CYBER RECONNAISSANCE, an Expanding Threat to Homeland Security

By John Bumgarner

Almost monthly, police departments in major metropolitan areas receive tips about potential terrorist plotters scouting national monuments, office buildings or pieces of critical infrastructure for possible targets. Since 9/11, it has been purported that several possible attacks have been thwarted because the potential terrorists were using cameras or other obvious devices for their reconnaissance. What if these terrorists could do the same from the comfort of their computers?

The sad truth is that any terrorist with Internet access can conduct cyber-reconnaissance of thousands of potential targets anywhere within the boundaries of the United States, with only a limited possibility of being detected by any United States intelligence agency. The resources required to conduct virtual reconnaissance activities is available for free to anyone worldwide with access to an Internet-accessible computer.

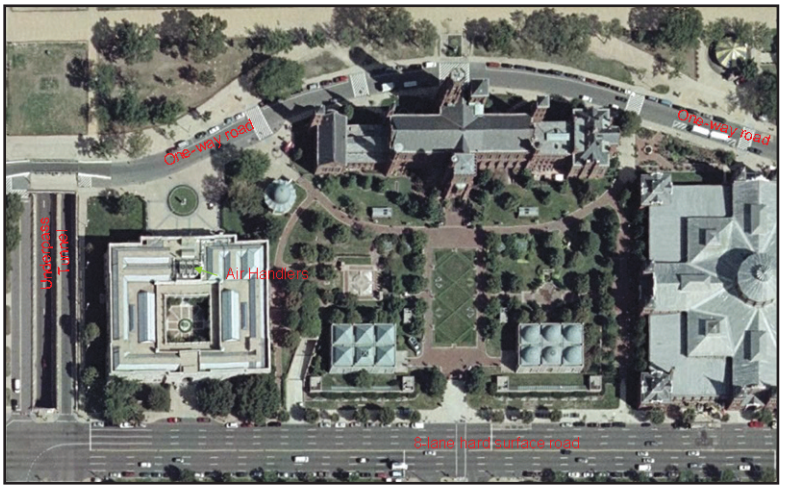

Figure 1 Google™ Earth image of a Smithsonian complex

The primary online resources that can be utilized to perform this reconnaissance are Google™ Earth and Microsoft® Virtual Earth™. Both of these applications allow anyone to analyze almost any point of interest within the United States using standard mapping and satellite imagery technologies. A potential attacker can use one of these applications to accomplish photo reconnaissance of a potential critical infrastructure target, without drawing unwanted attention to his research activities.

For example, figure 1 is a Google Earth image of a Smithsonian building in Washington, DC. This Google image provides the potential attacker with enough detail to make out the Smithsonian complex, including the paths between the buildings, air handlers on the roof of one building, deciduous trees, traffic patterns and a loading dock. If the adversary has more advanced photogrammetric, he can calculate the measurements of the target and even determine construction materials. Using basic targeting skills, an adversary can also identify ingress and egress routes to the target using either Google Earth or Microsoft Virtual Earth.

The national threat posed by cyber-reconnaissance is increasing due to newer applications, such as Google Street View and Microsoft Virtual Earth 3-D modeling capabilities. Since Google Street View is a new concept, it currently has limited coverage of about 15 large metropolitan areas in the United

States. Even though the coverage is limited, the cities included are some of the highest profile in the nation. The cites are: Chicago; Denver; Houston; Las Vegas; Los Angeles; Miami; New York; Orlando; Philadelphia; Phoenix Pittsburgh; Portland; San Diego; San Francisco and Tucson.

Using this technology an attacker could virtually drive the target's route, looking for potential choke points and other obstacles that could hinder the success of the attack. This cyber-reconnaissance could be conducted daily until the attacker has familiarized himself/herself with the target environment. Since this level of reconnaissance is performed in cyber space, it has little chance of ever alerting local or federal law enforcement officials.

