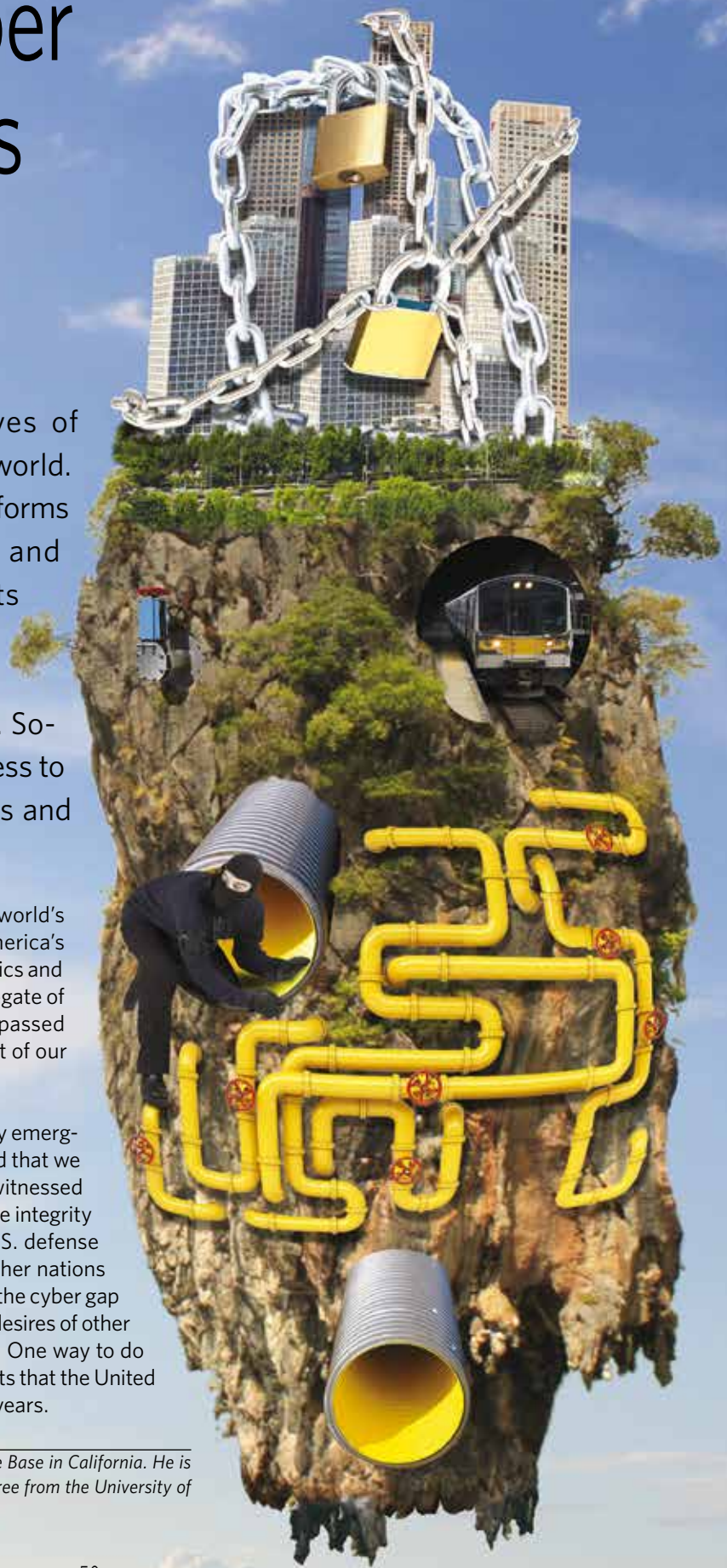
Securing Cyber Acquisitions

Michael Cook



Technology touches the lives of almost everyone in today's world. Our society has embraced all forms of emerging technologies and has thrived from the benefits provided. Personal and professional cellphones have proliferated and enriched the lives of typical Americans. Social networking provides 24-hour access to data and information between friends and strangers alike.

Technology also has played a significant role in the world's economy and in the control and management of America's critical infrastructure, including the power grid, logistics and supply lines and the water supply system. The aggregate of technology that allows these capabilities is encompassed within the definition of cyber and is inherent in most of our acquisitions today.

Yet, with all the benefits of technology, there are many emerging dangers that we are only beginning to identify and that we struggle to address. Acquisition professionals have witnessed the challenges firsthand. Issues such as protecting the integrity and confidentiality of data as well as the critical U.S. defense infrastructure are today at the political forefront. Other nations actively seek to steal our capabilities in order to close the cyber gap we now enjoy. Many reports and articles point to the desires of other nations to expand their influence in the world arena. One way to do this is to gain access to the technological developments that the United States has spent so handsomely to acquire over the years.

Cook *works at the 412th Range Squadron at Edwards Air Force Base in California. He is Project Management Professional certified with a master's degree from the University of Management and Technology in Arlington, Virginia.*

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
FEB 2015		**00-00-2015 to 00-00-2015**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Securing Cyber Acquisitions	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Defense Acquisition University,Defense AT&L,9820 Belvoir Road ,Fort Belvoir,VA,22060**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**3**	

Unfortunately, we are not competing on a level playing field with other nations. We have laws that prevent us from actively stealing trade secrets, intellectual property and military technology; other nations do not. One of the most significant issues that Information Technology (IT) professionals constantly strive to address is information assurance and the protection of sensitive data and associated cyber assets.

Traditionally, managers have sought to protect data, to ensure that it is not accessed or tampered with. IT managers have implemented numerous mitigation strategies to prevent hackers, competitors and rogue agents from gaining access to technology data and information systems. However, the industry's philosophy has shifted recently as the focus has expanded.

