By Isaac R. Porche III, Jerry M. Sollinger, and Shawn McKay

AN ENEMY WITHOUT BOUNDARIES

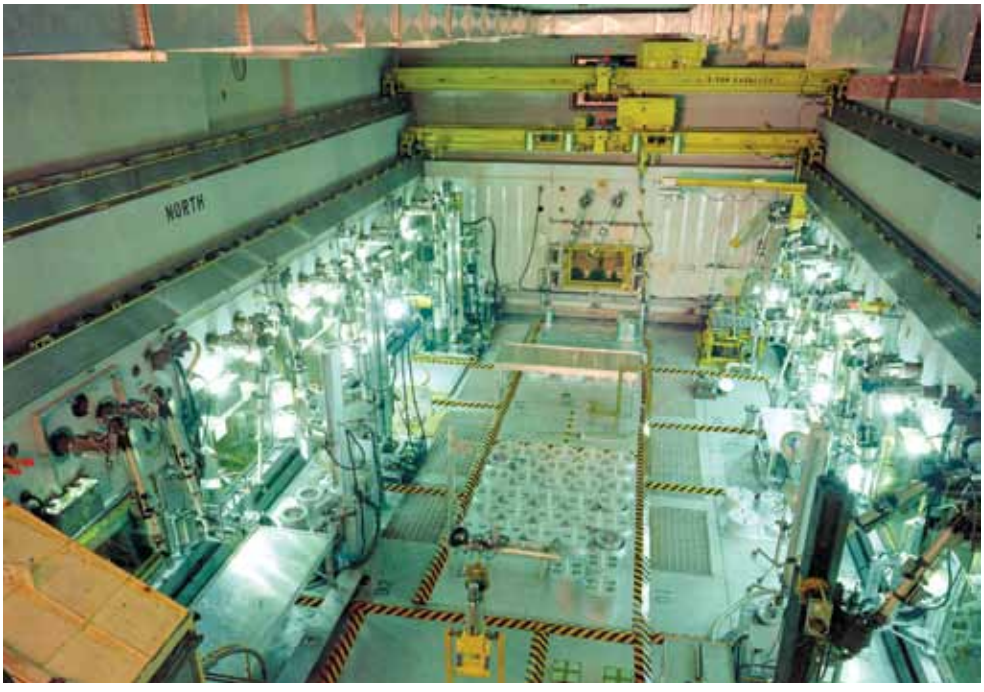
ISTOCK PHOTO

People tend to speak of defending U.S. cyberspace in the same way they would speak of protecting its physical borders, the authors note. But they caution that such a defense cannot be mounted: An attack can come from virtually anywhere, and the essential components of cyberspace are constantly in a state of change.

It is impossible to block every cyber attack, so strategy and policy should be focused on how to respond once that attack occurs.

In August the largest oil producer in the world—Saudi Aramco—was forced to take operations offline to purge its network of a virus that infected tens of thousands of workstations. In April, Flame malware was found to have penetrated Iranian Oil Ministry computers. That attack, which came just two years after the highly damaging activation of Stuxnet—widely believed to be the product of a U.S.-Israel effort—led to rumors that Iran would establish a national intranet to protect it from future threats.[1]

Although recent rounds of high-profile international cyber attacks have targeted the energy sector, other industries have much to learn from the vulnerability of those networks and the capability of their respective attackers. The attacks and their predecessors, including Conficker and Agent.btz, expose and exploit the weaknesses of critical networks, even those that are ostensibly "offline." They are not just difficult to detect and stop: They are nearly impossible to prevent. The message for network administrators is that there is no single defense against a sophisticated and constantly morphing offense.



IDAHO NATIONAL LABORATORY

A determined attacker no longer requires an Internet connection to insert a worm or a virus into a network. Work at the Department of Energy's Idaho National Laboratory (INL) in 2007–2008 showed how a "closed" system could be maliciously compromised. A significant contributor to national defense research, INL also has a strong focus on nuclear energy. Shown here is its Hot Fuels Examination Facility.

As Stuxnet and its like have proved, a determined attacker does not require an Internet connection to implant a worm or a virus, and a network's weaknesses can be exposed quite by accident. Cyber defense is difficult, in large part because a cyber attack is not always obvious. Unquestionably, cyberspace favors the attacker, not the defender.

