

DNI-PRIVATE SECTOR WORKSHOP ON EMERGING TECHNOLOGIES THAT COULD CHANGE THE WORLD¹

*Carnegie Endowment for International Peace
1779 Massachusetts Avenue, N.W.
Washington, D.C.*

December 7, 2006

SUMMARY

This conference brought together leading technology experts in academia, the business community, and the US intelligence community to assess emerging technologies in the areas of advanced power sources, biometrics, computing and biomedical technology. Industry has a different vantage point and a different method of dealing with security issues, and has a different understanding about what national security issues are. The question remains is what is in the future? What emerging technologies are available that government should be worried about, investigating, or developing? What are the breakthrough technologies that industry is working on, or that might “rock the boat” if developed elsewhere? The global economy now utilizes talent in countries where regulatory and legislative disincentives are far less burdensome than in the U.S. High R&D costs and few incentives to innovate have driven most U.S. companies out of long term R&D. There are not enough engineers and scientists being trained who are U.S. citizens with limited foreign contacts (for clearances). Furthermore, the U.S. is falling behind China, India, and other countries in the training of engineers and scientist.

* * *

¹ This paper provides a summary of some of the key points raised in this Workshop on emerging technologies, which was held at the Carnegie Endowment for International Peace on December 7, 2006. The Workshop was sponsored jointly by the Center for Strategic and International Studies, the US Chamber of Commerce, the Business Roundtable, the Intelligence and National Security Alliance, the Office of the Director of National Intelligence, and the US Department of State’s Bureau of Intelligence and Research. It was organized to solicit the views of non-governmental specialists and to facilitate the exchange of views between the outside specialists and government officials. The workshop was conducted on an unclassified, off the record, and not for attribution basis. The views expressed in the discussions and in this summary are solely those of individual experts who attended the event and do not necessarily reflect the analysis, views, or opinions of any company, consortium, or US Government agency.

Thinking imaginatively beyond the horizon

Cultural boundaries of all kinds are diminishing—such as legal, private/public, financial, state/non-state, and cyber. Boundaries “across the board” are eroding because of the vast nature of available information. This poses potential problems from a national security perspective. What is considered ‘secret’ is eroding. The erosion of state/non-state boundaries has opened a vast array of potential targets that are not controlled by the government (such as power systems, financial centers, etc.). Ownership becomes less relevant, while all systems can become targets.

The world is accelerating—increase in product cycles, speed of piracy, and speed of fashion, for example. Companies must be faster to market to make a profit, but they can often be overtaken by pirates with small R&D budgets and little or no overhead costs. In the current world, “all intelligence advantage is transient.” In the confrontation between security and robustness with seamless convenience, convenience wins every time.

Identifying disruptive technologies is imperative. Pearl Harbor, for example, was the quintessential intelligence failure. The US “knew” ships were safe because torpedoes worked in deep water. Shallow water torpedoes did not exist in the “Intelligence” community, thus US ships were perceived as safe in shallow ports. All the while, Japan had developed shallow water torpedoes (and other concepts that could be used e.g., kamikaze). The US intelligence community and the private sector must think imaginatively -- “beyond the horizon”.

New Strategies for the ODNI/S&T

There are three main events that changed the nature of intelligence:

- *Collapse of the USSR.* With the collapse of the USSR, the predator-prey relationship ended.
- *September 11th.* The significant “show of force” or, at the least, show of planning capability by hostile non-state actors signaled a change in the nature of intelligence gathering and potential threat assessment.
- *Advances in technology:* Israel found laptops in Hezbollah tunnels networked together with night vision, forming a system of systems network to allow better targeting for mortar fire. These system-of-systems concepts were previously thought to be beyond non-state entities’ capabilities. This has signaled a shift in the nature of intelligence.

Technology globally is improving exponentially and terrorists are taking advantage of these advances. The US is more comfortable with its legacy systems developed decades ago, making only incremental changes to these existing systems rather than developing new (and cheap) ideas, concepts, and systems. However, the US has made

rapid deliveries in the past (with fast designs, developments, and implementations), such as the U-2.

