced ability to communicate with colleagues about their latest work, faster and more efficiently than before. ARPANET users were soon "voting with their packets," trading huge amounts of electronic mail. Quickly, more and more researchers, both within and outside the United States, were clamoring for access. The net's first "killer app" was born (Zakon, 2001; Mowery and Simcoe, 2002).

Throughout this early period, DARPA maintained formal jurisdiction over access to the ARPANET. DARPA administrators looked the other way as "unsanctioned" users,

mainly researchers at universities and corporate laboratories who were not working on DARPA-funded projects, logged on, some located outside the United States. Such openness suited the innovative academic culture that DARPA sought to support. The agency reasoned that a robust civilian demand for computing applications would ensure their continued availability for national defense purposes. In addition, the growth in network traffic facilitated more statistically significant evaluations of the system's overall technical performance. With DARPA's blessing, Jon Postel, starting as a civilian graduate student in UCLA's computer science department, held an important gatekeeper position over the ARPANET for many years. Beginning in 1969, suggestions for improvements and new features on the ARPANET were mediated via an informal online newsgroup and posted as successive Requests for Comment (RFCs) that were edited by Postel (Mowery and Simcoe, 2002). A precursor to the open source approach to developing computer software (Weber, 2000), these successive RFC posts became a central online exchange of ideas, critiques, and proposals from the entire user-developer network for improving and expanding the ARPANET; here originated technical specifications for Telnet, FTP, and several other novel network applications (Mowery and Simcoe, 2002).

Note these key features of the military-sponsored R&D efforts that led to the development of the internet: military involvement occurred at an early stage in the system's development, before a commercial development trajectory or set of uses had been defined and confirmed by a pattern of private investment. The military envisioned but did not insist on a specific use for the technology; it remained neutral with respect to civilian applications. Most important, the military allowed the civilian user-developer network to expand beyond those directly engaged in using the internet to work on military-funded projects, facilitating scale economies and more opportunities for learning, experimentation and innovation. Information about military-funded advances and innovations were permitted to diffuse broadly to other potential user-developers, most significantly a description of the core TCP/IP inter-networking protocol, which was published by its defense-funded creators in the *IEEE Transactions on Communication* in 1974 (Mowery and Simcoe, 2002).

DARPA never wanted to be in the business of running a routine data communications network, however; it was, and wanted to remain, strictly a research funding agency. By 1972, DARPA was ready to contract operational responsibility to a private entity, but its initial choice, AT&T declined the invitation (Abbate, 1999). So, on July 1, 1975, the responsibility for the ARPANET passed to the Pentagon agency normally tasked with providing communications services to the armed forces and the agencies that support their daily operations, the Defense Communications Agency (DCA).

The DCA's first moves upon gaining jurisdiction over the ARPANET were not of a type likely to promote the successful commercialization computer networking technology down the road. DCA had recently upgraded, with packet-switching technology, the global computer network used by commanders to store war plans and check on the status of armed forces (the Worldwide Military Command and Control System) (Abbate, 1999). This new technical capability was enhanced by a transfer to DCA of hardware and skilled

personnel from DARPA, both of which also facilitated DCA's assumption of operational responsibility for the ARPANET. But DCA's mission was to provide *secure* communications for military operations. It was not about to look the other way as unauthorized users trafficked on the ARPANET. The agency set about attempting to reign in the membership of the user network and put in place stricter controls around ARPANET access.

At the same time, DCA was preparing to deploy a new message-switching network of its own, purchased from Western Union (Abbate, 1999). The new network would replace the outdated Automated Digital Network (AUTODIN) that DCA had built in the early 1960's. The new network, to be called AUTODIN II, was initially slated to replace AUTODIN and the strictly military sites on the ARPANET. But keeping its own mission foremost, DCA soon concluded that research experiments of the type routinely conducted on the ARPANET might be dangerously disruptive to an operational military communications network. So DCA decided to leave the research portion of the ARPANET intact. When military users complained that the new AUTODIN II messaging network was balky and overly costly, DCA administrators turned to the best source of expertise available on global network communications – an international group of ARPANET users – to design an alternative system (Abbate, 1999). Employing the open and interactive approach to technology development that they had learned from participating in Jon Postel's Request for Comments process, the new international user-developer group created the Defense Data Network; it was based on the TCP/IP protocols and incorporated the existing ARPANET when it was chosen to replace AUTODIN II in April 1982.

It was at this point that the DCA (with DARPA's support) mandated the adoption of TCP/IP by all host computers connected to the ARPANET (Mowery and Simcoe, 2002). This decision was motivated by military interests; the armed services' command, control and communications systems required connectivity between multiple, technically-diverse computer networks, and the services needed a single, shared protocol to enable them to connect and operate as one system. Thus, at this point in the evolution of the internet, the operational needs of military and civilian users were technically complementary; both needed standardized protocols to enable disparate computer networks to communicate with each other, to construct a "network of networks." TCP/IP fit the bill for both sets of users.

Finally, in 1983, after several years of trying and failing to work with academic research sites to restrict access to the ARPANET, it at last became clear to the DCA that the needs of military users for secure, dependable communications networks would never be compatible with the needs of civilian users of the ARPANET for openness and experimentation. With DARPA's backing, DCA split the network in two (Abbate, 1999; Mowery and Simcoe, 2002). One section of the network, now named MILNET, would become the operational military communications network equipped with strong encryption to restrict access and enhance security. The other section, the ARPANET, would again become an entirely research-oriented network, based primarily at the nation's research universities. This was the fateful first step to what would soon become

civilian control of the newly named Internet, first by the National Science Foundation, which managed the process of privatizing the network and helped set the stage for its explosive commercial growth after 1995 (Kenney, 2001).

On balance, then, the same characteristics of military involvement that facilitated the early commercialization of integrated circuits in the 1960s worked to facilitate the commercialization of the Internet in the 1990s. The military R&D efforts in question were designed to advance the general technological state of the art of computer networking, not any specific networking architecture or application. Military needs, first for a less costly means of communication between geographically separate research groups and then for a standard interconnection protocol to enable communication between disparate computer networks around the world, coincided with the evolving needs of civilian users. This opened up a host of opportunities for commercial exploitation later on. The Internet was in the formative stage of its development, with mostly public investment and no established commercial development trajectory; military sponsors remained neutral about applications, allowing a diverse user network to develop and expand. Technical advances were allowed to pass quickly into the public domain; DARPA's procurement policies, which often funded work by start-ups with novel technical approaches, also supported dissemination of technical information and further expansion of the user-developer network. Finally, when it became clear that there was an unbridgeable divergence in the needs of military and civilian users for particular system performance attributes, the DCA abandoned its initial efforts to insist that the military's desired attributes prevail. Instead it split the network in two, spinning off the civilian network entirely but continuing to build its specialized MILNET network using the civilian Internet protocols and, wherever possible, commercial sources for network components.

