Computer Technology and National Security

“Advantages will go to states that have a strong commercial technology sector and develop effective ways to link these capabilities to their national defense industrial base.”

—Central Intelligence Agency, “Global Trends 2015”

The centerpiece of the revolution in military affairs is the shift from weapon-centric warfare to network-centric warfare. Many efforts are under way to incorporate information technologies into military operations. Future military operations will involve extensive networks of sensors, databases, command, control, and analytical capabilities that provide information directly to the warfighter and to smart weaponry on an immediate, real-time basis. Computing and network innovations will allow for seamless, real-time connections between troops, sensors, command, platform, and weapon. Data from sensor platforms such as remote sensing satellites or unmanned aerial vehicles, automatically processed and referenced against existing databases located hundreds or thousands of miles away, could be communicated directly to soldiers, platforms, and intelligent weapons. The physical dispersal of forces need not degrade command and control, and maneuver and targeting capabilities can be enhanced and accelerated.

The more flexible and precise military force that the United States could develop using information technology would have an advantage in the new international security environment. The more flexible and precise military force that the United States could develop using information technology would have an advantage in the new international security environment. Maintaining U.S. superiority requires taking a number of steps: forming partnerships with the information technology industry and academic community; creating a process to increase the flow of innovation and to change doctrine and practices accordingly; and building a strong foundation of education and research to ensure that U.S. technology is as advanced in 10 years as it is today.

Partnership with the private sector is a “new” tool for governance that the United States has already begun to use in areas like encryption policy and critical infrastructure protection to address national security problems where the private sector has an equal role to play. Vehicles for partnership include new, focused advisory groups, task forces, and exchange programs for DOD personnel at information technology companies, internships, and the establishment of joint research programs. The broad objective should be to create connections between the government and the private sector that match warfighters’ needs and private sector innovations. Ideally, DOD warfighters and private sector technical personnel

Creation of a joint evaluation center, staffed with both government and industry
detailees to look at technologies and applications either in development or planned
for development, would help the United States better understand, and adjust to,
the new global technological environment. As a related measure, the United States
might want to expand existing programs at the National Defense University (NDU)
and other military education facilities. Existing efforts at NDU and the War
Colleges could be reinforced by additional programs and faculty staffed by
technologists from the information technologies industries. The United States may
also want to integrate private sector information technology expertise directly into
facilities like the Army’s National Training Center for the development of new
doctrine and tactics. Private sector experience may not translate directly to the
military and government, but the experience of applying new information
technologies to global companies and the effects this had on organizations could be
valuable for guiding changes in the national security community.

New technologies are not a panacea—they must be accompanied by doctrinal and
organizational changes to reap their full benefit. The French had better, and more,
tanks in 1940 than did the Germans, but the Germans used their tanks in new
ways. The United States, given the strength of its industry, will have greater
opportunities than its potential opponents to gain the advantage if it can find ways
to use these technologies to transform processes rather than merely injecting them
into existing processes. The most immediate example of this would be logistics and
acquisitions reform at the Department of Defense. The private sector has made
advances in improving supply chain management and acquisitions that the national
security community could mirror. Using B2B (business-to-business) models would
streamline acquisitions activities.

The creation of a business-to-business portal by General Motors Corporation,
Ford Motor Company, and DaimlerChrysler is a useful model for DOD. This
experience of large competitive bureaucracies working together could map well to
DOD and the armed services. The three companies formed a business-to-business
integrated supplier exchange through a single global portal. It is an online global
network that provides for catalog purchasing, bidding and price quotes, online
sourcing, and auctions. In addition, it provides supply chain management functions
such as capacity planning, demand forecasting, production planning, transaction
automation, financial services, payment, and logistics. The companies were able to
set up this supply chain network quickly and without putting sensitive information at
an unacceptable risk.

Improved logistics and acquisitions processes will help address the problem of
DOD’s information technology often lagging behind the private sector in

From Computer Exports and National Security in a Global Era - New
Adopting business-to-business practices could allow the DoD to have a faster “refresh rate” for IT, thus allowing them to keep pace with the private sector.

Current acquisition regulations may be the biggest obstacle to greater use of information technologies.

信息技术。使用旧技术可能很昂贵，因为模型会过时，备件和维护成本会增加。采用B2B（企业对企业）的做法可以让DOD和武装部队拥有更快的“更新率”来获取信息技术。解决这个问题将需要改变资金和采购实践，但它也将要求使用DOD采用的开放系统和标准以及“即插即用”技术，以允许更轻松地升级系统。

合作伙伴与私营部门的合作可以增加创新对国家安全社区的流入。这需要改变采购实践和将采购权交还给“客户”而不是某些中介或复杂、分层的审查过程。现有的采购实践对创新性信息产业公司是一个阻碍。虽然国防承包商已经掌握了复杂的国防采购系统，但信息企业，其主要市场是全球和民用，可能会发现与DOD在特定应用上合作的机会成本太高。领先的创新者不是国防承包商，他们不愿意承受学习如何向DOD销售的成本；他们可以赚得和销售到商业市场一样多甚至更多的钱。采购规定可能是信息技术更大规模使用的最大障碍。国会和政府需要改变采购过程，使美国能够充分利用其在商业技术方面的领先地位。

一些国家安全社区（全球运作与物流、采购、采购、数据挖掘）感兴趣的问题已经经历了几个迭代，在私营部门。美国可以利用这些经验。DOD和私营部门可以探讨这些商业创新，以实现国家安全利益。作为将这些概念转化为实用工具的第一步，DOD或DARPA可能希望开始四到五个快速通道项目，与领先的信息技术公司合作开发新的应用。可能的快速通道项目领域包括：

——无线宽带应用。军事很可能成为最热衷于无线宽带应用的消费者。这些应用可以帮助解决“最后一英里”问题，大大扩展数据和通信网络。一个商业模型，例如，使用低地球轨道卫星网络来提供数据传输速率高达每秒200千字节。全球宽带系统（GBS）及其前身联合宽带系统提供了一种集成新技术的现有平台。其他在开发中的商业产品（如使用蓝牙或其他短距离、安全无线标准的产品）也可应用于军事应用。

——普适计算/嵌入智能。便宜、强大的CPU和...