The new strategy for the ODNI/S&T is speed, surprise, and synergy to outmaneuver the “exponential curve”. Several examples in implementing this strategy include:

- Speed
 - o Rapid Technology Transition Initiative (RTTI)
 - o Intelligence Community Rapid Prototyping Facility
 - o Find or create pockets of “early adopters”, such as Open Source Works
- Surprise
 - o Intelligence Advanced Research Projects Agency (IARPA), to capitalize on the successful DARPA model
 - o Sheppard disruptive or revolutionary projects, for example the Advanced Remote Ground Unattended Sensor (ARGUS)
- Synergy
 - o Link S&T leadership, such as through the National Intelligence S&T Committee
 - o Reward technologists with programs like Fellows, Ambassadors, Expo, and ADNI/S&T Awards
 - o Joint projects that solve mission problems with cross agency teams
 - o Create new opportunities for informal social networks
 - o Intelligence Community S&T Investment Plan
 - o Outreach through the Intelligence Science Board, National Technology Alliance, and In-Q-Tel

Advanced Power Sources (*break out session*)

In the past, the Intelligence Community (IC) had the knowledge, resources and capabilities in knowing what the emerging technologies were. Today, however, the IC is relying more heavily on the private sector. Industry and DNI should lobby with one voice to fix:

- *Excessive policy regulation.* The global economy now utilizes talent in countries where the regulatory and legislative limiters are far less burdensome than the US, requiring the IC to ask what new technologies will change the world. The DNI and its industry partners should lobby (with one voice) to change the policies that create this conundrum – the high labor costs, no tax incentive for R&D efforts, low incentives to acquire technical advanced degrees, excessive acquisition regulations, and Sarbanes Oxley burdens. With a comprehensive policy reform comes a return to the appropriate levels of investment in fundamental sciences from both industry and government, and in turn US technical leadership.

- *High research and development costs and low incentives to innovation.* The US competitive environment (shareholders short term vision) has driven most companies out of long term R&D. It used to be that 100+ person teams at large firms (Xerox and Bell, for example) could apply their technical expertise to important technical problems. This is not possible with the current short-term dollar driven paradigm (and part of this is an outgrowth of the breakup of relative monopolies).
- *Brain drain.* There are not enough engineers and scientists being trained who are American citizens, with limited foreign contact (to enable clearances, for example). The US is falling behind China, India, and other countries in the training of engineers and scientists. In fact, US institutions continue to train foreign students who return home with the education and insight into current emerging American technologies. Furthermore, there is concern about maintaining the ability to train in these fields. If not enough technical people are trained here, the institutions providing leadership in the training will lose their capability.

Advanced Biometrics (break out session)

There will continue to be improvements in sensors, algorithms, and networks, as well as improved processes and hardware. Assured technology advances will be in rapid face, finger, and iris identification. Some issues will remain—deception detection and virtual agents and their ability to use increasing sophistication. Deception detectors may have a downside, potentially hindering business relationships for example. As with many technologies, there is a positive impact with Biometrics, such as a potential for increased security, conversely, there are negative impacts, such as developing a false sense of security.

For the DNI and security-minded companies:

- Data integrity must be enhanced and secured with biometric capability, to determine hostile people approaching key infrastructures. It could also be used to detect and track people, such as a lost child. Security sensors can determine their location based on biometric identification.
- Security, insurance, benefits of personal security, medical operations will be drivers for improvements in biometrics.
- For the intelligence service, when performing clandestine operations, biometric sensing capabilities will increasingly complicate those operations.

Advanced Computing (break out session)

Participants in this break out session highlighted four key issues of concern in advanced computing:

- More data will be created faster, and will outdo our ability to create computational systems to deal with it. Organizations may have fewer secrets and release more information.
- The United States' ability to stay competitive in a virtual world.
- Sudden erosion of brands. For example, a company's stock drops because it can not control rumors on the Internet.
- How do companies protect what makes them unique and gives them a strategic advantage?

Advanced Biomedical Technology (break out session)

Participants in this break out session highlighted the concern that any information can be used against us, raising the question, how can we detect and prevent this and stay ahead? We must stay at the cutting edge of technological development. The prospect of advanced technology online available to everyone is of concern. The US thrives on freely available information. However, we need to learn how to control and learn how to prevent others from taking that information without affecting our research and development process.

Biotechnology advances will dominate the 21st century. DNA analysis machines will certainly accelerate our understanding of genetics and profiling, and this will help track disease movements in populations. Genetic identification and biosensors can identify biotechnology threats, and enable us to monitor health. A single lab will be able to sequence 10x10 bases in a day on genomes, which will revolutionize what we know on genome technology.