3.2. Intelligent Transportation Systems (ITS)

During the late 1960s and early 1970s, years in which new technologies were being developed to network computers, a small group of aerospace and defense engineers was beginning to imagine how computer and communications technologies might be used to control and track motor vehicles. With Congress and the Pentagon wishing to keep these engineers gainfully employed despite cuts in military and space budgets in the wake of America's declining involvement in Vietnam and the pending end of the Apollo space program, many of these engineers were transferred to the U.S. Department of Transportation (DOT), where they continued to develop their ideas (Wilshire, 1990; Klein, 2001). The entire NASA Electronics Research Center, for example, was reassigned to DOT. Defense contractors, including Raytheon, instigated work on freeway merging control systems, and radar specialist Sperry Rand began work on technologies for enabling traffic lights to change their timing in response to changes in the flow of traffic (Klein, 2001).

When defense spending rebounded beginning in the late 1970's, funding for this research dropped and the work stalled, but not before interested engineers from Japan and Germany had visited an early U.S. test track (Klein, 1996a). They returned home and

proceeded with efforts to realize the American defense engineers' ambitious technical vision: automated highways, the application of networked computer and communications technologies to passenger vehicles and surface roads, the transformation of the passive road network into a dynamically-controlled system for moving parcels and people more quickly and efficiently and cleanly. While the technical vision of the Japanese and the Germans was adapted to the institutional realities of their domestic polities, the U.S. vision remained dormant – and unchanged – until the next major defense build-down following the end of the Cold War.

When the Cold War did end, a large socio-technical network in the form of academic researchers, defense-trained engineers in government (including those who had worked on the original ITS projects at DOT twenty years earlier) and private defense industry faced the prospect of permanent reductions in government support. Coincidentally, the construction of the interstate highway system, a massive public infrastructure project started under the National Defense Highway Act at the height of the Cold War, was nearing completion; its government patron, the Federal Highway Administration (FHWA), was searching for a new mission. Traffic congestion, highway safety and air pollution seemed to be obvious social ills demanding some type of organized public response. With the personal computer revolution of the 1980s still fresh in mind, high tech competition from Germany and especially Japan a hot topic of debate nationally, and the burgeoning internet already a routine tool for researchers in government, industry and academia, it did not take long for a coalition of engineers, academics, and transportation planners to promote the development of "intelligent vehicle highway systems" (later re-christened "intelligent highway systems" or ITS) as a matter of urgent national priority. Their efforts sped passage of the Inter-modal Surface Transportation Efficiency Act (ISTEA) of 1991, which would, among many other things, devote $1 billion, ultimately, to the development of intelligent transportation systems in the United States.

Just as developers of ITS in Germany and Japan adapted their ITS plans to reflect their main sources of technical expertise and the needs of their primary sources of funding – in Germany, the primary source for both was the Siemens Corporation, and in Japan, the auto manufacturers and two government ministries, one with authority over roads, the other over highways – the U.S. ITS projects reflected the composition of the American socio-technical network that emerged to direct the technology's development.[3] Klein (2001) details the military-specific projects on which a majority of U.S. ITS researchers had previously worked: "aircraft radar target simulators, fire control systems for B-52s, military identification/friend or foe, electronics intelligence, vacuum tube fuses, and weapons system engineering." Because deployment was a few years down the road, so to speak, the American developers did not need immediate access to the highway on-ramps and surface roads over which they had no jurisdiction; auto manufacturers were content to lend a few test cars and assign a few engineers to participate in sub-projects. So the interests and needs of the largest groups of prospective civilian users – state and local

[3] Klein (1996a) demonstrates how the composition of the socio-technical network evolves as the sources of critical resources (financing, technical expertise, jurisdiction over the sites where new technologies are deployed) shift through sequential stages of technological development (design, testing, deployment).

transportation authorities and car buyers – did not intrude on the technical vision of the former defense engineers and their partners in the defense industries and academia.

With little input from prospective civilian users to nudge their technological explorations in different directions, the problems and solutions that characterized projects in the U.S. ITS program continued to reflect an overall orientation toward technical performance attributes typically valued more by military than civilian customers: systems integration and automation. One major ITS project aimed at the creation of system architecture for a comprehensive national approach to traffic communications and control; Lockheed-Martin, Loral, TRW, Rockwell, and IBM were among the established defense contractors involved in the project, and two federal nuclear weapons laboratories plus NASA's Jet Propulsion Laboratory were signed up to lend their powerful supercomputers to simulate the effects of various highway monitoring approaches on nationwide freight and auto traffic (Klein, 1996a, 2001). Another major U.S. ITS project, led by transportation researchers at the University of California at Berkeley, focused on the creation of a system for enabling cars to "platoon," that is, to connect like the cars of a train on highway lanes specially outfitted with sensors and actuators. The platoons would be guided automatically at higher speeds but with a lower probability of accident than groups of conventional non-networked cars speeding after one another down regular asphalt lanes (Hsu, 1991; Alvarez and Horowitz, 1997).

The attitude of state and local highway officials to these projects ran the gamut from skepticism to simple disinterest; they had more immediate problems to solve. As the largest group of likely civilian end-users of ITS technologies, the state and local transportation agencies were still almost entirely devoid of the expertise in computing and electronics that would be required to install and run them. They certainly lacked the billions of dollars it would cost to construct the new automated highways. Technological advances that they might actually use to monitor and manage traffic in the near term were of a more mundane order, technologies such as electronic toll collectors, highway on-ramp meters, and video cameras for real-time monitoring of traffic conditions. Meanwhile U.S. automobile manufacturers possessed enough technical expertise and financial resources on their own to provide the few "intelligent" vehicle innovations that American car buyers appeared to desire and that German and Japanese auto makers were preparing to provide, things such as on-board navigational assistants, theft protection devices and auditory warning systems. One by one, the automakers dropped out of the federally funded projects. At last, in 1996, the Clinton Administration reoriented the federal ITS program dramatically to focus on the diffusion of ready-to-go technologies that would be more in line with the actual expressed needs of civilian end-users. Funding for the largest defense-oriented technical approaches was cut or eliminated outright (Klein, 1996b).