Early Precedents

In the aftermath of its discovery, the nature of Stuxnet did not surprise those who had known that such an attack was theoretically possible. The likelihood of such a targeted attack was revealed as long ago as 1997, when a U.S. Department of Defense exercise called "Eligible Receiver" demonstrated the ability to gain surreptitious access to computers controlling an electric power-grid plant.

A decade later, the U.S. Department of Energy's Idaho National Laboratory showed that it could insert malicious code into a closed network to inflict severe physical damage on an industrial generator. Indeed, Stuxnet may not have even been the most successful or catastrophic cyber attack on a supervisory control-and-data-acquisition system.

In his 2004 book *At the Abyss: An Insider's History of the Cold War*, Thomas Reed describes how in 1982 a Trojan horse was deliberately inserted into Canadian software designed to control natural-gas pipelines. That software in turn was "allowed" to be stolen, and was then used by the Soviets. According to Reed, "[T]he pipeline software that was to run the pumps, turbines, and valves was programmed to go haywire, after a decent interval, to reset pump speeds and valve settings to produce pressures far beyond those acceptable to the pipeline joints and welds. The result was the most monumental non-nuclear explosion and fire ever seen from space."

No Borders

People often speak of "defending U.S. cyberspace" in much the same way they do of defending the country's borders. The difficulty is that cyberspace really has no boundaries. The data, services, and applications in cyberspace flow across routers and servers that span the globe. Thus, there are two primary challenges to mounting a defense.

First, because cyberspace has no boundaries, an attack can come from virtually anywhere. Individuals with sinis-

ter intentions can mask their electronic identity or simply steal one, either by collecting the information required to take on a purloined identity or by using an Internet robot—a "bot"—to take over a computer that can be used to facilitate or perpetrate the attack. Second, cyberspace changes constantly. The components of cyberspace are regularly being created, destroyed, moved, lost, physically relocated, hidden and exposed, and connected and disconnected. So assuming a new identity is far easier in cyberspace than it is in the physical world.

What this means is that it is not possible to stop all attacks. Firewalls and intrusion-prevention systems will thwart only so many attacks. Defenders must be right all the time; the attacker, just once. Careless use of a portable hard drive, the failure to update virus-protection software, a compromised password, and dozens of other events can open the door to an attack. Thus, as we discuss later, a key policy focus must be how to respond once an attack has occurred.

But mounting a response to a cyber attack requires knowing that one has occurred, and in cyberspace that is not necessarily easy. Malicious activity is common in cyberspace, but not all such activity constitutes an attack. Examples include "phishing" expeditions designed to steal personal or financial information, efforts to obtain proprietary information from private-sector firms, and simple hacking attempts to penetrate computer systems for the purpose of spying. Those are not technically classified as attacks but as espionage attempts. (Such collection activities or probes are known as computer network exploitation and are differentiated from computer network attacks, which seek to destroy, alter, or degrade capabilities.) However, they could pave the way for more destructive activity, or they could be used to plant a worm that, at some later time, could launch its own attack.

