Editorial

It reads like the plot of a gripping novel: Iranian hackers have infiltrated the networks running the aging United States power grid and may already have the ability to knock out electricity flowing to millions of American homes! (See page 16 for related feature).

Some editors might consider this storyline overly dramatic or unrealistic to support a work of fiction. But the problem is, this scenario is not taken from a novel. It is from a frightening special report by the Associated Press, the result of more than 120 interviews and examination of dozens of sets of data, government reports and private analyses.

As the report indicates, many of the substations and equipment that move power across the United States were never built with network security in mind, and hooking these plants up to the internet over the last decade has given hackers new backdoors in.

According to top experts, who understandably spoke only on condition of anonymity, on some dozen occasions during the last decade, sophisticated foreign hackers have gained enough remote access to control the operations networks that keep the lights on.

Such a nightmare scenario may cause far more devastation than the extraordinary power blackout that hit steamy U.S. and Canadian cities in August 2003, depriving some 45 million people in eight states of electricity, stranding people in subways, closing nine nuclear power plants, and choking streets with workers driven from stifling offices.

In the 2003 blackout, New York City subways, elevators and airports lost electricity or resorted to limited backup power. Some subway commuters were stuck underground for long hours after the blackout hit, and people lined up 10 deep or more at pay phones after cell phones stopped working. At least 11 deaths were attributed to the effects of the blackout, and the financial cost was an estimated $6 billion.

Though it was a terrifying event for tens of millions, there were some factors that made it more manageable. Old fashioned “landline” telephones continued to work, allowing those in the afflicted areas to communicate with relatives and close friends. The fact that the blackout started during daylight hours gave many individuals the ability to prepare for the coming darkness, and in many areas, electricity was restored by nightfall. Most crucially, as it turned out, the blackout was caused by a combination of human error and equipment failure, and not by an act of terrorism.

Twelve years later, with pay phones all but obsolete and a great number of landlines dependent on electricity to work, a lengthy blackout beginning in the middle of the night that would be the work of cyber-terrorists or an enemy country like Iran would include no such reassurances.

Although, baruch Hashem, terrorists have not plunged us into darkness, it would be a grave error to extrapolate that they don’t have the technical ability to do so. In fact, experts fear that their poisonous cyber-fangs have penetrated deep into the system, and likely have the capability to strike at will.

There can be no doubt that the internet has dramatically changed the way the material world operates, but we must also recognize that this change not only contains weighty spiritual perils, but also physical ones.

While astronomical sums are being spent trying to prevent infiltrators from gaining access to sensitive systems, it appears that hackers are continuously managing to outwit the defensive shields being put up.

The material hazards of the internet are hardly limited to hacking. The internet and social media are prime recruiting grounds for terrorists, and instead of traveling to overseas camps, would-be jihadists simply go online to receive both their practical training and their inspiration to commit infamous acts of horror.

Leading presidential candidates on both sides of the political divide are calling for ratcheting up efforts to fight against global terrorism in cyberspace, and close down terror-disseminating websites. But that is far easier said than done. Websites can be located anywhere in the world, and even if found and shut down, they can be quickly started up elsewhere.

Ultimately, the fate of all of mankind is dependent on the protection of Hashem. But that doesn’t preclude the obligation to make every possible hishtadlus in this regard.

It is crucial that not only is this very real danger approached with the gravity it deserves, but that we recognize that each advance in technology brings along its share of severe drawbacks and serious risks. Taking off rose-colored glasses and accepting this basic truth is already a key step in the right direction.

The Frightening Finger on the Light Switch

TERRORISM

File under

11 Teves 5776