Thus, at a stage when ITS technologies were just emerging, before the trajectory of commercial development and use had been set and confirmed by a pattern of private investment, space and defense engineers transferred to FHWA and their colleagues in the research universities and the aerospace industry focused on the development of product attributes and architectures that continued to embed the distinctive priorities of military

end-users. For several years, years during which parallel German and Japanese projects were testing and then implementing large-scale integrated road-vehicle communications systems for civilian use, the U.S. research effort paid little heed to the needs of the two largest groups of potential civilian end-users, state and local transportation agencies and domestic car buyers. As a consequence, the program contributed little in the way of useful commercial spin-offs and contributed instead to the delayed and fragmentary deployment of ITS technology in the United States.

4. Case Studies of Military Investment in Commercially Available Dual Use Technologies

When military interest turns to a technology whose commercial development trajectory has already been set and confirmed by a pattern of private investment, military efforts to enlist U.S.-based firms to further develop the technology can have a detrimental competitive effect, as can military efforts to assert more control over further commercial development or diffusion of the technology. In some cases, however, commercial production and use of the technology is already so widespread at home and abroad that the competitive impact of new military interventions is negligible. Finally, other than providing a small, but potentially lucrative set of new customers, there is not much prospect that military involvement at this stage will facilitate significant additional benefits for domestic commercial producers.

In many cases, the markets for existing commercial applications are already so much larger than the market for prospective military applications that the Pentagon's main challenge is simply to coax commercial enterprises to build additional versions of the technology, equipped with the specialized performance attributes that military users need. The Pentagon has undertaken several initiatives that attempt to make this prospect more attractive by encouraging its suppliers to use as many commercially-available parts and processes as possible and by trying to reform procurement procedures so that the suppliers' on-going commercial activities are not gummed up in government red tape. In other cases, however, new security restrictions on the involvement of foreign nationals in research and development or strengthened export controls on commercial technologies that are already available abroad and at home can still prove highly detrimental to the economic performance of U.S. firms. Where both American and foreign-based suppliers exist, the detrimental impact on U.S. producers is more likely to be felt through the mechanisms that attempt to control diffusion (e.g., export controls); when there are only a few small prospective U.S. players, then their fledgling attempts to establish market share can be stymied if military efforts to help them also exclude foreign-based partners from participating in U.S. government-funded procurement and research. The case studies that follow examine the development histories of two more technologies that attracted intense commercial attention during the 1990s and have since attracted renewed attention in the war against terror; flat panel displays (FPDs) and strong encryption software. The case studies illustrate that military efforts to intervene in the further development of commercially available technologies can have a detrimental competitive impact on U.S. firms.

4.1. Flat Panel Displays (FPDs)

The Department of Defense had rather little involvement with the development of flat panel display technology in its early stages, but once important military applications of the technology became apparent in such things as portable navigational devices for soldiers in the field and heads-up cockpit displays for pilots of fighter planes, the Pentagon became more interested in getting commercial suppliers to adapt the devices for military use (Murtha, Spencer, and Lenway, 1996; Murtha, Lenway, and Hart, 2001). When the world's dominant FPD supplier, the Sharp Corporation of Japan, balked at taking the Pentagon on as a customer, the Defense Department began to focus on securing a reliable domestic source of supply. This posed a problem: by the early 1990s, U.S. based firms accounted for less than 10 percent of global FPD production. Military demand would never make up more than 5 percent of the U.S. market for the devices, and makers of defense R&D policy, having learned some lessons from prior failed attempts to promote dual-use production in the civilian sector, wanted military FPDs built off a robust domestic commercial base (US Department of Defense, 1995).

Like so many other essential component technologies, the displays so successfully commercialized by Japanese electronics companies in the 1990s had been invented in the United States. During the 1960s and 1970s, engineers at several U.S. universities and industrial labs examined the properties of liquid crystals as an alternative to traditional transistors and cathode ray tubes for use in television sets. Then, one by one, large U.S. electronics manufacturers abandoned such research, opting instead to recoup their investment more quickly by licensing their un-marketed technologies to Japanese companies. The devices soon showed up in Japanese-made pocket calculators, then watches and clocks, then portable black and white TV sets. The Japanese companies built production expertise and added both technical sophistication and global market share product by product. By the early 1990s, FPDs were critical components in a range of advanced mass consumer products, particularly laptop computers, as well as in medical devices and, as noted, military equipment, and Japanese producers dominated the world market (Borrus and Hart, 1992).

A few small U.S. based start-ups had managed to persist, emphasizing proprietary versions of FPD technology, and struggling to attract large-scale investment. The Defense Department provided them some small amounts of funding for research aimed at developing military-specific variations of FPD devices (Murtha, Spencer, and Lenway, 1996, p. 266). FPD technologies can vary across a set of attributes, including weight, durability, power consumption, viewing angle, clarity, and manufacturing cost. Military applications tended to value durability and low power consumption over more commercially critical attributes, such as the breadth of the display's viewing angle and cost. When the Pentagon turned its attention toward FPDs in a more focused way in the early 1990s, commercial demand was virtually the sole driver of technological development in the industry, and the large producers, including the largest, Sharp, had little motivation to invest in producing the specialized displays that the Pentagon wanted.

Defense technology planners in the incoming Clinton Administration developed a novel solution. The National Flat Panel Display Initiative, launched in 1994, would seek to generate a domestic source of supply for military-specific FPDs by creating conditions that would reduce the perceived risk to U.S. producers of investing to enter high volume consumer markets for the devices. The government would subsidize the construction of two manufacturing test beds and provide research funding to firms that committed to domestic volume production of current generation FPDs. They also had to commit to supply some devices that met the Defense Department's specialized performance requirements. The goal was to increase U.S. commercial production capacity to 15 percent of the world market, a quantity of production sufficient, program designers believed, to guarantee a self-sustainable infrastructure of FPD materials and equipment suppliers in the United States, as well as to secure early access for the Pentagon to new FPD designs (US Department of Defense, 1995).

