Drone Emergency Response: A Planning System for Critical Infrastructure

Bill Edwards[1]

Abstract:

This study considers the infrastructure effects of drone attacks. After reviewing the methods and risks of drone attacks, this article proposes a planning system to protect critical infrastructure. Public events are also considered as an extension of this methodology.

Keywords: *Drone emergency response, infrastructure security, coordinated drone attacks*

THE KINGDOM OF SAUDI ARABIA AWOKE on September 14, 2019, to the alarming news that its largest oil-producing facilities had been attacked and were quickly downgraded to 50% operational capability. The world watched as an estimated 5% of the world's oil capacity burned (Safi and Wearden, 2019). These attacks, in addition to being a tragedy, were also an enormous wake-up call regarding the use of drones and drone swarms in attacks on critical infrastructure. It sends a message that the use of unmanned aerial vehicles (UAVs) and current drone technologies represents a severe threat that governments and security professionals should take seriously.

Those responsible for the attack are only doing what a determined enemy always does in a protracted conflict against another military power—using whatever tools possible to give them parity. The use of inexpensive drone technology accomplishes this. The technological evolution of drones and a drone's use of highly sophisticated state-of-the-art functions, including autonomous flight, proximity sensing, geo-location, and extended attack distances, means creative planning and counter-drone solutions are needed for immediate deployment and execution.

Additionally, UAVs can operate from extended distances, carry larger payloads, and in some instances fly in elevations that easily allow for "under the radar" realities. Furthermore, proximity sensing and global positioning sensors allow for swarm tactics to take shape as they did in this reported combined missile and UAV (drone) attack.

The technologies associated with this type of strike and the use of drone platforms will only continue to evolve. Therefore, understanding the nature of the threat landscape is vital to preparing for and executing a Drone Threat and Vulnerability Risk Assessment (DVRA) and a Drone Emergency Response Plan (DERP). These two processes represent the focus of this article.

[1] Bill Edwards is an Associate Principal of protective design and security at Thornton Tomasetti and can be reached at BEdwards@thorntontomasetti.com. He is responsible for planning, coordinating, resourcing and building operational/technical security services across a range of project types. Bill and his team are experts in counter-terrorism, counter-theft, cybersecurity, electronic security, and physical security and provide customized solutions to protect clients' critical assets and investments.

1. DVRA and DERP

DVRA and DERP are processes and methods that give security professionals at the planning and operations levels a way to view the threat and develop proper reactions when an event occurs. They also provide a methodology to combine a proactive and predictive posture to any security situation. It is important to note that combined human and technological solutions are needed to ensure that a comprehensive, layered and integrated approach is taken to mitigate risk and limit the physical harm and damage to people and facilities.

The DVRA is the foundation and consists of a detailed threat analysis, UAV and commercial drone capability review, identification of critical assets, vulnerabilities of those assets and risk mitigation recommendations and measures that could be implanted to "buy down the risk." This includes an understanding of UAV and commercial drone capabilities, layered zones of interest, a defense in depth mindset, mutual aid agreements and partnerships, and knowledge of applicable laws and regulations that support a comprehensive plan. Additionally, a thorough understanding of critical assets is necessary to achieve a targeted use of resources in situations where drones are a threat, but only one of many, in a complex security environment. Lastly, the ability to employ technology to detect, monitor, interdict and even destroy must be considered important courses of action depending on the Special Event Assessment Rating (SEAR) level in the U.S. or its equivalent outside of the U.S.

The DERP should at a minimum address the following key elements from a framework perspective:

1. *Identify the area you will defend.* Assess the site and the surrounding area and identify critical assets. Essentially, this is where you set physical boundaries in depth around the Restricted Area that is intended to be protected. At a minimum, there should be a detection zone, a no-fly zone, and a restricted area. In order to accomplish this, a clear understanding of approach routes and most likely flight patterns is needed. Additionally, RF or a combination of RF and Radar sensors can provide the standoff needed for detection and proactive response.

2. *Form response teams and identify their functions and reporting procedures.* Define response team expectations during an event. This is initially an organizational task that helps to provide an operational response. Response teams assist in the overall security plan during events. They are trained to understand the necessary action to take when a threat arises. An example may be as simple as executing shelter-in-place instructions to event participants or helping to provide orderly evacuation on designated routes. Response teams help large venues secure space in manageable increments. This also applies to drone detection, as response teams can have designated areas to observe that help with providing early warning. If organized, trained and exercised on a regular basis, response teams are a security force multiplier across a myriad of events.

3. *Identify laws and regulations that limit the effect of the plan.* Current laws with regard to drone detection and monitoring in the U.S. are still maturing and do not allow for disrupting a drone's flight unless it is determined a threat over critical infrastructure or Department of Defense facilities. As the commercial drone market continues to expand and grow, it is important for security professionals to understand their limits of response. Additionally, as cybersecurity concerns grow with drone usage, a general

understanding of the recently published European GDPR (2018) and California's CCPA (2020) should be considered with any drone response plan as it pertains to data and personal privacy (Umhoefer and Shpiro, 2019).

4. *Identify zones of interest and influence, and develop a listening and observation post (LP/OP) array for deployment.* Essentially, this is an added layer of defense with regard to the DERP. As mentioned previously, a layered approach to drone detection includes the use of RF and Radar technologies, but it is also important to think in terms of physical audio and optical posts connected via dedicated communications that allow for real-time reporting as an additional measure of proactive planning and response. LP/OP's are an effective way to extend the perimeter of the restricted/protected space during an event.

