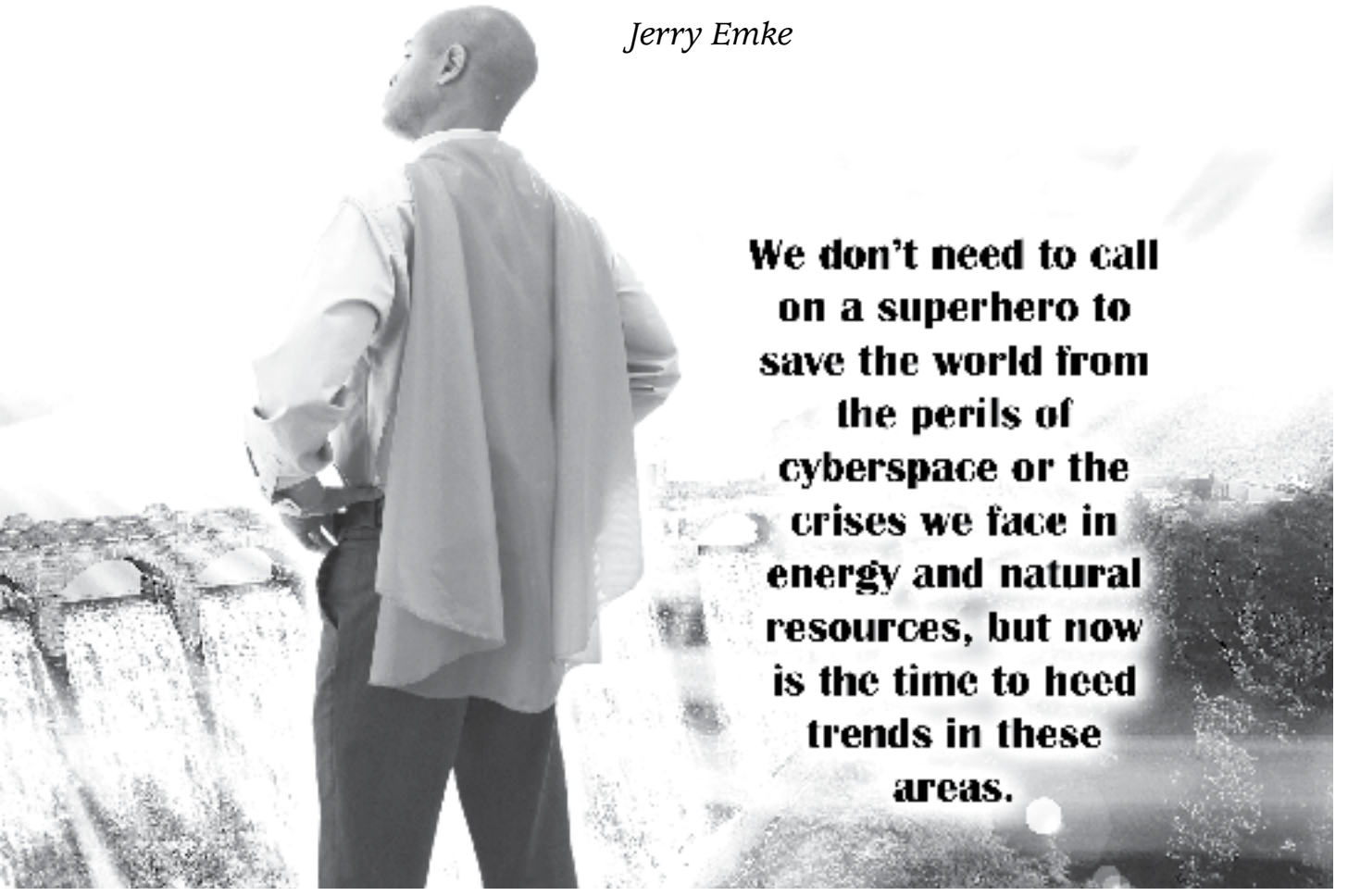
# Trends and Shocks, and the Impact to the Acquisition Community

*Jerry Emke*




Trends and shocks that will impact the future of business in the global community are receiving a great deal of attention in business, government, and defense planning circles. I participated in trends and shocks discussions at three meetings on Department of Defense transformation, and this spurred me to research the subject further and consider what impact probable future effects will have on the acquisition community.