Creators of the initiative were careful to keep it neutral with respect to FPD technologies and the U.S. companies that specialized in developing each one; Pentagon officials were exquisitely sensitive to the claims of academic and Congressional opponents who criticized the initiative as a thinly-veiled attempt at industrial policy that would enable the Pentagon (and the White House) to substitute their own politically-motivated investment preferences for those of the market.[4] Thus many competing companies and many competing FPD technologies (LCD, TFT, EL, PDP, and FED) received financial support from the program, even though Japanese producers had already standardized around active-matrix LCDs. Any companies able to demonstrate a "firm commitment" to volume manufacturing of current generation FPDs in the United States were eligible for the program's "focused R&D incentives" to promote the development of next-generation product and process technologies.

The hitch came over whether the definition of "any companies" really meant only *American* companies. A primary motivation for the Defense Department's attempts to influence the course of the FPD industry's further commercial development was the security concern about overdependence on foreign sources of supply for militarily critical FPD components (US Department of Defense, 1994). Pentagon technology planners were quite aware that the cutting edge of FPD technology development was located in Korea and Japan. So designers of the National FPD Initiative and the broader Technology Reinvestment Project (TRP), which provided a large portion of the funding for the FPD initiative, specifically planned to allow for the participation of the most technologically advanced firms in the industry, even if they were foreign-owned. However, although the funding for the initiative came from the Department of Defense, the Department's funding was authorized and appropriated by the U.S. Congress. And the congressional authorization language specifically prohibited the participation of non-U.S. firms in these U.S. taxpayer funded technology development projects.

The conflict was never fully joined nor was it ever fully resolved. The Republican victories in the congressional elections of 1994 effectively ended the FPD initiative

[4] The next few paragraphs draw heavily on the author's personal experiences as senior economist for science and technology on the staff of the White House Council of Economic Advisers (1993-1995).

before it ever had a chance to have a major impact, for good or for ill. The plug was pulled on the Pentagon's dual use investment experiments; henceforth military R&D was to target military-specific applications only. In practice, however, the congressionally mandated limitations on foreign participation had already proved detrimental to the competitive prospects of U.S.-based FPD producers. Participation in these programs biased U.S. producers toward working only with U.S.-based materials and equipment suppliers, the very firms whose lack of high volume FPD manufacturing capacity and experience had motivated the FPD initiative in the first place. The political context of the program, inescapable so long as Congress held the purse strings, kept U.S. participants from forming strategic alliances with foreign partners. But foreign partners were the best available sources of technical expertise on FPD design and manufacturing in the world, the very firms who knew the most about high quality, low cost FPD production.

The U.S. Display Consortium, the private non-profit organization of FPD producers, users, materials and equipment suppliers that persevered following the FPD initiative's demise, belatedly acknowledged this reality in 1999, when it amended its charter to admit foreign-owned companies to associate membership. By then it was too little, too late. U.S. computer manufacturers had continued to source their high volume FPD purchases from Japan and Korea. Despite the FPD initiative's steps to avoid it, the small U.S. industry had become dependent on specialized military orders, and the military market was too small to keep even the last two remaining U.S.-based FPD suppliers in business. Indeed, the Pentagon used comparisons with the high volume Asian producers to set prices, despite the fact that the small U.S. suppliers of specialized military devices faced significantly higher costs. The crowning irony came at the beginning of 2000, when the only remaining U.S.-based producer of a certain class of military FPDs, Planar Systems, declined to supply the Pentagon further, just as Japan's Sharp Corporation had done a few years earlier, unless it could raise prices to cover costs (Murtha, Lenway, and Hart, 2001).

4.2. Strong Encryption Software

In contrast to the case of FPDs, strong encryption software was a focus of concentrated military attention early on. For nearly half a century, however, the discovery and development of ever more elaborate crypto algorithms by the National Security Agency (NSA) remained a state secret; for a commercial sector to evolve in the United States, the same or similar innovations had to be generated independently by civilian researchers. Their extraordinary achievements from the 1970s on were not viewed as benign by the world-class eavesdroppers at the NSA. From the very beginning, the NSA and its allies in the military-intelligence establishment sought to control and direct the technology's commercial evolution in the U.S. As commercial applications developed by U.S. companies nevertheless became ever more sophisticated and widely accessible, the full weight of the federal government was brought to bear to control the pattern and pace of their diffusion. Backed by tremendous pressure from large civilian users, particularly after the commercialization of the Internet in 1995, the commercial producers finally won. However, their victory did not come before the U.S. government's export

restrictions had enabled a number of foreign-owned firms to gain a substantial competitive foothold in the international marketplace for strong encryption products.

The first steps toward commercialization of strong encryption were taken in the mid-1970s by groups of researchers working independently (though with some awareness of one another) at IBM, Stanford and MIT (Levy, 2001). These researchers shared a precocious appreciation for the importance of data security in the dawning age of digital communications, and they arrived at a common solution: cryptography. NSA's initial reaction was to try to block the publication of such schemes. Failing that, the agency struck a deal with IBM to develop a data encryption standard (DES) for commercial applications in return for full pre-publication review and the right to regulate the length, and therefore the strength, of the crypto algorithm. The academics at Stanford and MIT viewed this compromise with deep suspicion, however. This was the immediate post-Watergate era, a time of epic revelations about the cavalier treatment of civil liberties by CIA "spooks" and their counterparts at the NSA, and the young academics viewed DES as born in sin. Their key innovations were published in the late 1970s, even as the NSA attempted to block their dissemination and further research funding by the National Science Foundation (Diffie and Hellman, 1976; Merkle, 1978). By the end of the decade, the NSA had a new director, Admiral Bobby Ray Inman, who understood the new reality and adopted a new approach: export controls (Shapley, 1978; Levy, 2001). Forced by court decisions to respect the freedom of academics to conduct and publish research on cryptography, and hoping to benefit from the innovative work of the burgeoning community of crypto researchers outside the NSA, the government shifted toward controlling the commercial distribution of encryption products.

