Recognize the Role of Private Enterprise in Protecting Critical Infrastructure and Cybersecurity

In both the physical and cyber worlds, the line between government protection and private security is not necessarily a bright one. The government's role is rooted in its defense function, a power delegated to it by citizens. We rely upon the government's courts, police, and military to protect us; yet at the same time, we rely upon a complementary and indispensable private sector *security* function. While government's primary reason for being is the protection of society, we nonetheless require private strategies—such as security guards, gated communities, door locks, burglar alarms, firewalls, and anti-virus software—to be really secure.

Better appreciation of distinct public and private roles is warranted in the critical infrastructure and cybersecurity debates, particularly since the September 11, 2001, terror attacks. To safeguard critical and information-age assets exposed to physical or cyber-attack, we ought to not automatically assign security roles to government that would best be carried out by private parties. Critical infrastructure is privately owned, after all, and private sector leadership and responsibility for still-uncertain cyber and physical security needs should not be lightly overruled. For example, technical matters involving secure infrastructure design, such as backup, redundancy, and duplication of data and network pathways, are the province of the private sector.

A close look at alleged market failures involving large-scale enterprises often reveals heavy government regulation, and thus *government failure*. Franchise laws and network regulation, like open access requirements, interfere with competitive incentives to improve products or services and invest in infrastructure and maintenance.

Security policy should avoid rigidities like those that characterize airport security, where the federal government has taken over the entire baggage checking function, for example, with unfavorable implications for future private luggage delivery efforts, the ability for airlines and airport operators to adapt to changing threats, and longer term airport privatization efforts.

Private identity systems managed and protected by answerable firms—in which owners reserve the right to refuse to admit anybody who is not a member—may often be preferable whether the issue is access to a piece of critical infrastructure, such as an airport or power plant, or access to a computer network. In some cases, owners seem to have no interest in matching faces against a database of terrorists, for example, preferring instead to know exactly who you are, rather than whether you are on a list of criminals. Biometric technologies and other forms of authentication offer significant

promise for securing both critical infrastructure and electronic networks.

Following the 9/11 terrorist attacks, America faced a choice of whether to seek private or government security strategies.

Privately, security could have been beefed up by private sector mechanisms and technologies like IDs and biometrics, and even non-technical means like private sector-mandated background checks and insurance innovations like premium adjustments. While a new government role was probably unavoidable after 9/11, to further government's entrenchment in security is not necessarily a good thing.

Entrenching government on behalf of critical infrastructure security is a step backward toward viewing large enterprises as "utilities," hampering both industry growth and security. In electricity, for example, mandates to supposedly enhance "reliability" can impair operation of the infrastructure itself. The blackouts of 2003 served to justify renewed calls for enhanced eminent domain powers to seize land for transmission lines. In such cases, we see the idea of central regulatory control of critical infrastructure proposed in the name of security and reliability without sufficient regard for the broader consequences to either security or industry viability itself.

Wayne Crews