

Protecting Data Centers and Critical Infrastructure from Targeted Terrorist Attacks

It is widely recognized by the U.S. Department of Homeland Security, leaders in global infrastructure and security experts, that the impact of the terrorist events of September 11 could have been far worse if a coordinated attack against strategic Data Center and Communications Infrastructure hubs was perpetrated. In many cases, these data centers provide vital connectivity for command and control systems that are critical to incident management and post-event recovery. In fact, many people are unaware that the collapse of the former 7 World Trade Center building severely damaged Verizon's West Street Central Office (CO) which, in turn, either knocked out or affected New York City's 911 systems, the NYPD's critical lower Manhattan radio circuits and Headquarters Command Center, and a huge cross-section of voice and data circuits feeding surrounding buildings. Of these buildings, national assets such as the New York Stock Exchange, N.Y. City Hall and dozens of top-tier financial services firms were catastrophically affected by being logically isolated from public and private networks.

While the recovery and restoral efforts that were undertaken in the wake of the September 11 attacks allowed completely new data centers to be constructed, and data center assets to be relocated from certain known high risk areas, it highlighted the vulnerability to such potential data center and critical infrastructure failures. Although security precautions were upgraded and new procedures implemented, there remain many critical data center and critical infrastructure facilities globally vulnerable to the targeted terrorist threat.

Because there are many top-tier data center locations that play a critical role in keeping critical infrastructure operating for the flow of data to government and commercial enterprises, it is only a matter of time before terrorist efforts focus on U.S. and global data infrastructure with the priority to not only damage certain facilities but to disrupt data flow. Much of that targeted data flow disruption will be against the operations of the Blue Chip companies and the global financial system.

Terrorists of today understand that using explosive devices are not always the most effective means to achieve their goals. An alternative technique is to focus on debilitating the personnel who operate the large hubs and data centers knowing that even the most autonomous and redundant centers still require human interaction. The use of toxic industrial chemicals (TICs) or a radiological dirty bomb near the target will, in most cases, achieve the terrorists' goals. Chemical compounds, as plentiful and readily available as Chlorine, Hydrogen Cyanide or Arsine, are commonly accessible in the open market and can easily be weaponized using an aerosol carrying agent. Once weaponized, terrorists can identify street/low-level HVAC intakes and easily distribute the toxins through building ventilation systems. This is also the case with low grade nuclear material/waste that can be easily procured from hospital waste to nuclear age countries currently under siege through wartime efforts or internal civil war.

In the absence of a mechanical response to such a toxic release/attack, a building's HVAC system will continue to circulate these toxins without regard to the toxicity levels, loss of human life or saturation of such compounds within the structure. It's important to note that the likelihood of being a building target for terrorism increases directly in proportion to the importance and critical nature of the data and the infrastructure that uses that data.