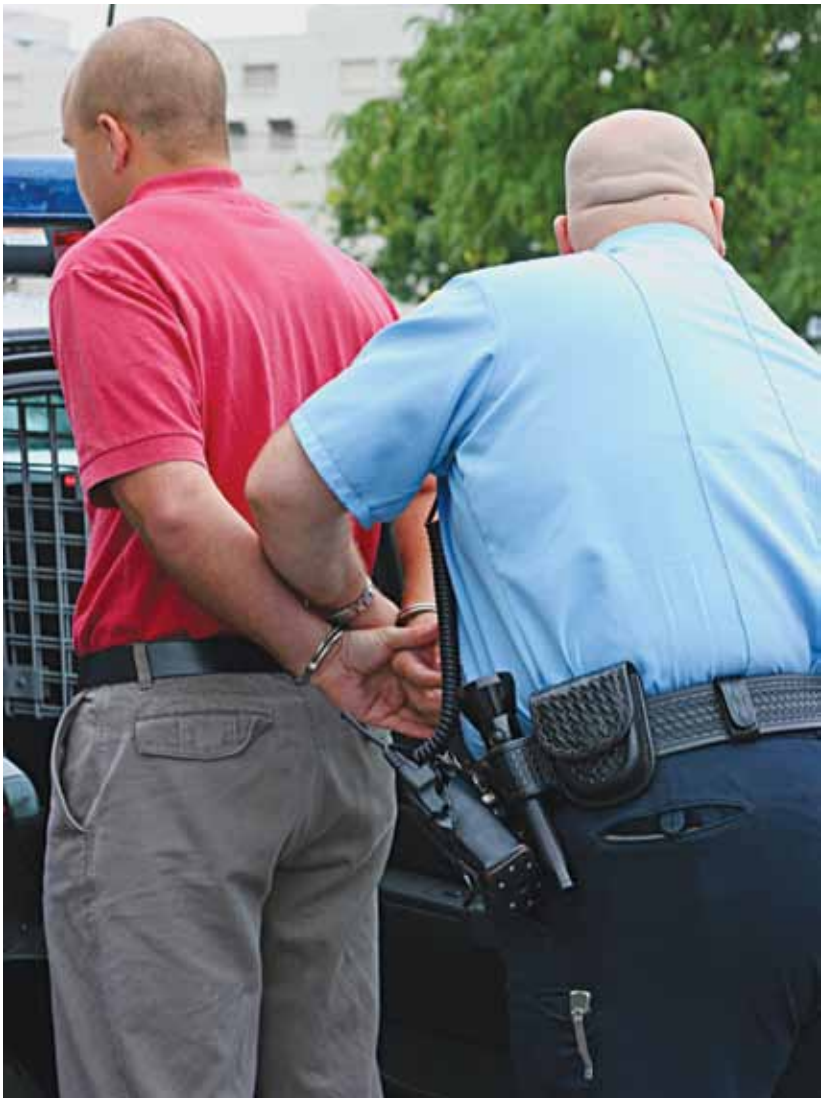
Complicating matters, worms can lie dormant until the circumstances they have been built to exploit appear, and only then do they become active. Thus, the actual "attack" can occur days, weeks, or even months after the initial intrusion.

Don't Depend on the Air Gap

The critical distinguishing characteristic of cyberspace is that it has become a "global commons," existing almost everywhere, open to anyone, allowing its inhabitants to move across it with ease and at ever-increasing speeds. It is difficult to imagine how to defend a space that has no boundaries, changes constantly, lets anyone in, and exists virtually everywhere. Even so-called closed networks, such as those that are not connected to the Internet (i.e., air-gapped networks) are at risk from the manual insertion of malware (by means of portable storage devices). In other words, even if the entire country of Iran were to go "offline," it would remain at risk—or even invite a challenge from attackers.

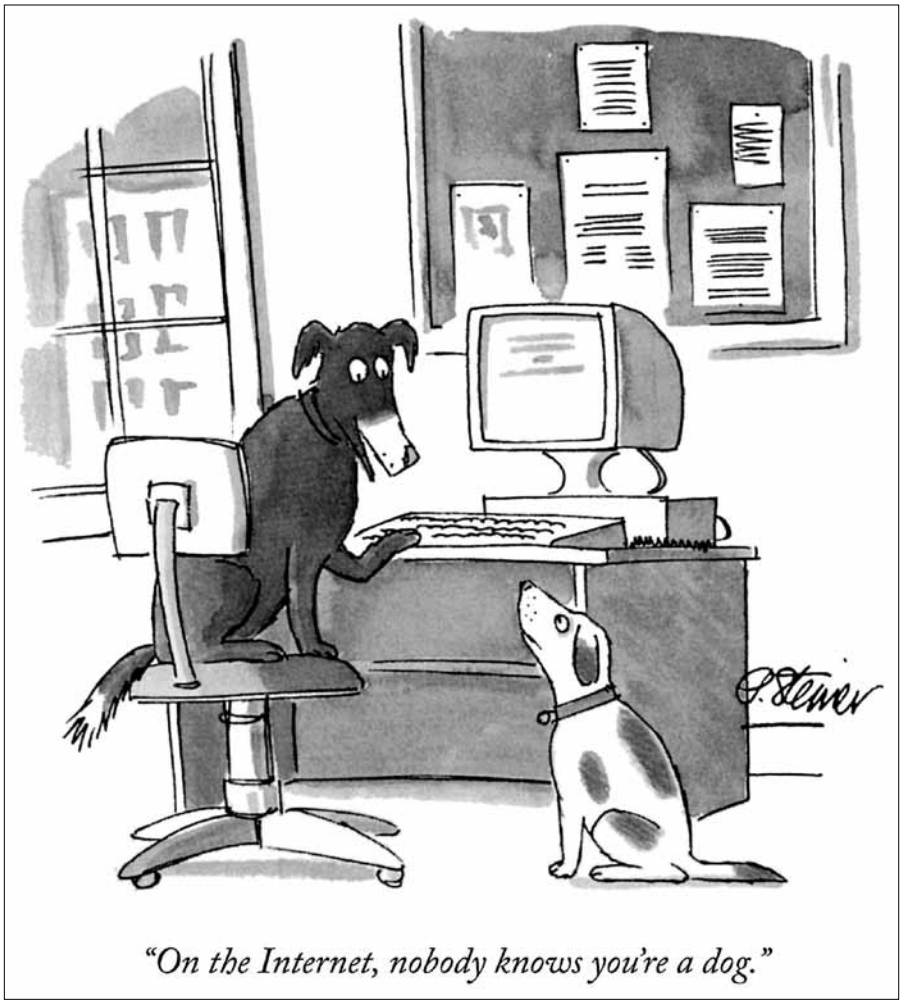
Thus, the so-called U.S. cyberspace cannot be fenced off.[2] Some portions are within territorial borders, but others are not. Server farms in Canada, for example, support the BlackBerry that is practically standard equipment for American government officials and private-sector employees. Real-world barriers have no counterparts in cyberspace. Nor do electronic barriers offer sanctuary. While organizations can (and should) build electronic firewalls, such defenses can be breached or bypassed.