从《计算机出口与国家安全在全球化时代 - 新工具为新千禧年》CSIS专家小组报告，2001年6月。
specially designed operating systems and applications can be incorporated into ships, aircraft, vehicles, and facilities, creating dense networks of “intelligent” devices. These devices could automate functions and provide a more detailed and complete situational awareness. Managing the floods of data generated by these dense networks of intelligent devices will itself have to be automated, using software agents, data mining, and other applications. Pervasive computing and network technologies would enhance redundancy and improve communications across commands, and artificial intelligence functions could improve computerized pattern recognition to allow automated rules of engagement, rapid assignment of weapons to hundreds of targets, and some automated maneuver and logistics functions.

—**Software agents, or “bots.”** Bots are software tools for retrieving and managing information from remote sites on the network. Defense has a number of projects already under way to exploit software agents. These tools can perform statistical analysis, resource discovery, network maintenance, and updating and can provide “mirroring” of information. More sophisticated bots can be self-configuring and can make decisions on how to refine searches based on their own search experience.\(^1\)

—**Data mining.** Database applications that automatically search for new patterns or new relationships in a large amount of data offer possibilities for improved intelligence functions, maintenance, personnel, and other activities. Combined with software agents, data mining would enhance and accelerate the tasking, processing, evaluation, and dissemination (TPEDS) process used in the intelligence community.

—**Collaborative virtual workspace.** Group-to-group communications networks can bring people together in real time, regardless of their physical location, for large-scale distributed meetings, collaborative work sessions, and training, using large-format displays and “intelligent” meeting rooms.

**Education, Research and Development**

Enhancing national security with new information technology also requires addressing fundamental problems in education and long-term research and development. The United States faces a shortage of skilled workers in the information technology sector. This shortage has worsened in recent years, particularly in the government, where organization and pay scales put it at a disadvantage in competing for skilled information technology personnel. The general shortage means that information technology workers are expensive, making it difficult to staff positions at government salaries—particularly at entry levels. The private sector can overcome this shortfall by recruiting skilled labor from foreign countries, but this does not work for national security applications. The United

States needs to find the incentives and develop the programs that will produce an adequate supply of information technologists. One solution is to adopt a scholarship model where the United States would pay for higher education in exchange for a commitment to service for a number of years, as is already done with other short-supply skills such as medical care.

Maintaining U.S. superiority also requires addressing the long-term problem of funding research and development. The United States needs to ensure that the pipeline of innovation does not run dry, as that would eliminate an important element of U.S. superiority. This expansion should apply to research both in specific information technologies and in the basic research that underpins developments in information technologies. Basic research funded by DARPA and others in the 1970s and 1980s underlies much of the progress made in information technology in the past two decades. This kind of long-term investment must be repeated to maintain U.S. superiority.

Attention to the fundamentals (education and research and development) is essential for the United States to protect its national security in the face of challenges from potential opponents. Other nations are deeply interested in the use of information technologies to gain “asymmetric” advantage over the United States. Export controls do nothing to help manage this risk, as they cannot catch the technologies involved. An increased pace for innovation by the United States, however, will make it harder for potential opponents to benefit from asymmetric approaches. Although the United States is perhaps the nation most vulnerable to cyberattack, it is also the best positioned (given the size of its industry and its defense establishment) to exploit new technologies to its advantage, including in information warfare.

Potential opponents will also face a more difficult task if the United States pays sufficient attention to information security. To some extent, this is a question of making strong, well-designed interoperable encryption an integral part of national security applications. Progress is also necessary in critical infrastructure protection and information assurance efforts. Some efforts are already underway at Defense, such as DOD’s Public Key Infrastructure (PKI) for its own network. The United States has made progress in protecting its critical infrastructures, but the task is not complete. Information technologies can strengthen U.S. military forces’ ability to operate in physical dimensions, but the United States also needs to ensure that U.S. cyberspace capabilities match the deterrent and defensive capabilities of U.S. strategic and conventional forces.

As part of this, the United States also needs to expand its ability to assess what other nations’ forces can do with commercial technology and widely available military technology. It could perhaps use joint military/private sector evaluation.

centers and industry partnerships to counter attempts to gain asymmetric advantage by developing DOD programs and initiatives.

Developing and strengthening partnership with the information technology sector requires finding new vehicles that differ from the traditional relationship with a “contractor” and to make the changes in organizational structures and procedures that would allow and accelerate these partnerships. These partnerships are central, as the bulk of innovation and development of applications and networking technologies is taking place in the private sector. There is a precedent for this—the resolution of the debate over encryption is one such model. It will not be possible to turn information technology companies into defense contractors (and it is not in the national interest to do so), but there are ways to build cooperative relationships that provide benefits to both.
Notes

1 There is abundant literature in military periodicals on this point. A recent recommendation would be, for example, the 2000 Report of the Independent Commission on the National Imagery and Mapping Agency (“The Information Edge: Imagery Intelligence and Geospatial Information in an Evolving National Environment,” December 2000) which says: “NIMA should aggressively explore ways to realize the large potential for improving effectiveness through ‘force multiplier’ opportunity in automated extraction tools or both geospatial and image analysis.”