"How Vulnerable is your Airspace to Drone Intrusion?"

Whether it's your corporate campus, sports stadium, energy plant, public water supply or a glamourous outdoor Hampton's style event; the airspace above you is more vulnerable to a nefarious drone intrusion than you may think.

Think about it, in 2016 there were more than 2.4 million drones sold to the general public, and by the year 2020 it is projected there will be 6.2 million drones sold. While most people purchase drones for recreational or professional use, the utility of drones in criminal and corporate espionage activity is increasing significantly in all parts of the world. Security experts agree, even with huge access control investments on the ground, the airspace above presents itself as a significantly larger area of exposure.

Consider the average $500 Drone can travel at speeds in excess of 50 mph, it can climb up to 3,000 feet and it can carry a payload of up to 6 lbs. There are already multiple, documented occurrences of drone intrusions on airspace around nuclear power plants, prison facilities, political rally's, major sporting events, parades, and even the most protected piece of real estate in the world; **The White House**. On Monday, January 21, 2015 at 3:00 AM, a $500.00 unmanned drone crash landed on the front lawn of The White House. The unidentified operator was a male who was a U.S. intelligence agency employee, claiming he lost control of a borrowed personal quadcopter drone that he'd been flying around his apartment.
Again only 4 months later, on Thursday, May 14, 2015 the Secret Service had to detain a man who eyewitnesses reported, was trying to fly some sort of remote-controlled aerial device over the White House fence.

It’s easy to understand, given its speed capability, altitude and sophisticated video processing systems, a drone can penetrate the security of your airspace virtually undetected; obtaining video, taking photographs, eavesdropping, or causing willful destruction of property and other valuable assets. Now imagine, adding a payload onto a drone that can breach your airspace, deploy the payload, and be out of your airspace in 2 minutes or less.

A danger to both executives and corporations

The security industry has begun taking drones into account when it comes to providing protection. The threat and collateral damage of a Drone attack is similar to that of an active shooter or a vehicular attack in that they both can easily cause mass casualties and injure as many people as possible unless stopped. Subsequently, the use of a drone in this fashion would have multiple opportunities to seek out the most target rich environment to cause damage.

The threats are too credible to be ignored: we've seen a drone land right in front of German Chancellor Merkel during a 2013 campaign event. Drones also photographed Tina Turner's wedding. In January 2014, a U.S. senator publicly spoke about a drone that peeked into the window of her home. The list of incidents where drones have ventured into airspace is long and still growing quite aggressively as individuals find more nefarious uses for a drone. People can fly model airplanes without restriction, but it is illegal to operate a drone as a civilian above 400 feet and beyond line of sight for any commercial reason unless they have received permission from the Federal Aviation Administration. Some experimentation in taking a drone apart revealed that most ready-to-ship drones come with the same electronics as a smartphone or tablet. Nearly all drone code is the same as that found in Android except for open-source coding efforts built on Linux platforms. Onboard cameras are capable of storing video — anywhere from five minutes to two hours of video on a USB stick. Some advanced operating systems allow for real-time upload of video to external storage networks. Even the cheapest drones have fully operational Wi-Fi, radio frequency and Bluetooth antennas or a combination of all three.

Corporate campus's and other large foot-print facilities are easy soft targets for drone intrusion, and could be vulnerable to more collateral damage then they realize. If you consider the infrastructure value of a company's world headquarters and the vast amount of proprietary information within that facility—think of a drones' ability to compromise the safety and security of that corporate campus—especially a pharmaceutical or chemical campus. There have been well documented incidents where an intrusion drone breached the airspace of a major energy provider and caused massive disruption of a power grid. In other situations, intrusion drones have been found on roof-tops of facilities attempting to hack into corporate IT systems, and they have also been found surveilling a corporate campus.

Celebrities, public figures and executives can be surveilled from the air, which means that their activities and movements can be tracked in real-time. This is not only a huge security risk, but also a breach of privacy. When it comes to corporate and industrial espionage, nefarious entities may utilize drones to obtain video footage and audio recordings, since many drones are equipped with HD cameras, infrared cameras, or long-range microphones. Sensitive locations (clients' residences, private properties, offices, stadiums, public venues, etc.) can be surveilled by drones to collect critical intelligence, which could reveal vulnerabilities and potential gaps in the security arrangement and leave a site vulnerable to attacks.

Assess the vulnerability of your airspace

Sensitive sites across the United States are vulnerable to attack by store-bought drones, according to a new assessment by the Department of Homeland Security office in charge of sharing threat information with first-line personnel. The DHS "intelligence assessment" does not cite any actual or known drone-related threats within the U.S. homeland, but it cites several recent instances overseas when terrorist groups and criminal organizations used drones "to support illicit or violent activities." Corporations and other operating entities spend a tremendous amount of money and resources to make their physical security as tight as possible to insure unauthorized access. Naturally, the size of the company determines its total security spend. The median spending on physical security at firms with less than $10 million in annual revenue is $337,000, while it tops $1 million at firms with more than $1 billion in annual revenue. Companies will now be required to re-allocate budgets to allow for some form of air-space intrusion monitoring, before this however, a thorough air-space vulnerability study should be initiated. Similar to conducting a typical facility security and vulnerability assessment, you would now focus on the space above your facility, and its surroundings.

The K Street Group had previously developed a proprietary, quantitative tool to rate a facilities overall security capability—K Street Group has revised the model somewhat to allow for its utilization in airspace vulnerability assessments. The example below shows specific attributes that define what makes the airspace above a facility vulnerable to a drone intrusion. Typically, we focus on no more than 4-6 vulnerability attributes, and apply a weight to each depending on importance. Each vulnerability attribute is then scored based on the findings of the assessment. The model then generates a numerical score, as you can see in the example below; 34.7 out of 100, which is basically a highly vulnerable facility. Based on thousands of data points over 5 years, we have found that any score at 65 or above is adequate, and certainly the higher the number the more secure the facility.

AirSpace Risk Assessment and Vulnerability Model					
Vulnerability Attributes	**Weight**	**Score**	**Preference**	**Ratio**	**Effectiveness Score**
Campus size	25	7.0	9	0.7778	19.4
Critical Infrastructure Housing	10	1.0	8.0	0.13	1.3
C-Suite location	15	1.0	8.0	0.13	1.9
Proximity to residential area	15	2.0	8.0	0.25	3.8
Security Presence/Visibility	20	3.0	9.0	0.33	6.7
Airspace Intrusion Detection	15	1.0	9.0	0.11	1.67
Total	**100**	**15.0**	**51**		**34.7**

Contact The K Street Group now to schedule a confidential risk and vulnerability assessment discussion to improve the overall safety and security of your facility.

The K Street Group, LLC
1220 State Route 31, Suite 15
Lebanon, NJ 08833
(Office) 908.200.7344
(Fax) 908.200.7346
(Website) www.kstreetgroupsecurity.com
(Email) baromando@kstreetassociates.org