Ubiquitous access also makes establishing a defense especially difficult. Is the packet of information asking



ISTOCK PHOTO

Despite locks, alarms, laws, and penalties, societies everywhere have crime, and thus need police forces to identify illicit activity and arrest the perpetrators. The authors contend the need for similar protection in cyberspace is hampered by a tangle of conflicting and overlapping authorities among government agencies and private-sector entities.



"On the Internet, nobody knows you're a dog."

PETER STEINER / THE NEW YORKER COLLECTION / WWW.CARTOONBANK.COM

for entry to a server what it says it is, or is it a disguised piece of malware that intends to offload data from the site and sell it? Not only is cyberspace universally accessible, it lets anyone be whoever he or she wants to be. As the famous *New Yorker* cartoon by Peter Steiner points out, on the Internet, no one knows you are a dog. No one knows whether you are a criminal, either.

Cyberspace can incorporate the unwilling, too. Air gaps are difficult to maintain and thus do not sufficiently protect devices from nefarious actors who operate in cyberspace.[3] The computers infected by Stuxnet—in all likelihood—were not intended to be connected to the Internet (or any other network). As long as a device is not "dumb" (that is, as long as it contains a processor and some memory), it can be accessed, affected, and controlled to some degree.[4] Electric power is also not a requirement. Modern corporate badge readers and electronic tollbooths communicate with inert badges or cards. Many devices and appliances, such as printers and cell phones, have wireless connections and can be surreptitiously turned on and accessed.

The upshot of the inherent nature of cyberspace is that no country or private-sector organization can prevent attacks entirely. It takes only one person, one device, one opportunity to compromise one component of a system. At the state level, this means that the playing field can theoretically be leveled: All nations have the opportunity to embrace the advantage of the attacker, and all will potentially suffer the embarrassment of the unsuccessful defender.

An Active Defense Is Critical—and Difficult

An argument can be made that the best way to defend is to take offensive action in a form termed *active defense*.[5] For example, in their 2009 edited volume *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, William Owens, Kenneth Dam, and Herbert Lin state that active defense includes both the "neutralization of an attacker's ability to attack and the imposition of costs on the attacker for the attack." The authority to proceed in this manner (attack and counterattack) is a potential bottleneck that can limit the ability to operate at the "speed of cyber." In mid-2011, President Barack Obama signed orders to clarify authority and permission with regard to when presidential approval (a slow process) must be obtained. According to the article, exploit (or intelligence) missions are preapproved, but not those actions that deploy viruses and worms.[6]

There are many parallels to draw on in considering the nature of conflict in cyberspace. Police protection is one. Consider conventional crime, such as robbery or burglary. Those crimes have never been eliminated, and occur regularly in every community—despite locks, alarms, gates, laws, and penalties. As a result, every community has a police force to identify the activity and arrest the criminals so they can be removed (at least temporarily) from civil society. Police exist to give chase and apprehend criminals.