It was not clear at first how large the commercial demand for crypto would be, especially for small start-up companies, such as RSA Security, which was founded on the basis of the work done at MIT (Rivest, Shamir, and Adleman, 1978). During the early 1980s, academic interest in cryptography blossomed, and a large user-developer network of academics, math geeks and libertarian hackers began to trade ideas via the (pre-commercial) Internet, academic publications and an annual conference. It took the development of software applications for use by networked PC's to create a clear commercial need for strong encryption products. In 1983, Lotus Corporation needed a built-in encryption system for the first "groupware" product, Lotus Notes; the mechanism was necessary to ensure the confidentiality of the electronic messages that Lotus Notes' major corporate users would exchange by the thousands across computer networks (Levy, 2001). Over the next several years, such networking applications and the consequent commercial demand for encryption products exploded. Markets developed for products to preserve the secrecy of data against eavesdropping from outside and sabotage from within: authentication and digital signature software, antivirus software, data storage protection, firewalls, utility software, network software security products, and virtual private network access software (Giarratana, 2002).

Led by NSA, however, the U.S. government continued to insist on constraining the power of the encryption products that companies could sell to customers outside of the United States. Producers of encryption products, such as RSA, and their large,

multinational customers, protested vigorously, but the government held firm. Meanwhile, non-U.S. producers began to fill the gap. As U.S. export controls persisted through the end of the 1990s, foreign-based firms such as F-Secure (Finland), Checkpoint and Aladdin (Israel), and Trend Micro (Taiwan) gained significant market share at the expense of their American rivals, both abroad and in the United States (Giarratana, 2002).

Efforts to restrict the security provided by crypto products within the United States continued as well. January 1991 saw the introduction of a Senate bill that sought to guarantee government access to the plaintext content of any voice, data or other communications for purposes of national security and criminal investigation (Levy, 2001). This meant that manufacturers would have to equip their encryption products with "trapdoors" that would enable federal authorities to read the plaintext contents of encrypted texts – the very messages of users whose growing concerns about confidentiality had only recently created a massive commercial market for software products with built-in encryption, such as Lotus Notes. Alarmed by the potential clampdown, the developer of one such strong encryption product, PGP (for Pretty Good Privacy), took an unprecedented step: he distributed his crypto algorithm for free over the internet, which was by then in wide use by thousands of academics and on the verge of its volcanic eruption as a mass communications medium (Levy, 2001). Although PGP was carefully released only to Internet sites within the United States, its release on the Internet meant that it was instantly available worldwide, completely subverting the U.S. export laws. The milk was spilled, the water was under the bridge, and the genie was out of the bottle. Pick your favorite.

Significantly, the mass release of PGP subverted not only the U.S. export laws, but also the U.S. laws protecting intellectual property. The key feature of any encryption product is the crypto algorithm, the mathematical formula that is used to transform normal text (plaintext) into secret code, called cipher text. The cipher text can only be transformed back by a user in possession of the secret combination that "unlocks" the plaintext. This algorithm is the principal object of a company's patent. Companies differentiate their products with respect to the balance they strike between the length of the mathematical encryption algorithm (the longer it is, the stronger it is) and the amount of time it takes the software to perform the processes of encryption and decryption. When PGP was released over the Internet, it raised the hackles not only of the NSA, but also of private companies such as RSA Security that believed PGP was illegally based on its patented proprietary algorithms (Levy, 2001). The notion of "crypto anarchy," making strong encryption available instantaneously for free to potentially millions of users over the Internet, was dazzling to civil libertarians keen to preclude government snooping. To the government snoops, it was a boon to hackers, terrorists, international drug cartels, and child pornographers. And to the companies that depended on revenue from commercial sales of such products to stay in business, it seemed like the end of the world.

It was against this backdrop and commercialization of the Internet in the mid-1990s that commercial demand for strong encryption exploded and the NSA and the Clinton Administration attempted to broker a compromise. The so-called "Clipper Chip" would enable companies to build the strongest possible encryption protection into their products

both for domestic use and for export (Denning, 1993). But the products would have to include the Clipper Chip, which would make it possible for U.S. government agencies, with a proper court order, to decrypt any digitized text. The scheme was proposed in a variety of forms, to ensure skeptics, first, that no government agency would ever have access to the whole decryption algorithm, then that no government agency would have access, period (the "keys" would be held by a private entity) (Schneier and Banisar, 1997). But it was all to no avail. Not only civil libertarians, but more importantly, the computing, telecommunications and financial giants that were by then the world's largest users of strong encryption products, insisted that no U.S. customers and most certainly no foreign customers would ever trust a data security system equipped with a trapdoor that might allow the U.S. government to snoop (Gurak, 1997). Near the end of the century, it became increasingly clear that protection of computer-controlled critical infrastructures worldwide (privately-managed nuclear and other energy plants, water, sewage, and telecommunications facilities, etc.) now depended on private companies having access to the strongest available encryption (Levy, 2001). The military-security establishment retreated, the Clipper scheme was abandoned, and the export restrictions on strong encryption were mostly removed.

Thus in two prominent recent cases in which U.S. military-security agencies attempted to intervene in and guide the further commercial evolution of important advanced technology sectors, the impact of that intervention ended up being detrimental to the competitive position of U.S.-based firms. In both cases, the military sought to benefit from the expanded commercial development of the underlying technology, but only if the commercial industry agreed to provide it with the specialized versions of the products that the government said it needed for security purposes. In the case of flat panel displays, the detrimental effects were an indirect consequence of military involvement – direct Pentagon sponsorship of commercial technology development, no matter how critical to addressing military needs, invited political fights over foreign participation and industrial policy. As a result, though the result is contrary to what the designers of the Defense Department's flat panel display initiative desired, military involvement ended up distancing U.S.-based companies from the foreign partners they needed to credibly enter high volume FPD production. In the case of strong encryption, the NSA's efforts first to restrain and then to regulate the technology's commercial evolution served only to leave overseas markets open for foreign-based competitors, who established strong positions in those markets and had already leveraged them to enter U.S. markets successfully by the time U.S. producers were finally freed to sell their best products anywhere in the world.

5. Explaining Patterns of Dual Use Technology Development and Diffusion

As we have seen, a set of advanced technologies now recognized as key to domestic security in the post-9/11 era underwent simultaneous development and diffusion in the military and civilian sectors during the 1990s. Relying on commercial markets to spur innovation and lower costs, the military/security establishment adopted a 'dual-use' approach toward technology development as a centerpiece of its strategy for accessing state-of-the-art technology in the digital era. The approach recognizes the fact that military applications of new technology now 'spin on' from sophisticated civilian

applications as often (or more often) than military technologies 'spin off' in the opposite direction.

