Tourism is the Next Big Target

Voltaire wrote, "Everything is fine today: That is our illusion." As civilization becomes increasingly reliant on technological advancements and artificial intelligence, the illusion that "everything is fine" in tourism and hospitality is inexorably approaching an irreversible and potentially catastrophic event horizon. Tourism, owing to its ease of access, has long been the target of violence perpetrated by terrorists, nihilists, criminals, and mentally deranged individuals, from ancient Rome to modern-day Las Vegas.

In addition, earthquakes, cyclones, volcanic eruptions, and other adverse natural phenomena have posed threats to travel and travellers since ancient times. The internet and social media have made global awareness of such attacks near-instantaneous. Inevitably, cybernetic attacks now loom large on the horizion.

The Internet of Things (IoT) is the latest pop-science fad, describing devices of all kinds connected to the internet, from refrigerators and washing machines to light bulbs, autonomous cars, and even rubber ducks. IoT devices rely on the internet to relay commands from the user's smartphone, or from the device itself, to a network server, which in turn activates the connected thermostat, light bulb, garage door opener, or rubber duck. For example, an AI-empowered refrigerator, upon detecting a shortage of milk or eggs, might send the relevant information by email to the nearest grocery store. In 2014, a hacked smart refrigerator sent unsolicited messages to routers, multimedia centers, smart TVs and other smart refrigerators. From December 23 to January 6, email messages were sent three times per day in batches of 100,000 in the first Internet of Things cyberattack. Such attacks have since become commonplace. To illustrate the gravity of the risk, a virus called Stuxnet was able to decommission uranium enrichment centrifuges with ease.

Virtually every industrialized nation is vulnerable to a “cyber Pearl Harbor” in which trains can be derailed, water supplies poisoned, and power grids crippled. It has been demonstrated with much publicity that any car or truck with an internet connection can be hacked by means of almost any WiFi-equipped device. An ominous threat is posed by drones with WiFi connections, capable of hacking and taking control of virtually any device, or infecting it with a cybervirus. Security researchers have revealed that medical devices, such as an insulin pump, can be hacked and the attacker can alter the dosage and schedule of the insulin release.

It has been predicted that, by 2020, 25 billion devices will be connected to the internet, and by 2025, a trillion. Already, there are 4.9 billion devices in the IoT, including smart home-automation devices, consumer products such as smart watches and health monitors, vehicles, and

smart infrastructure used in buildings and cities. Unfortunately, virtually any device that can be connected to the internet is vulnerable.

Security researchers discovered that a computer-controlled sniper rifle is vulnerable to cyberattack via its WiFi connections. The scope's calculations can be altered so that the shooter misses the target or shoots a different target. Software intruders can also disable the scope's computer or even prevent the weapon from firing. The shooter would not even be aware that the rifle had been hacked.

It has been established by security specialists that, by hacking a kitchen appliance, a hacker could penetrate an entire hotel, including its thermostats, garage door openers, automobiles, and offices. The hacker would then be able to attack the hotel chain and its bank and, thereby, the entire international banking system. It has been demonstrated repeatedly that an airplane in flight can be commandeered or sabotaged via its internet connections.

On a global level, the Internet of Things itself is threatened by the vulnerability of power grids to solar storms. The most powerful solar storms send coronal mass ejections (CMEs), containing charged particles, into space. If the earth happens to be in a CME's path, the charged particles are capable of disrupting satellites in orbit—or even causing them to fail—as well as disrupting telecommunications and navigation systems of high-flying aircraft. They have the potential to affect power grids, and have been known to black out entire cities, even entire regions.

Tourism and hospitality are especially susceptible to threats emanating from the Internet of Things. From reservation systems and databases to airplanes, trains, and automobiles, the risk of cyberattacks is no longer theorectical. Global Distribution Systems, hotel data systems, and airline operations both on the ground and in the air are attacked on a daily basis. Local and global airline disruptions, hotel chain piracy, and cybervirus penetration have become commonplace. Over one billion credit card accounts have been stolen from hospitality companies alone.

In the popular vernacular, the Internet of Things is widely acclaimed as "The Next Big Thing." As civilization becomes increasingly reliant on connective technologies, tourism, inexorably, will be "The Next Big Target." It is the nature of profit-based enterprises, including technology companies, to "race to the bottom," maximizing profits by minimizing costs. Conspicuously, the cost of designing and incorporating security safeguards against hacker attacks, sabotage, terrorism, and other inevitable hazards are routinely omitted in the design, engineering, and manufacturing of devices based on artificial intelligence.

Technology-related job losses in industrialized countries, unless mitigated by governments and employers, will result in extreme wealth inequality, spurring increased social upheaval, mass

migration, crime, and civil unrest. Increased dependence on technology will make civilization as a whole vulnerable to sudden collapse as a result of numerous causes, including sabotage, depletion of available resources, and adverse natural phenomena such as solar storms and climate events.

Conclusion

Thinking-machine chaos may already be inevitable. Most likely it will occur not as a sudden explosion of out-of-control autonomous devices, but as a phenomenon that makes its way into everyday life, much in the same methodical way that natural disasters resulting from climate change have now become commonplace. T. S. Elliot mused that the world will end "not with a bang but a whimper." Though overreliance on emergent technologies may not end the world, it will unavoidably complicate and challenge human existence.

Dennis L. Foster, Ed. D.