Defentect
Intelligent Threat Awareness

Backgrounder

Radiological Dispersal Devices (RDDs)

A radiological dispersal device (RDD) or dirty bomb is recognized as a major terrorist threat. By wrapping a relatively small amount of radioactive material around a traditional explosive device and detonating it, terrorists can cause drastic psychological, sociological and economic destruction. Depending on the location of the attack, radiation cleanup costs could range from millions to billions of dollars. The quantities of radioactive material stored at commercial sites such as hospitals and irradiation facilities are more than enough to make a dirty bomb.

RDD Threat

The threat of a dirty bomb attack within the United States is real. In mid-August 2007, chatter regarding dirty bomb attacks against New York, Miami and Los Angeles prompted the City of New York to effectively shut down Manhattan in order to conduct sweeps. Police armed with hand-held radiation detection devices were stationed at checkpoints. When the threat passed, the checkpoints were removed. As a long-term solution, drawbacks to the effectiveness of this reactive approach are apparent.

If sixty to ninety Curies (Ci) of radiological material were stolen and detonated with conventional explosives, a major transportation hub or facility could be shut down for six months or more, according to recent Nuclear Regulatory Commission/Environmental Protection Agency rules outlining clean-up standards for severe attacks.

One estimate by the National Academy of Sciences places the costs for clean-up of dispersed radiological material in an attack to be as high as $100 billion. Bruce Blair, president of World Security Institute and the Center for Defense Information warns that even a low-tech dirty bomb using small amounts of dynamite and radioactive material probably would accomplish one of the chief goals of terrorism — creating widespread fear and panic. The National Academy of Sciences places estimates for the cost for cleanup of dispersed radiological material in an attack to be as high as $100 billion, with potential business interruption losses going as high as $1 trillion.

The threat posed by a dirty bomb attack is international in scope. According to a 2007 Canadian study led by Defence Research and Development Canada, the explosion of a small dirty bomb near Toronto's CN Tower would spew radioactivity over 4 square km, resulting in mass anxiety, a rush on Toronto's medical facilities and an economic toll of up to $23.5 billion.

The Nuclear Regulatory Commission noted in May 2002 that some 835 devices containing radioactive material disappeared around the nation over five years. The devices ranged widely in potency. Some elements, such as cobalt, emit gamma particles which can penetrate the skin, cause immediate cellular damage and, with sufficient exposure, death. Others are dangerous only if particles are inhaled and some are relatively benign.

The Department of Homeland Security believes key facilities are the likely targets of terrorist attacks and is investing in detection technologies. Until recent IP-based monitoring technologies were developed, it was impractical and labor-intensive to detect radiation in large public areas and facilities housing radioactive material. Under current Nuclear Regulatory Commission and Environmental Protection Agency rules outlining clean-up standards for severe attacks, the detonation of sixty to ninety Curies (Ci) of radiological material stolen from a hospital, combined with an explosive, would shut down a major transportation hub for a year or more.

CBRNE Threat Events

Chemical, Biological, Radiological, Nuclear, Explosive and other threat preparedness provides complex challenges to states and hospitals creating components of all hazards plans. Governments and health care systems need to prepare for and be able to respond to mass casualty incidents. Critical components of public health emergency preparedness strategies include the availability of tools to assist government agencies and healthcare facilities alike in emergency preparedness planning. Agencies, security personnel, first responders, government officials, health care system administrators and individual health care facilities need to include multiple threat detection systems in their assessments of preparedness planning. Multiple threat detection sensors can be integrated with DM3™ management, monitoring and messaging software, which is central to Defentect's solutions.

Defentect Solution

Defentect brings an important new technology to the fight against terrorism. Defentect DM3™ software provides an early warning alert system against terrorists preparing for a dirty bomb attack or the movement of threatening source materials. DM3™ is the proprietary software that connects broadly deployed radiation or other threat-event sensors to a server. When threat-level radioactive material is located, it sends alerts to existing monitoring stations and mobile clients. And Defentect's DM3™ is programmed to avoid innocent positives caused by low level radiation from medical treatments or naturally occurring radiation.

DM3™ is networked using IP and managed over the Web. When high-energy gamma rays from dirty bomb components interact with Defentect's Gammatect™ sensors, DM3's™ proprietary algorithms analyze the data and alert authorities to radiation that may pose a security threat. Communication features of DM3™ provide the ability to receive and process data over a network from the radiation sensor to the command center as well to PDAs, cellphones or pagers. The addition of strategically placed Gammatect Plus™ sensors enables Defentect to identify the isotope causing the radiation, providing control over false positive alarms.

Marketplace

Defentect recognizes a large demand both domestically and internationally in the private and public sectors for its intelligent threat awareness solutions. Over 100,000 domestic facilities are deemed critical infrastructure and potential targets by the Department of Homeland Security. RDD detection is an international concern and Defentect is in active discussions with prospective clients in Europe, the Middle East and Asia. The company is continually engaged in R&D and plans future enhancements to its products and the introduction of additional market offerings for chemical, biological, nuclear, explosive and other threat-event detection. Defentect sees the requirement for added protection in thousands of facilities across numerous market segments including - hospitals, chemical plants, food irradiation plants, research facilities, tunnels, truck stops, toll booths, seaports, borders, landmark buildings, power plants, train stations, airports, distribution centers, government buildings, military bases, courts, arenas, theme parks, malls,

stadiums, casinos, petroleum refineries, factories, utilities, highways, marinas, financial districts, etc.

For more information, please contact:

Defentect
Laura Wessner
Vice President of Corporate Development
P: 203-354-9164
lw@splinter.net

535 Connecticut Avenue
Norwalk, CT 06854
P: 203-354-9164
P: 888-868-8386
F: 800-536-1952
www.defentect.com
www.splinter.net