There will be nefarious applications in biological development. The availability of synthesizers on the market, like eBay, is disturbing. These technologies are widely available, which raises concerns about biological terrorism. These technologies are developed in many places, so it poses a challenge for protecting microbiology—and what the protocol might be for monitoring the process and security. Although it is not routine now, certainly it will be easily accessible in 10-15 years.

We are one year away from having the first synthetic bacterium, and five to seven years away from having reverse-engineered synthetic bacteria, such as anthrax. The unintended consequences and implications of research are a serious issue. Laboratory accidents can be honest mistakes, or it can be total negligence or deliberate creation to do harm.

All biotechnology is dual-use -- it can be used for good, or it can facilitate harm for unsophisticated use. This all exists in open literature. As a community, there is no one

biotechnology use articulated that can be used for nefarious purposes. The psychological use of biotechnology will have much to do with this.

The complicating factor for the Intelligence Community in the use of biotechnology for stealthy malevolent use is that it could look like Mother Nature if the person or group does not claim credit for it. Probably 10-20 years from now, we will have the capability to genotype the type of warfare to be racist; the tools will be available to create an ethnic conflict. Motivation and satisfaction from bioterrorism may be the same as from a nuclear attack.

Workshop Closing Discussion

Technical intelligence has always been perceived to be linked with satellites. Now they are taking more time to build, and are costly. This is all occurring when targets are shifting, particularly with the current focus on terrorism. S&T is not a large unwieldy contraption, it is possible for technologies to be developed fast without much money. However, technology is diffusing around the world, the world has changed and we must adapt to these changes.

How can we be confident that there is an emerging technology out there that we have not discovered? We are reasonably confident now, but trends work against us, and there will be tensions in the future. In terms of military technology, the US is very comfortable and has good visibility, but the speed in the transition of emerging technologies is alarming.

Globalization and control

With globalization we are facing computational issues and reduced bandwidth, a ubiquitous virtual presence, and migration patterns such as labor movements around the planet which can disrupt social patterns worldwide.

Because of globalization and the IT boom, US comparative advantage is no longer assured. Whoever is capable of bringing technology to the market fastest (especially India and China) will have the advantage. The US is eroding in technical educational advantage, advantage in IT infrastructure, and government receptiveness to business is degrading. Furthermore, military power is affected by speed of acquisitions. Can we afford to get the best weapon systems?

China, India, Korea, and Japan are very industrious and have a culture that promotes growth. They are leading the world in automobile transportation, wireless, and robotics. There are also significant amounts of technical expertise in Russia.

Technology is being outsourced and new ideas are often emerging abroad. We must work on our partnership between private industry and government instead of just business. We need longer-term relationships in the future.

We need to look at how we use technology. Social factors, especially abroad, should be considered as well. We need to be innovative and look at older technologies in new ways and with a different perspective. We also need to work on education, understanding basic physics, biology, and chemistry.

The reach of the Internet is ubiquitous. People are less likely to be disenchanting with the world if they have access to the web. On the other hand, disinformation exists out there. Al Qaeda, for example, can organize mass campaigns online. How do we quantify and correlate data and determine if it is correct or not? How can you determine what information is right or wrong? In the future, people tag a website if they feel it is correct. There is a spectrum of credibility on the Internet; people will use sites they think work. Google Scholar is at the cutting edge, whereas blogs can be very unreliable.

The Workshop participants identified three critical issues:

- *The energy environment.* The growth of industrialization around the world, especially in Asia sops up energy and resources. China alone will double and triple its burden on the environment; same with India. The US is not addressing this, this is a good opportunity for the US to lead the world.
- *Theme of IT, innovation, and intelligence.* This is the basis for how we obtain knowledge and S&T. This is a healthy cycle and it will accelerate over the next few years. Forecasting emerging technologies is something we could do better.
- *How social institutions work.* Government, health and academic institutions are falling behind. Because of excessive centralization, institutions create barriers, which can slow business. Groups like Al Qaeda do not face these same barriers. Furthermore, people used to share ideas freely but now, academics sell their ideas. This lack of sharing is disappointing. It is not because they are worried about national security, but rather making a profit.

March 6, 2007