We have also seen that some high profile military-led efforts to manage dual-use technology development and diffusion in the 1990's produced highly unexpected results. One dual-use technology that the Pentagon sponsored solely for its own purposes, with no thought given to potential commercial use, (the Internet) has become one of the most widespread and rapidly adopted infrastructures for commerce and commercial communication in the history of the world. The dual-use technology whose diffusion the security agencies fought hardest and longest to constrain (strong encryption) is the dual-use technology that has nevertheless diffused the farthest and the fastest from its roots in the security sector. At the same time, a dual-use technology whose development and diffusion defense engineers in and out of the federal government promoted heavily (the computer-controlled sensor, surveillance and location-tracking technologies known in combination as intelligent transportation systems, ITS) diffused through the U.S. private sector only slowly and spottily. Another technology whose domestic development the Pentagon vigorously promoted (flat panel displays) continued to diffuse widely and rapidly in the commercial sector, but with little or no regard for the special needs of military users, and little or no manufacturing located in the United States.

What accounts for these surprising outcomes, and what can these cases teach about how military and law enforcement agencies should now think about promoting the development and diffusion of these and other dual-use technologies deemed critical to homeland defense? My argument is that the different outcomes stem directly from specific differences in the social organization of communication (exchange of information) between the developers of the technologies, their initial lead users, and subsequent potential users. These differences are amplified by the fact that dual-use technologies themselves, and essential information about them, more and more often come in a digital form that enables their extraordinarily rapid dissemination via the Internet. We have seen, specifically, how organized socio-technical networks[5], their ability to exchange information and technology greatly enhanced by the Internet, facilitated the widespread diffusion of (a) the Internet itself and (b) strong encryption software. The ease of information exchange spurred rapid learning and constant experimentation among developers and lead users; it prodded an already robust development process in new directions by forcing the development network to stay open to the demands of subsequent potential users. Their interests in different performance attributes of the same underlying technologies spurred further innovation and broader commercial acceptance.

In the Internet case, development was facilitated by the creation of a user-developer network that was allowed (with a wink and a nod) by the technology's original military sponsor (DARPA) to expand beyond the initial group of Pentagon-funded lead users. Subsequent attempts by the Internet's second military sponsor (DCA) to close the

[5] For more on the theoretical perspectives underlying the notion of "socio-technical networks," see Bijker, Pinch, and Hughes (1987); and Elzen, Enserink, and Smit (1996). Kulve and Smit (2002) employ this approach to analyze dual-use development of the bipolar lead-acid battery.

network to new users were defeated, in part by characteristics of the technology itself, but also by aspects of the culture and governance mechanisms of the social network that had by then evolved around it. In the case of encryption, the emergence of a robust civilian network outside the NSA that was devoted to refining and diffusing strong encryption trumped the domestic legal and technical barriers raised by intelligence officials and law enforcement about the security threats posed by the technology's widespread commercial availability. Because encryption products are digital in form and, again, because the internet is such an extraordinary medium for the mass distribution of digitized goods and services, the security establishment's efforts to restrict membership in the technology's user-developer network were unsuccessful.

By contrast, U.S. government-sponsored attempts to develop and diffuse intelligent transportation systems (ITS) and domestic production of flat panel displays were impeded by the stove-piped, hierarchical organization of the federal, state and local agencies, academic institutions and private entities involved in each effort. Without efficient and timely mechanisms for communicating user demands and design options across a variety of organizational boundaries, communications between technology developers and lead users were disjointed. As a consequence, in the case of ITS, technical characteristics originally inspired by military needs but inappropriate to civilian needs were retained long after they had clearly undermined civilian/commercial interest in developing alternative applications. The developer network did not expand sufficiently to include the putative lead users (state and local transportation agencies), or subsequent potential users (trucking companies, for example) despite the vigorous efforts of an active advocacy group, ITS America, to overcome the institutional barriers to a more networked form of organization. In the case of flat panel displays, political interests opposed to the Pentagon-sponsored effort created barriers to the expansion of the user-developer network. This excluded from the network foreign FPD producers who possessed critical expertise in state-of-the-art design and manufacturing techniques. Lead commercial users declined to participate in the new Pentagon-sponsored network lest they undermine the advantages they derived from the multinational network to which they already belonged.

6. The Right Strategy for Generating Advantage from Dual Use Technology in the Digital Age: Shield or Share?

History shows that military/security agencies can facilitate the successful commercialization of an emergent technology when the agencies encourage (or, at least, allow) the technology's socio-technical network to include user-developers not directly interested in exploring military-favored applications. This is true regardless of whether those favored applications are military-specific or dual-use in nature. If government R&D projects are the main source of funding for applied research in the field, and military influence effectively excludes user-developers interested in exploring the technology's other potential performance attributes, then the military's early involvement can impede successful commercialization. This was true in the 1950s and 1960s, and it continues to be true now.

If commercial development of the technology is already advanced, then military efforts to influence subsequent commercial development choices will have limited impact. Military/security agencies are now more likely to be technology borrowers than technology pioneers and, as highly specialized and small-scale customers in large consumer markets, their financial leverage over commercial producers is weak. Moreover, in a global economy in which the United States no longer dominates technological development in a number of relevant fields, policies aimed at restricting foreign participation in U.S. technology development or the diffusion of homegrown knowledge or products outside U.S. borders are counterproductive, if not doomed to fail outright. Most likely the countries the U.S. targets with controls will find alternative sources -- or simply develop the technologies themselves. The fact that many of these products (and much of the information about them) can be disseminated electronically means that their propagation over the Internet is exceptionally difficult to completely monitor and control. The surest way for the United States to influence the way the technology is used (and to find out who is using it) is to participate in its development by foreign-based scientists and manufacturers, as a sponsor of applied research projects that include them or as an active customer willing to pay them premium prices for producing specialized applications.