Consider a trend to be a prevailing direction and a shock to be an event affecting people much like the first jolt of an earthquake. In these cases, hindsight is far better than foresight. When, after the fact, you examine why a shock occurred, the long-term trend that resulted in the shock is readily apparent. Strategists perform research on trends and shocks so the acquisition community can shape plans to keep us from being surprised in the future.

History is replete with examples of how key events have been shaped by surprise—a lack of contingencies, random chance, and unexpected events are some examples. Niccolo Machiavelli reminded us in the 1500s that "the one who adapts his policy to the times prospers, and likewise that the one whose policy clashes with the demands of the times does not."

This article reviews current trends and describes anticipated shocks in the areas of cyberspace, energy, and resources—all areas that can affect acquisition. We don't need to call on a superhero to save the world from the perils of cyberspace or the crises we face in energy and natural resources, but now is the time to heed trends in those areas.

**Emke** *is the chair of the Defense Acquisition University's transformation efforts. He has also served as a dean for the university and has held numerous leadership positions within the acquisition community.*

## Defending the Networks

Cyberspace is the world of information and systems available through connected computers, the Internet, and telecommunications. When a computer is remotely controlled by an adversary or criminal, it is called a *bot*. Groupings of bots into a network of thousands—and today, millions—of computers are called *botnets*. These rogue bot networks are constantly being upgraded by their creators in order to avoid detection.

In the spring of 2007, the world saw its first war in cyberspace. Estonia, a small Baltic nation, defended itself for a month from an attack that emanated from within Russia. Estonia's computer systems received denial-of-service attacks that flooded the country's Web sites with data and clogged their servers, routers, and switches that direct traffic, shutting down key networks within the country. Though the attack originated in Russia, millions of bots from around the world were combined into a botnet, forming a giant network used to mount the assault.

This is one example of a cyberattack, and it demonstrates that there are potential problems for anyone who is networked. A cyberattack on the United States would likewise have a significant impact. In June of 2007, an attack originating from China shut down the unclassified network in the Pentagon for a week. Targets ripe for cyberattacks include power grids, energy infrastructures, banking and financial services, defense services and the defense industry, emergency response networks, and telecommunications.

The sources of these cyberthreats are just as varied as the targets. Today's connected world also provides not only countries, but individuals; criminal organizations; and political, business, and religious groups with the means, knowledge, and ability to mount cyberattacks against any individual or organization connected to the net. The nature of threat used depends upon the desired outcome. Types of threats include cyberattacks, remote code executions, espionage, malicious code attacks, the compromise of secure and sensitive information, and the theft of secure and sensitive information.

"Nine out of 10 businesses in the U.S. were affected by cybercrime last year," Andy Purdy, the former acting director for cybersecurity with the Department of Homeland Security, recently stated.

Software development today has become globalized. The U.S. industry is saving hundreds of billions of dollars through offshore outsourcing of software development. Both outsourcing software development and moving it offshore increase the threat of cyberattacks on U.S. networks. Protection of intellectual property either doesn't exist or is only haphazardly protected if the nation developing the software has inadequate intellectual property laws on the books. So far, the United States and the global community have been reactive to this problem.

**Perhaps the greatest threat is unsecured transactions and activity by community network participants, exposing the entire network.**

We have readily embraced the many benefits and money-saving results of the information revolution and today's cybersociety. One result is that the U.S. business infrastructure is collected and integrated into a global information infrastructure. Many business systems rely on real-time information processing to operate, and they are monitored and controlled using supervisory control and data acquisition (SCADA) systems that depend upon the global information infrastructure. This integrated aggregation greatly increases the vulnerability to cyberthreats.

## The Threat to the Acquisition Community

Program-focused acquisition communities networked together will be vulnerable to cyberthreats of the types described earlier. A wide range of routine Internet transactions expose acquisition communities. Networked, computer-aided design activities with a prime contractor and associated tiers of suppliers participating expose their networks to potential cyberthreats. When the entire supply chain participates in enterprise resource-planning activities, an acquisition network is exposed to potential cyberthreats. The introduction and use of commercial off-the-shelf software has the potential to contain embedded malicious code, although significantly improved private and government information assurance programs for COTS software would help to mitigate cyberthreats. Perhaps the greatest threat is unsecured transactions and activity by community network participants, exposing the entire network. A final threat is malicious code embedded in outsourced or offshore code, which could allow a malicious attack on defense industry software, weapons system software, or even the acquisition networks.