An effective cyber defense requires excellent capabilities marshaled into a coherent and coordinated response. In our view, the United States is capable, but lacks the ability to execute a coherent and coordinated response, due in part to the conflicting and overlapping responsibilities and interests of various federal agencies and private-sector entities. Responsibilities can overlap or conflict. Consider: Theft of financial information is a crime and falls under the jurisdiction of the FBI. But the Department of Homeland Security has a mandate to protect the civilian agencies of the federal executive branch and is responsible for the protection of critical cyber-

NEWSCOM

The now-notorious Stuxnet worm provided a real-world demonstration of a cyber weapon breaching a "closed" computer network in 2010 when it infected Iran's nuclear-weapons program. Its existence became public when it "escaped" the Natanz nuclear plant and circulated via the Internet. This file photo shows Iranian President Mahmoud Ahmadinejad visiting the Natanz facility prior to the attacks.

space. Good intelligence has always been a prerequisite for good defense, but many attacks come from overseas locations. Therefore, efforts to garner intelligence outside the United States must involve those agencies authorized to do so. Many regard the National Security Agency as the most capable government entity when it comes to analyzing and defending against cyber attacks, but it is a spy agency. Legal limits constrain DOD actions. Additionally, much illicit activity masks itself in emails, but privacy laws preclude the extent to which the government can monitor such transmissions.

None of that is to say that the limitations cannot be overcome. However, the challenge is great—and further compounded by the speed needed to respond to increasingly sophisticated threats. Worms can be scrubbed from systems, but administrators need to act quickly, or the worm will have done its damage and then erased itself.

No Substitute for Strong Policy Action

Stuxnet and similar threats offer the following basic lessons for both network defenders and policy makers:

- The threat of physical damage from cyberspace is real and increasing.
- It is not possible to prevent all attackers from intruding on all networks and devices.
- The best defense includes an offense.
- Current federal organizational boundaries hinder efforts to successfully identify and mitigate intrusions.

Accordingly, we recommend additional congressional action to grant new authorizations that accomplish at least the following two goals:

- Enable substantially better collaboration among the various government organizations that have a role in cyberspace and between those organizations and the private sector.
- Grant *at least one capable organization* the authority to track cyber intruders and criminals with the same freedom of maneuver that these adversaries enjoy. New authorities must be established for this to occur and it will likely require substantial revisions to the U.S. Code—undoubtedly a daunting challenge—and significant public debate.

There is no simple solution to the threat posed by adversaries in cyberspace. Clearly, one challenge is determining how best to navigate within the requirements and expectations of a democratic society that relies heavily on its computer systems and networks, against an enemy that has no boundaries and can act with impunity in the face of national or international norms and legal frameworks.

Options in the Era of Stuxnet

The implantation of Stuxnet and the successful execution of its instructions are worrisome for at least four reasons. First, the incident ends the debate about whether such a worm is even possible. It is real, and it can do serious physical damage. Second, it was a state-sponsored effort, not the creation of some whiz-kid hacker, or even

a more sophisticated criminal enterprise to which a state turned a blind eye.

A third implication is that control systems other than those for both nuclear and non-nuclear power plants could be co-opted. The list of control systems that, if penetrated, could wreak substantial damage is long: electrical grids, systems that facilitate financial transactions, air- and rail-transportation, water and sewage, and even those in space, such as the Global Positioning System. While it is unclear exactly how vulnerable these systems are, the experience of Stuxnet suggests that the most prudent course is to treat them as though they are—and determine what steps should be taken to protect them.

This leads to a fourth cause for concern: All of those systems involve both private and government entities. Trying to coordinate defensive activities across government agencies is challenging enough. Add the private sector to the mix and coordination efforts become even more complex and thus more difficult.

The ability of a worm like Stuxnet to affect the systems on which so many depend makes defense everyone's problem; if GPS were to go down, the outage would affect not only those trying to navigate their way to a meeting in a strange city, or a ship charting its course to port, but also military units that depend on GPS for location information, and weapon systems that depend on it for accurate delivery. A disrupted power grid would affect government and civilian organizations alike.