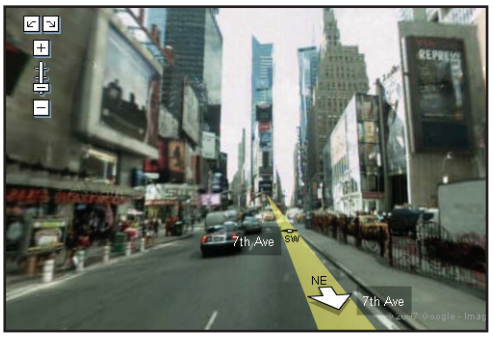

Figure 2 Google™ Street View in New York Time Square vicinity

Figure 2 below shows the Google Street View image located within the vicinity of New York Time Square. As you can see, the level of detail is usable for conducting street-level reconnaissance of a potential target's surroundings.

Another looming cyber-reconnaissance threat is posed by the 3-D modeling within both Google Earth and Microsoft Virtual Earth. These modeling techniques provide a potential attacker with the ability to perform a 360° reconnaissance of any physical target from all angles. Both applications also allow for the manipulation of a target's visual perspectives, which is useful in determining areas that have higher operational significance than others of lesser importance. Figure 3 below was produced using the 3-D rendering capabilities of Microsoft Virtual Earth.

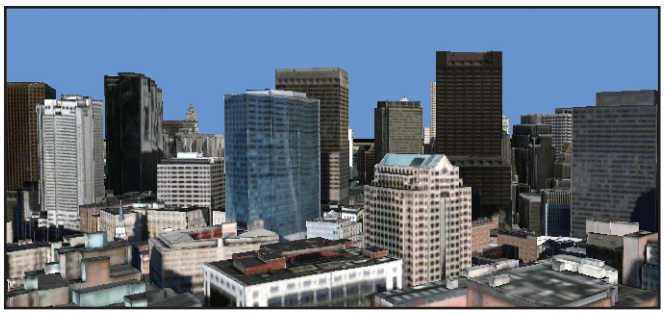
Figure 3 Microsoft® Virtual Earth™ 3-D of Boston

A potential attacker could use a 3-D model, like the one above of Boston, to study the impact of a chemical dispersion or a dirty bomb – a type of "radiological dispersal device" (RDD) that combines a conventional explosive, such as dynamite, with some form of radioactive material – on a densely populated target, based on building and street locations within the target environment. These 3-D models could also be incorporated into flight simulator applications, which could be used to simulate flight paths to the target.

Microsoft Virtual Earth currently has limited 3-D modeling of approximately 15 large metropolitan areas within the United States: Atlanta; Baltimore; Boston; Dallas; Denver; Detroit; Fort Worth; Houston; Las Vegas; Los Angeles; Philadelphia; Phoenix; San Francisco; San Jose and Seattle. Several of these cities also have Google Street View coverage.

Geo-tagged photos present another cyber-reconnaissance method that has gotten almost no coverage. This involves adding geographical information to items, photos and videos. The geographical information usually consists of latitude and longitude, but can also include items, such as altitude and place names. Normally geo-tagged photos are taken mostly by tourists and then added to various online sites for others to view. Most photos are taken within public locations, but some of those posted online are located on restricted military installations.

A potential attacker can use these geo-tagged photos to obtain an onsite perspective of the target from a precise location within close proximity of the target. The figure below is one of the hundreds of geo-tagged photos of surveillance systems within the Washington, D.C., area that have been posted to publicly accessible websites. Using this public information, an attacker could plot the known locations of surveillance systems along the route to their target.

A more sophisticated adversary could used the application programming interface (API) for either Google Earth or Microsoft Virtual Earth to constructed complex virtual models of the potential target environment from a safe house thousands of miles away. The geographical information created from these virtual targeting models could easily be plugged into a Global Positioning System (GPS) as waypoints – points of reference on earth. This information would allow any attacker to enter this country with a GPS device preloaded with targeting information. An attacker having this basic geographical information would greatly reduce his chances of getting lost on the wrong road during the execution of a mission.

Figure 4 Metro Police CCTV located on North Capitol Street in Washington, DC

As the capabilities of applications, such as Google Earth, Google Street View and Microsoft Virtual Earth, evolves, the potential for misuse of these applications increases. The looming question for our government and the vendors of these technologies is where the balance lies between national security and the general public's right to use this technology in a post-9/11 world.

John Bumgarner is Research Director for Security Technology at the U.S. Cyber Consequences Unit. ■