Acquisition programs will be vulnerable to cyberthreats targeting critical energy and service networked infrastructures as well as cyberthreats to the SCADA systems that manage and control these infrastructures. Programs are impacted by disruption of services and energy flows within the United States, and they are impacted far more so as the length of the disruption increases.

## Problems with Energy and Resources

The electric power grid is both fragile and vulnerable—the U.S. infrastructure and the SCADA systems that control it depend upon a grid with little backup reserve capability. Research has shown that if a cascading failure begins, only 2 percent of the nodes within the grid need to fail before power will shut off in one or more regions within North America.

Both the natural gas pipeline infrastructure and the location of nuclear reactors are concentrated within the United States. However, as the global economy grows, so will the demand for energy. U.S. economic growth is dependent upon readily available, reliable, plentiful, and affordable energy resources, both internal and external. The nation's energy dependence is now being considered as a part of all strategic national security discussions.

Energy facilities, ports, pipelines, terminals, refineries, nuclear reactors, and the electricity grid are all vulnerable to some form of terrorism or extreme weather events. In a recent article in *National Defense*, retired Air Force Lt. Gen. Lawrence P. Farrell Jr. stated that "most of the places we go for oil are tough neighborhoods." Radical religious and terrorist groups have targeted the global oil infrastructure. Currently, failing or failed governments are expected to be a key supplier of oil and strategic minerals such as chromium, platinum, manganese, cobalt, and tantalum in the next 10 years. Many of these increasingly unstable regions are also the primary source of other key natural resources that will make access more difficult.

It should be noted that non-Organization of Petroleum Exporting Countries countries produce about two-thirds of the world's oil. Private companies control much of the non-OPEC supply, and they hold back very little production while maintaining very little spare production capacity. Therefore, the world is dependent upon OPEC for quick relief from any temporary losses in supply because the oil supply and production is controlled by an organization of centralized and state-controlled members.

It should also be noted that the United States imports more than half of what it uses, and most of the imports are transported by sea. Much of what China and India will consume in the future will also come by sea. Safe sea lanes and transport are critical for maintaining the oil needs of the United States, China, and India.

## The Threat to the Acquisition Community

Local and regional disruptions to power, water, and energy will impact the cost and schedule of programs at the prime contractor and various tiered supplier levels. Global disruption in the access to critical minerals needed for manufacturing will impact design, cost, and schedule of programs at all levels of procurement or the manufacturing and testing of vital defense systems. Proprietary designs, business information, and sensitive and advanced technology will become more difficult to keep secure and shared only as intended.

## How to Respond to Trends and Shocks

The acquisition community is faced with this uncertainty, and we need to act to forestall a bad future. As the global world speeds up, decisions need to be made faster. Acquisition leaders need to consider trends today in order to be able to mitigate unwanted impacts tomorrow.

Acquisition guidance and procurement cycles require revision to accommodate fast-paced innovation, rapid obsolescence of software and IT systems, and the supply of energy and resources. The acquisition life cycle needs to be greatly reduced for weapons and supporting systems that are heavily laden with software and IT systems in order to minimize the reliance on prohibitively expensive legacy systems. An alternative to shortening life cycles would be to design new systems that use IT/software subsystems that can be changed out and replaced with state-of-the-art IT/software every two to three years in order to keep pace with technology and innovation breakthroughs.

Maintaining extended secure networks within the acquisition community is essential. Review of risks and identification of when to take additional security measures is on-going yet merits further study. Proper emphasis by both the private and government sectors on information assurance programs can minimize the threat of remote code execution vulnerabilities. Steps can be taken to ensure continued reliance on networks and infrastructures. Security and the management of SCADA systems used to control critical infrastructure need to be reviewed. Measures can also be taken to ensure access to strategic and program-critical energy and resources. Research needs to be accelerated to develop alternatives and reduce reliance on energy and minerals identified as having the potential for supply and availability problems. Alternative designs of critical subcomponents and components that are currently built with threatened minerals require expanded research. The added risk to contractors and programs that do not take steps to forestall adverse impacts of the trends and shocks discussed should be considered.

Overall, a comprehensive review of the impact of trends and shocks on acquisition would help the United States develop alternative strategies and practices to mitigate adverse impacts.

The author welcomes comments and questions and can be contacted at Gerald.Emke@dau.mil.