# 16.2: Protecting the Anthrosphere

The anthrosphere constructed with a high degree of human ingenuity has provided a generally safe and comfortable environment for human beings. The underpinning of this entire support system is the **infrastructure**, which includes systems to purify and deliver water, electricity generation and distribution systems, communications, fuel distribution networks, highways, and railroads. The sophistication and complexity of the infrastructure is what makes it work so smoothly (for the most part), but also makes it vulnerable to attack. A key aspect of this susceptibility to attack is **vulnerability due to interconnectivity**, which arises from the high degree to which various parts of the infrastructure are interconnected and mutually dependent. No part of the infrastructure illustrates vulnerability due to interconnectivity more so than modern electrical grids, which can stretch across vast geographical regions and across national borders. A reminder of this vulnerability occurred on August 14, 2003, when a failure of the electrical grid in the northeastern U.S. and southeastern Canada resulted in a power outage for tens of millions of people in New York City, Detroit, Cleveland, and Toronto. In this incident a total of 68,100 megawatts of generating capacity — equivalent to 68 very large, modern power generating facilities — was lost as dozens of high-voltage transmission lines shut down. This occurred within about 5 minutes, and the event that caused it probably took only about 10 seconds. The precipitating event was not terrorism — although it well could have been — and probably resulted from nothing more dramatic than tree limbs interfering with transmission lines.

The electrical power failure described above illustrates a phenomenon called **cascading failures** on complex networks discussed in a 2009 article in *Scientific American*.1An electrical power distribution system is a complex network of hundreds of electrical power plants interconnected by electrical transmission lines. Such a system enables very efficient generation, distribution, and utilization of electrical power in that a surge in demand on one part of the system can be compensated by redistribution of power from the network to that segment of the system. Therefore, local generating facilities do not have to maintain the capacity to meet temporary demand, and this results in high efficiency and much lower costs. Other parts of the infrastructure have similar networks. Routers on the Internet are designed to route Internet traffic around bottlenecks or other routers that are temporarily out of commission. Modern manufacturing operations using “just-in-time” deliveries of components make it unnecessary to stockpile large quantities of parts, thereby minimizing the need for production capacity and maximizing efficiency. The downside is that these systems operate “close to the edge” so that a relatively small failure, such as one brought about by human mischief, can rapidly cascade into a major failure.

Arguably the part of the infrastructure most vulnerable due to interconnectivity and subject to cascading failures resulting from terrorist attack is the vast, intricately interconnected computer network that is now part of all modern systems of communication, commerce, and military operations.[2] These systems are vulnerable to so-called cyber crime in which key components can be disrupted leading in worst cases to total system breakdown. Much of the effort in homeland security in the U.S. and similar efforts in other countries is devoted to combatting cyber crime.

Chemistry can be applied to infrastructure protection. One area in which this is true is the production of materials that resist heat and flame. Such materials used in buildings can provide substantial protection from fire. Processes that are consistent with the practice of green chemistry also provide protection from attack. For example, green chemistry attempts to reduce the production and use of hazardous materials. Sophisticated analytical chemistry and analytical instrumentation can be used to detect agents of attack before damage is done.