The substitution of an open, collaborative, networked approach to developing dual-use technology for a closed, "members only" approach places foreign nationals as well as commercial producers and research universities at the center of America's security apparatus. This obviously poses significant new security challenges. But for most technologies that can be constituted and disseminated electronically, the United States has little real choice. When a technology is already being developed commercially, military/security agencies cannot reign in all of the financial, expert, or jurisdictional resources necessary to its further development and diffusion. Their best strategy for achieving advantage in this circumstance is to enter partnerships with strategic allies, both foreign and domestic, to ensure enhanced *access* to information about new technology developments and the technical capabilities of adversaries, wherever they are located. To avoid politically motivated constraints, U.S. government agencies need not fund development activities by foreign scientists or foreign-based firms directly, but they must allow U.S.-based universities and firms that receive public funding to engage foreign partners.

Only when the potential diffusion of a technology poses a grave security risk *and* has a good chance of being successfully controlled – thus excluding most technologies that can be disseminated electronically – should security agencies attempt to use top secret classification and/or tight export controls (Berkowitz, 2001). This strategy is the surest approach they have for preserving secrecy via stringent *control* over information flows. In general, however, this approach is less and less viable in the digital age. It is also bad for innovation, so the work of such networks should not be based at research universities, where an open academic environment must be preserved, or corporate labs, where an open, collaborative learning environment is equally necessary for generating and testing out new ideas. Such work should be conducted at national laboratories and other

specialized, secure research facilities, and there should be a clear distinction drawn between classified and unclassified research.

In a global economy in the digital age, secrets about the development and use of dual-use technologies will be increasingly difficult or even impossible to keep. This includes secrets not only about technologies that can be disseminated easily over the Internet, but also secrets about any technology that is already available in the private sector, especially, perhaps, if it is already available outside the United States. This means that the strategic choices of military/security agencies for managing information about new technology have boiled down to two: (1) create cross-agency task forces and other boundary spanning organizations to overcome the balkanization of information in bureaucratic networks, and (2) establish partnerships with strategic allies to gain access to technological information generated or discovered by commercial producers (foreign and domestic), foreign researchers, and the governments that sponsor them. The best dual-use technology policy for the digital era, that is, the best technology policy for decision makers who want simultaneously to achieve both commercial and security advantage for the United States, is a policy that enables U.S. companies and the U.S. government to fully understand what foreign companies and governments are learning via their own efforts at technology development, marketing and use. The best way to ensure that the information flows is to let it flow both ways, to encourage American scientists and American companies to engage in the activities of research, development and deployment right alongside their foreign colleagues, both abroad and at home.

References

Abbate, J., 1999. Inventing the Internet. MIT Press, Cambridge, MA.

Air Force Systems Command., 1980. Statement on Defense Industrial Base Issues (General Alton Slay), November 21, 1980, Department of Defense, Washington, D.C.

Alic, J., Branscomb, L., Brooks, H., Epstein, G., Carter, A., 1992. Harvard Business School Press, Cambridge, MA.

Alvarez, L., Horowitz, R., 1997. Safe Platooning in Automated Highway Systems. Institute of Transportation Studies Partners for Advanced Transit and Highways (PATH), University of California, Berkeley.

Berkowitz, B., 2001. Keeping secrets in the digital age. The Hoover Digest, No. 2. The Hoover Institution. Stanford University, Stanford, CA.

Bijker, W., Pinch, T., Hughes, T., (Eds.), 1987. The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology. MIT Press, Cambridge, MA.

Borrus, M., Hart, J., 1992. Display's the thing: The real stakes in the conflict over high resolution displays. Berkeley Roundtable on the International Economy Working Paper #52. University of California, Berkeley.

Borrus, M., 1988. Competing for Control: America's Stake in Microelectronics. Ballinger, Cambridge, MA.

Borrus, M., Millstein, J., Zysman, J., 1983. US-Japanese Competition in the Semiconductor Industry. Policy Papers in International Affairs #17. Institute of International Studies, University of California, Berkeley.

Brand, S., 2001. Founding father: An interview with Paul Baran. Wired Magazine, March 2001.

Braun, E., MacDonald, S., 1978. Revolution in Miniature: The History and Impact of Semiconductor Electronics. Cambridge University Press, London.

Bruekner, L., Borrus, M., 1984. Assessing the commercial impact of the very high speed integrated circuit program. Berkeley Roundtable on the International Economy Working Paper #5. University of California, Berkeley.

Collis, D., 1988. The machine tool industry and industrial policy, 1955-82, In: Spence, M., Hazard, H. (Eds.), International Competitiveness, Ballinger, Cambridge, MA.
Cowan, R., Foray, D., 1995. Quandaries in the economics of dual technologies and spillovers from military to civilian research and development. Research Policy 24, 851-868.

Defense Science Board Task Force, 1980. Report on industrial competititiveness, Richard Furhrman, chairman, November 21, 1980, Department of Defense, Washington, D.C.

DeLauer, R., 1984. Technology development and transfer, In: Kuhn, R.L. (Ed.), Commercializing Defense Related Technology. Praeger, New York, NY.

Denning, D., 1993. The Clipper Encryption System. American Scientist 81, July-August.

Diffie, W., Hellman, M.,1976. New Directions in Cryptography. IEEE Transactions in Information Theory, IT-24(6), November.

DiFilippo, A., 1986. Military Spending and Industrial Decline: A Study of the American Machine Tool Industry. Greenwood Press, Westport, CT.

Elzen, B., Enserink, B., Smit, W.A., 1996. Socio-technical networks: how a technology studies approach may help to solve problems related to technical change. Social Studies of Science 26 (1), 95-141.

Flamm, K., 1988. Creating the Computer: Government, Industry and High Technology. The Brookings Institution, Washington, D.C.

Fong, G., 1986. The potential for industrial policy: lessons from the very high speed integrated circuit program, Journal of Public Policy and Management 5(2).

Gansler, J., 1980. The Defense Industry. MIT Press, Cambridge, MA.

Gansler, J., 1989. Affording Defense. MIT Press, Cambridge, MA.

Giarratana, M., 2002. Entry, survival and growth in a new market: The case of the encryption software industry. LEM Papers Series, Laboratory of Economics and Management, Sant'Anna School of Advanced Studies, Pisa, Italy.

Gurak, L., 1997. Persuasion and Privacy in Cyberspace: The Online Protests over Lotus MarketPlace and the Clipper Chip. Yale University Press, New Haven, CT. and London.
Hooks, G., 1991. Forging the Military-Industrial Complex: World War II's Battle of the Potomac. University of Illinois Press.

Hsu, A., 1991. The design of platoon maneuvers for IVHS. Proceedings of Annual Control Conference, Boston, MA.