5. *Develop reporting standards and templates, such as the technological package to be deployed and operations center standard operating procedures.* This is an important step within the DERP. Synchronizing reporting templates, communication packages, and security operation center (SOC) actions is critical for emergency response planning and action. Typically, simplifying how a report is formatted and sent to the SOC is the first step. Publishing a Size, Activity, Location and Time (SALT) report is an ideal way to extend the drone perimeter and is easily communicated to the SOC for a response. It is also important to clearly determine how communications are set-up and executed. Ideally, as technology advances, security directors should have their own private LTE network that goes beyond the facility's WiFi architecture. This would allow for stability in the secure communications network and would negate using the system that is used by staff and guests during events. Redundancy with regard to communications is also key and establishing a Primary, Alternate, Contingency and Emergency (PACE) communication standard is a critical function for the overall security posture. Additionally, InfraGard members, at the time of writing, have access to GETS (Government Emergency Telecommunications Service) and Wireless Priority Service (WPS).

6. *Formulate individual munitions, biohazard, chemical response plans and organize quick reaction forces, communications plans, medical and HAZMAT response planning.* These plans are appendices to the DERP. Simply stated, each area should have its own emphasis and tie directly into the overarching plan. The keys to successful appendices are external support, points of contact and consistent training with local first responders. Additionally, understanding federal support in these areas is essential. Local exercises should be conducted quarterly and annually with federal entities. The Center for Disease Control (CDC) provides a simple template as an example of how to tailor to the DERP (Center for Disease Control, 2020).

7. *Develop evacuation plans.* Identify ingress and egress routes by both land and air, and develop lockdown and shelter in place procedures. Emergency response planning should include triggers for potential evacuation or shelter-in-place decisions. In the case of a kinetic drone threat, security directors will need to establish when to evacuate and when to shelter-in-place. As we saw with the attacks during the Paris soccer match

between France and Germany the situation was nebulous as players, fans and staff were confused about what to do (Borden, 2015). This scenario is all too common in large-scale public events. In the event of a drone threat in the US, such as the one in the Bay Area during NFL games, leaflets dropped from a drone could easily have been ordnance or a chemical (The Seattle Times, 2017). Preparing security personnel and staff on these actions is another important step with regard to DERP development.

8. *Stock emergency supplies, such as water, food and medical.* Specifically, stock emergency supplies for a shelter-in-place event that may require a large crowd to remain in a place for an extended period of time.

9. *Coordinate with local public support agencies and emergency services.* Coordination with relevant government agencies should be a standard within all steps for DERP where applicable. Leveraging external support outside of the venue or facility is a smart way to extend the security program's effectiveness and depth.

10. *Consider cyber implications and protect crucial data and information.* Cybersecurity assessments are an important subset of the DVRA and should be considered as a standard for identifying vulnerabilities to critical assets. The IoT is a major contributing factor to all of the functions of modern facilities in particular life systems (power, water, and HVAC) that are of critical importance to secure (CDW, 2019).

11. *Establish business continuity options/plans and form mutual aid agreements for support.* The DVRA and DERP provide solid foundations for the development of business continuity plans (BCP). How a business maintains functional capability after an event is critical to its survival. BCP along with mutual aid agreements help to keep a business viable. A subset of BCP is continuity of operations (COOP) actions such as training and exercises for off-site relocation to maintain the business's momentum.

Security professionals need to better understand these threats and have the capability to advise the public. Kinetic attacks using drones are only the beginning. In the near future, complex cyber attacks will emerge from these platforms and critical data will be freely exploitable in everyday life. Combing kinetic and cyber attacks will present a formidable challenge that requires inventive security solutions. The increase in these types of attacks based on successful events such as the recent attacks in Saudi Arabia will promulgate further among nefarious groups and individuals. The growth of these types of scenarios will be very similar to what we've already seen with hostile vehicle attacks and active shooter events.

Simply put, drone attacks are another way for terrorists to grab the media's attention and send a message that no one is safe. Drone technology should be taken very seriously and approached in a manner similar to how the world has reacted to vulnerabilities in the cyber domain. There is no way around this. Drones and their use as weapons of disruption and destruction are here to stay.

References

Safi, M. and G. Wearden, "Everything you need to know about the Saudi Arabia oil attacks", *The Guardian*, September 16, 2019, https://www.theguardian.com/world/2019/sep/16/saudi-arabia-oil-attacks-everything-you-need-to-know.

Umhoefer, Carol and Shpiro, Tracy, "CCPA vs. GDPR: the same only different", DLA Piper, April 11, 2019, https://www.dlapiper.com/en/us/insights/publications/2019/04/ipt-news-q1-2019/ccpa-vs-gdpr/

CDC, "Emergency Action Plan (Template), Center for Disease Control, Accessed on January 4, 2020, https://www.cdc.gov/niosh/docs/2004-101/emrgact/emrgact.pdf

Borden, Sam, "As Paris Attacks Unfolded, Players and Fans at Soccer Stadium Remained Unaware", The New York Times, November 14, 2015, https://www.nytimes.com/2015/11/15/world/europe/stade-de-france-paris-soccer.html

The Seattle Times, "Leaflets dropped over NFL games revive concerns about drones", The Seattle Times, November 27, 2017, https://www.seattletimes.com/nation-world/drone-pilot-arrested-for-dropping-leaflets-over-nfl-games/.

CDW, "What is the Internet of Things (IoT)", Tech Tips, January 24, 2019, https://www.cdw.com/content/cdw/en/articles/networking/2019/01/24/what-is-the-internet-of-things.html