Some experts downplay such threats and vulnerabilities. They point out, accurately enough, that the first thing that happens after a breach is that programmers and system engineers go to work to plug the gap. In that sense, cyber attacks are self-defeating, since their very attack calls into being the means to overcome them. We contend that state sponsorship makes it difficult to defend against Stuxnet-like worms. A state can devote substantial manpower to cyber warfare, but defending against a state-level threat will require the best capabilities available in industry and government. Fortunately, the United States has some very good capabilities in both sectors. However, it will take a coordinated effort and therein, we maintain, lies the challenge or—more accurately—one of the challenges.

A complicating factor is that passive defense alone may not necessarily suffice. Retaliation (if in the national interest) requires determining who did what after an attack and precluding the next assault. Recent announcements that the United States may respond to a cyber attack kinetically or conventionally focus on that need (see, e.g., the White House's *International Strategy for Cyberspace*). But we contend that a more desirable goal would be to know what is likely coming next, because a very rapid response might be required, particularly against what are known as "zero-day" attacks. Zero-day attacks exploit software vulnerabilities that are unknown to developers.[7] Those types of attacks require responses within hours or days.

Congress is studying its options with regard to organizational assignments and new authorities to provide a comprehensive new approach to cybersecurity. Collectively, the bills have called for:

- More cybersecurity awareness and standardized notification of breaches in the private sector (at the federal level)[8]
- More cybersecurity education and training
- A new cybersecurity coordinator position in the executive branch, the Department of Homeland Security, or DOD
- Development, enforcement, or incentives for adherence to new cybersecurity standards or the study of such standards.

On many of those points, Congress, the White House, and the private sector are at an impasse. For example, in August, a bill intended to protect and regulate critical privately owned U.S. infrastructure (such as utilities, chemical plants, and water treatment facilities) failed to pass the Senate, in part because of objections from the U.S. Chamber of Commerce. In April, the House passed a bill imposing guidelines for information sharing between the government and the private sector to help improve the detection of cyber attacks. The White House objected to the legislation on the grounds of privacy concerns.[9]

Such approaches will require additional analysis and further development, particularly with regard to the need for a firm boundary between domestic law enforcement and intelligence agencies and the firewalls (if you will) between the public and private sectors that are so intrinsic to democracy.

This article is based on the RAND occasional paper "A Cyberworm That Knows No Boundaries" OP-342-OSD (Santa Monica, CA: RAND Corporation, 2011), www.rand.org/pubs/occasional_papers/OP342.html.

1. For a detailed account of the U.S.-Israel program dubbed "Olympic Games," see David Sanger, Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power (New York: Crown, 2012).
2. We hold a U.S.-centric view of cyberspace and other nations may not share the same view.
3. Another version of an air gap (between an IT device—with memory and processors—and cyberspace) is a long period of latency with intermittent connectivity.
4. Though the Stuxnet-targeted network likely was closed, it was "sucked into cyberspace" because computers that accessed it (reportedly technicians' laptops) could also have been used for email, linking to an open network.
5. A good defense is to try to anticipate an attack's nature and origin. Thus software developers try to write code with specific threats in mind—no trivial task.
6. Lolita Baldor, "Pentagon Gets Cyberwar Guidelines," Associated Press, 22 June 2011.
7. "Zero day" is the term for the day an attack is discovered, not the day it is launched, thus suggesting that the intended damage may have already occurred.
8. Many states already have notification requirements. A complicating factor is if the breach involves personally identifiable information.
9. Ken Dilanian, "U.S. Chamber of Commerce Leads Defeat of Cyber-Security Bill," Los Angeles Times, 3 August 2012.

Dr. Porche is the associate director of the Force Development and Technology Program for RAND Arroyo Center, the U.S. Army's only federally funded research and development center for studies and analysis. He joined RAND in 1998 and holds a Ph.D. in electrical engineering from the University of Michigan.

Dr. Sollinger joined RAND in 1990 after a career in the U.S. Army. His work in the national security arena has focused on military personnel, reserve components, acquisition, logistics, security policy, and training issues. Work in the domestic arena has included health care, drug policy, and education research.

Dr. McKay is a researcher who holds a Ph.D. in systems engineering from Purdue University. At RAND, he applies systems-of-systems analysis and modeling to problem areas in cyber, logistics, homeland security, and aircraft survivability.