The IT industry has come to learn that denying access to data and IT systems is not enough. Foreign states and agents now are motivated by socioeconomic and political interests to expand the breadth and width of network attacks on public infrastructure, critical supply lines and installations that house and process food and water sources. Today's modern hacker has developed the desire and motivation and technical proficiency for gaining access to large networks critical to national and political interests.

Malware is released into the environment daily to carry out these attacks. Malicious code has been a common method, specifically through one system that connects with others. The industry has seen much debate concerning many attacks on our critical infrastructure, attacks via supervisory control and data acquisition (SCADA) systems as well as other types of industrial control systems. Inherent vulnerabilities, and therefore risks, are associated with SCADA systems that have saturated the infrastructure management industry throughout the world. Although SCADA systems are prevalent, industry professionals have not focused on securing them from attack.

Over time, these vulnerabilities have been discovered and exploited, in many cases without the knowledge of those tasked with managing the systems. The predominant point of view for many years appears to have been that SCADA systems can be ignored because other systems, networks and data are more important and require the professionals' attention and focus. Unfortunately, a large-scale attack stemming from malicious code could spread rapidly from one network to another among the networks considered noncritical. The resulting vulnerabilities present the added risk of the attack spreading to larger, critical networks that monitor and control the nation's critical infrastructure.

This becomes even more significant when one realizes that many of our facilities are supported by commercial providers for key services such as fire monitoring. A facility's remote fire-monitoring system may not be considered when acquiring a cyber system, but once that system is installed the facility becomes vulnerable if the fire-monitoring system is hacked and reports normal conditions even while the building is engulfed in flames—thereby rendering the cyber system useless.

Fortunately, a number of SCADA industry standards can be implemented to mitigate the vulnerabilities within these systems. And recent events and advances in technological capabilities have made that mitigation critical to our national and economic interests. Unfortunately for the United States and many other countries, it appears many systems have failed to implement the best practices.

However, we now seem to be taking these vulnerabilities more seriously, from a defensive as well as an offensive standpoint. Members of the cyber and acquisition communities are familiar with the Stuxnet malware that reportedly destroyed 1,000 centrifuges that were being used by Iran to enrich uranium. The Stuxnet deployment renewed interest in protecting SCADA systems and in defending against cyberattacks on our critical networks. Essentially, our nation acknowledged that cyber was an area of warfare that could be both used against our enemies and used by our enemies against us.

There has been a paradigm shift in how we view network and cyber acquisitions. There is a growing awareness of attacks on cyber systems and critical infrastructure.

Another significant issue is the rapid development and evolution of the technology used for our cyber acquisitions. Mitigation efforts against current threats and vulnerabilities often come much later than the identification of those threats, leaving the industry struggling to play catch-up. Even more dangerous are threats and vulnerabilities that are not identified until serious damage has been done. Moreover, in today's daunting economic environment, many organizations look at cyber budgets as areas to cut back. And many top-level managers and members of the acquisition community do not understand the importance of funding and developing a robust cyber capability with a strong information-assurance suite.

One strategy used by the Department of Defense (DoD) in recent years to mitigate cyber attacks has been contracting out the requirement to the IT industry and paying the private sector to protect critical cyber systems. The industry possesses a great deal of experience and talent and at times is better suited to perform the tasks associated with cyber defense than is the military. Unfortunately, the cost is high at a time when military budgets are shrinking and our economy is still recovering from a severe downturn. In addition, when it is decided to contract out for cybersecurity or network and data services, some control is lost. This poses a significant issue for our military and the sensitive and classified data associated with it. The challenge will come in finding partners that are receptive to a comfortable middle ground where the mission of the military is met and the contracted services are provided by industry.

When services are contracted out, critical tasks performed by the government include contract monitoring, oversight and maintenance. Experienced contracting officers and knowledgeable contracting representatives are important in this work. A critical tool of contracting is the contract itself—or related documents that identify the contract requirements.

As we have seen, many serious threats exist to our networks, systems and data, and these threats grow every day as technology continues expanding and developing. Rapid technological change and our inability to keep pace both ensure that the threats will continue to exceed proactive measures against them. However, the goal of those in the acquisition industry is to develop methods to protect the cyber space in the absence of our ability to stay ahead of technology. Regardless of whether the industry or government agencies develop the methods, the benefit will be experienced by everyone.

Threats to our networks and our data affect us all—socially, economically and politically. The focus must be to eliminate as many threats as possible and to acknowledge that vulnerabilities exist all around us, not just in large facilities that maintain network devices and store data. It, in fact, includes the support systems and software that run our critical national infrastructures and enable our cyber capabilities.

From the defense acquisition standpoint, a closer look is needed at the support systems when cyber capabilities are acquired. Facility support systems such as remote monitoring and fire-suppression systems must be evaluated—along with the electrical power system's security.

Cyber systems require a comprehensive environmental analysis to be truly secure and hardened in a manner that will protect our cyber investment as well as provide the needed capability. This challenge requires that the information assurance effort be designed into the cyber acquisition. Although the current acquisition doctrine calls for early involvement on information assurance, we often find lacking either the expertise or a concentrated effort. The DoD needs to attract and develop more information-assurance professionals who possess the knowledge and skills associated not only with information assurance but with managing defense acquisition projects and programs—and who also are familiar with emerging technology.

A great deal of effort will be needed to perform this level of diligence; however, the acquisition community is not in this endeavor alone. As attention increasingly focuses on securing acquired cyber assets, the demand for enhanced security and protection will continue growing. As a result, the future will require a comprehensive environmental-analysis approach in cyber acquisitions. For the acquisition community, an early and proactive approach increasingly is imperative.

The author can be reached at **cookm49@hotmail.com**.