Column: Dangerous Codes Lurk on the Internet

People lie, cheat and steal. Fortunately that is not true for all people, but there is a sizable collection of rascals hanging out by the Internet. No more than 50 years ago, lying, cheating and stealing usually required some personal contact between the perpetrator and the target, but with the growth of the Internet, crime has become remarkably impersonal.

Last week several hospitals were paralyzed when their computer systems were “attacked” by cybercriminals, people who write computer code or hire people to write computer code that will disable computer operations.The criminals have probably never met any of the several thousand people whose lives they have put in jeopardy, and it is apparent from their demands that they just want money.

When the operations of the Colonial Pipeline Company were shut down by cybercriminals, there is no indication that anyone died as a result. The recent cyberattack on JBS meat processing plants also produced no human casualties and may have even delayed several heart attacks by interfering with the production of sirloin steaks, but the vulnerability of huge industries was again demonstrated.

The Internet developed from a network of computers intended to distribute scientific information quickly, easily, and widely. I doubt that any of the scientists involved in the birth of this innovation realized that their fact-sharing system would grow into an unruly adolescent capable of selling weapons of mass destruction. Perhaps the greatest surprise as this awkward teen entered adulthood was that it could be a weapon of mass destruction.

Malevolent code sent across the Internet from thousands of miles away could poison the drinking water of entire cities, sabotage the functioning of nuclear power plants, or just shut off the lights in an entire nation. I was in New York City on two occasions years apart when the electricity failed. It took about 10 minutes from lights out to gridlock, panic and chaos.

The United States has the most powerful (and expensive) army in the world. The U.S. Navy has at least 20 multibillion-dollar aircraft carriers in service; China has three; Russia has one. Our missiles and satellites, smart bombs and special forces have given us a sense of security in a world seemingly intent on blasting itself back into the Stone Age. We are certainly ready to fend off invading Vikings, Babylonians, Hittites, Tartars, Ottomans, and maybe even the Roman Legions, but these ancient civilizations bent on conquest are innocuous compared to a small group of trained technicians writing code to redirect our drones and confuse our global positioning satellites.

Why spend billions of dollars on an aircraft carrier when you can disable it with a computer program targeting its sewage system. Our modern defenses have become as pointless and impotent as the walls surrounding castles after the invention of artillery. Constantinople had miles of fortified walls and thousands of soldiers defending those walls. It was considered one of the least vulnerable cities in the civilized world. The Ottomans had cannons.The Ottomans blasted their way into the city. Technology was the ultimate conqueror.

We sit in our autos, airplanes, trains and living rooms hoping that a greedy, angry, or

simply insane computer programmer will not press the Send button on his or her computer to distribute a code that will inconvenience, hurt or kill us. How did we end up so unprotected? Didn't the people to whom we give hundreds of billions of dollars every year see this danger coming? I suspect they did see the potential dangers in a world dependent on programming that many clever 12-year-olds could master.

I suspect our vulnerability is a consequence of arrogance: we believed we could control this thing. We believed we were more clever than the people hoping to swindle or injure us. We believed we had enough people in our country dedicated to defending our lives, liberties, and pursuits of happiness to stifle the efforts of people who want to sew chaos or pursue personal agendas or who simply want to show how destructive they can be.

I toured one of Andrew Carnegie's mansions on the upper east side of Manhattan. It was attractive but not ostentatious. The house was obviously designed to keep a family secure and comfortable. Carnegie had his house equipped with the most modern of conveniences, including a highly sophisticated central heating system. New York City weather is often challenging in the winter, and in recognition of this, Carnegie built redundancy into the system. If one furnace or boiler failed, a duplicate would be fired up. It had the equivalent of a modern day backup generator.

Many decades after this house was built, the need for backup systems to avoid disasters was still not widely appreciated. While I enjoyed the darkness of my first New York City blackout, I learned that many of the hospitals and chronic care facilities in the city did not have backup generators and were scrambling to get units installed before patients on ventilators and other power-hungry devices died. How could such an obvious need be overlooked?

In a city with all of its electricity (at that time) coming from outside the island of Manhattan across just two supply points, even the most obtuse of city managers must have realized this was a disaster waiting to happen. After the power failure, every hospital had backup generators installed. Even earthworms can learn if they are

traumatized.

And so we face another obvious dilemma. We rely on the Internet for activities ranging from blood testing to oil pumping, meat packing, shopping, and finding that one and only who will make us happy for the rest of our lives. Access to this information highway is so easy that computer programmers in Moscow can retrieve voter registration information from Michigan or shut down sewage treatment plants in Louisiana.

Criminals and agents of hostile states are getting rich off the vulnerability of the Internet with Ransomware, the extortion of money from people, governments, or businesses that have had their computer systems disabled by code writers. Why is there no backup system to turn on when the principal system is frozen by Ransomware?

Why are there no adequate systems in place to keep Ransomware and potentially lethal attacks on our infrastructure from getting access to the Internet? Obviously, we must find techniques to protect the Internet from invaders before the hackers level their lethal lines of code on our negligible defenses and trample on our privacy, our assets, and our independence.

Dr. Lechtenberg is an Easton resident who graduated from Tufts University and Tufts Medical School in Massachusetts and subsequently trained at The Mount Sinai Hospital and Columbia-Presbyterian Medical Center in Manhattan. He worked as a neurologist at several New York Hospitals, including Kings County and The Long Island College Hospital, while maintaining a private practice, teaching at SUNY Downstate Medical School, and publishing 15 books on a variety of medical topics. He worked in drug development in the USA, as well as in England, Germany, and France.