Kaldor, M., 1981. The Baroque Arsenal. Hill and Wang, New York, NY.

Kenney, M., 2001. The growth and development of the Internet in the United States. Berkeley Roundtable on the International Economy Working Paper #145, University of California, Berkeley.

Klein, H., 1996a. PhD dissertation. Department of Political Science. Massachusetts Institute of Technology.

Klein, H., 1996b. Operation Timesaver: a political and institutional analysis. In: Proceedings of the ITS World Congress, ITS America, Washington, D.C.

Klein, H., 2001. Technology push-over: defense downturns and civilian technology policy, Research Policy 30, 937-951.

Kulve, H., Smit, W.A., 2002. Civilian-military co-operation strategies in developing new technologies. Research Policy (in press).

Levy, S., 2001. Crypto: How the code rebels beat the government – saving privacy in the digital age. Viking Penguin Books, New York, NY.

Lichtenberg, F., 1989. The impact of the strategic defense initiative on US civilian R&D investment and industrial competitiveness. Social Studies of Science, 19.

Markusen, A., Yudken, J., 1992. Dismantling the Cold War Economy. Basic Books, New York, NY.

Merkle, R., 1978. Secure communications under insecure channels. Communications of the ACM 21(4).

Misa, T., 1985. Military needs, commercial realities, and the development of the transistor, 1948-1958, In: Smith, M.R., (Ed.), Military Enterprise and Technological Change: Perspectives on the American Experience. MIT Press, Cambridge, MA, 253-287.

Molas-Gallart, J., 1997. Which way to go? Defence technology and the diversity of dual-use technology transfer. Research Policy 26, 267-385.

Mowery, D., Rosenberg, N., 1991. Technology and the Pursuit of Economic Growth. Cambridge University Press, New York, NY.

Mowery, D., Simcoe, T., 2002. Is the internet a US invention? Research Policy 31, 1369-1387.

Murtha, T., Lenway, S., Hart, J., 2001. Managing New Industry Creation: Global Knowledge Formation and Entrepreneurship in High Technology. Stanford University Press, Stanford, CA.

Murtha, T., Spencer, J., Lenway, S., 1996. Moving targets: National industrial strategies and embedded innovation in the global flat panel display industry, In: Advances in Strategic Management 13, 247-281.

Noble, D., 1984. Forces of Production: A Social History of Industrial Automation. Oxford University Press, New York, NY.

Pollack, A., 1989. Pentagon sought smart truck but it found something else, New York Times, May 30, 1989, p. 1.

Reppy, J., 1999. Dual-use technology: Back to the future?, In: Markusen, A., Costigan, S. (Eds.) Arming the Future: A Defense Industry for the 21st Century, Council on Foreign Relations Press, New York, NY, pp. 269-284.

Rivest, R., Shamir, A., Adleman, L., 1978. A method for obtaining digital signatures and public key cryptosystems. Communications of the ACM (21) 2, February, 120-26.

Schneier, B., Banisar, D., 1997. The Electronic Privacy Papers: Documents on the Battle for Privacy in the Age of Surveillance. John Wiley and Sons, New York, NY.

Shapley, D.,1978. Intelligence agency chief seeks 'dialogue' with academics. Science 202, October, 407-9.

Steinmueller, E., 1986. Industry structure and government policies in the US and Japanese integrated circuit industries, CEPR Discussion Paper, Stanford University, Stanford, CA.

Stowsky, J., 1986a. Beating our plowshares into double-edge swords. Berkeley Roundtable on the International Economy, Working Paper #17, University of California, Berkeley.

Stowsky, J., 1986b. Competing with the Pentagon: The Future of High-Tech R&D. World Policy Journal III (4), Fall 1986, 697-721.

Stowsky, J., 1992. From Spin-Off to Spin-On: Redefining the Military's Role in American Technology Development, In: Sandholz, W., Borrus, M., Zysman, J., Conca, K., Stowsky, J., Vogel, S., Weber, S., The Highest Stakes: The Economic Foundations of the Next Security System, Oxford University Press, New York, NY, pp. pp. 114-140.

Stowsky, J., 1996. America's Technical Fix: The Pentagon's Dual-Use Strategy, TRP, and the Political Economy of U.S. Technology Policy in the Clinton Era. Berkeley Roundtable on the International Economy (BRIE), University of California, Berkeley.

Stowsky, J, 1999. The History and Politics of the Pentagon's Dual-Use Strategy, In: Markusen, A., Costigan, S. (Ed.) Arming the Future: A Defense Industry for the 21st Century, Council on Foreign Relations Press, New York, NY, pp. 106-157.

National Academy of Sciences,1982. Committee on Assessment of the Very High Speed Integrated Circuit Program, An assessment of the Department of Defense very high speed integrated circuit program. National Academy Press, 1982.

Tilton, J. 1971. International Diffusion of Technology: The Case of Semiconductors. The Brookings Institution, Washington, D.C.

Tirman, J. (Ed.), 1984. The Militarization of High Technology. Ballinger, Cambridge, MA.

US Congress, House Armed Services Committee Industrial Base Panel Report, 1980. The ailing defense industrial base: unready for crisis. (Richard Ichord, chairman). December 31, 1980. Washington, D.C.

US Department of Defense, 1995. Dual-Use Technology: A Defense Strategy for Affordable, Leading-Edge Technology, Department of Defense, Washington, D.C.

US Department of Defense, Office of the Undersecretary for Acquisition, 1987. Defense Semiconductor Dependency, Department of Defense, Washington, D.C.

Utterback, J., Murray, A., 1977. The influence of defense procurement on the development of the civilian electronics industry. MIT Center for Policy Alternatives, Cambridge, MA.

Weber, S. 2000. The Political Economy of Open Source Software. Berkeley Roundtable on the International Economy Working Paper #140, University of California, Berkeley.

Wilshire, R., 1990. Intelligent Vehicle/Highway Systems – a feeling of déjà vu, ITS Journal, November, 39-41.

Yoshino, M, Fong, G., 1986. The very high speed integrated circuit program: lesson for industrial policy, In: Scott, B, Lodge, G., (Eds.), US Competitiveness in the World Economy. Harvard Business School Press, Boston, CA.

Zakon, R.H., 2001. Hobbe's Internet Timeline.
http://www.zakon.org/robert/internet/timeline