BLACK ROSE TECHNOLOGY

BRT-9-W-22-0008

2022

IRANIAN PJAK DRONE STRIKES: 2022-11-21

ANALYSIS OF SUSPECTED IRANIAN DRONE STRIKES ON PJAK FACILITIES IN THE SEMI-AUTONOMOUS KURDISH REGION SHORTLY AFTER MIDNIGHT ON 2022-11-21.

Title	Iranian PJAK Drone Strikes: 2022-11-21
Document Number	BRT-9-W-22-0008
Revision	0
Date Created	2022-11-24
Last Modification	2022-11-30
Author	David Gessel
Checked by	DJG

IRANIAN PJAK DRONE STRIKES: 2022-11-21

On the night of 2022-11-21, shortly after midnight, two synchronized attacks on reported PJAK (PDKI) facilities in Jazhnikan/Jejnikan (جەژنیکان) (near Erbil, verified POI 36.342596° N, 44.006713° E) and Koya (کۆیە) (reported POI 36.064012° N, 44.604222° E) were reported by the media[1] and on twitter[2][3]. The PJAK base in Koya has been a reported target on previous occasions[4] and that region of the KRG has been subject to multiple attacks recently[5].

1 REPORTED DETAILS

The Koya attack modality appears to have been fairly standard: a combination of suicide drones and theater ballistic missiles reportedly launched from the Hamza Sayyid al-Shuhada base of the Islamic Revolutionary Guard Corps.[6] The approximate flight distance to Jazhnikan is roughly 170 km, to Koya roughly 185 km.

Note: Володимир Зеленський (Zelensky) shown for scale only, the Iraqi attacks of 2022-11-21 had nothing to do with Ukraine.

At least some reports[7] indicate that the attack on Jazhnikan were carried out with a Shahed-136 drone[8] (شاهد ١٣٦). Media reports are fairly consistent in describing the drones as "suicide" and the audio from the two Jazhnikan videos has a clear sound of a gas engine up to but not detectable past the explosion that correlates with the loss of electricity. The reported drone type used and the result of the attack (disruption of electrical service) is highly reminiscent of recently evolved Russian tactics in Ukraine.

Reports indicate the target was the transformer feeding the village of Jazhnikan, which was stored inside a building and not visible from the air or the street. Accepting these reports as representative of mission intent, the necessary targeting accuracy (1–2 m CEP) is meaningfully higher than civilian GPS-based targeting achieves, generally reported as yielding a CEP of 5–15 m. Differential GPS can improve this accuracy by as much as 10[3], but this requires precision located ground transmitters to detect and transmit a differential error code, something unlikely to be deployed in Iraq by Iran. Military receivers that can decode the P-code (or newer M-code[9]) should be able to target with the required accuracy on GPS alone (~1 m CEP), but such decoders are unlikely to be deployed by Iran. Russia may have provided official support for GLONASS high precision decode, but even that signal yields at best 3 m accuracy.

A few key unvalidated assumptions are integral to the premise that the attack relied on high precision targeting including:

- That the destruction of a specific transformer was the mission plan,

- That the success of that plan was attributable to something other than luck.

Neither of these are known to be true, however the attack did hit and disable a small target inside a structure with a drone (likely suicide, but possibly a ground-attack drone).

2 BETTER THAN GPS TARGETING

Ground evidence provided by Dari Concepts[2] indicates one of the two drone strikes that hit Jazhnikan struck the west facing wall of the structure shown above about 1m above ground level and destroyed the villiage transfomer located therein.

This implies both local intelligence sources (as the location of the transformer inside the structure is not apparent remotely) and either anomalously high targeting accuracy or a mission planned with a very low probability of success; the targeting accuracy implied, on the order of 1–2 m CEP, is not achievable with uncorrected GPS. Typical methods of enhanced drone targeting other than differential GPS include:

- **Laser designators:** a forward observer paints the target with a laser designator so that a steerable munition can easily find the target and correct any deviations. This is a well-proven technique that relies on relatively simple electronics and optics, but requires a forward observer with a laser designator within line-of-sight of the target, a high risk assignment.

- **Vision-based final approach:** modern systems would typically implement a deep-learning AI system—either programmed to autonomously and locally (within the drone's control system) recognize a type of feature, such as a vehicle or person, and target it or to seek a visual match to an image taken of the target with reference fiduciaries.

- **Live Video over Air to Ground radio link:** to carry a camera image or other targeting data stream to a human controller to provide final guidance to the target. Such links can operate over as much as a few hundred kilometers in ideal circumstances, but are generally limited not by RF range, but line of sight.

- **Live Video over Air to Satellite radio link:** to carry camera imagery to a remote location. This is standard for US drone strikes and other countries as well, but absolutely requires sufficient satellite coverage and the aircraft end of the link is also somewhat pricey. Starlink[2] and other commercial, high speed, low-latency satellite data services

should enable non-state armed insurgent groups access to this advanced technology, heretofore limited to space-faring nation-states.

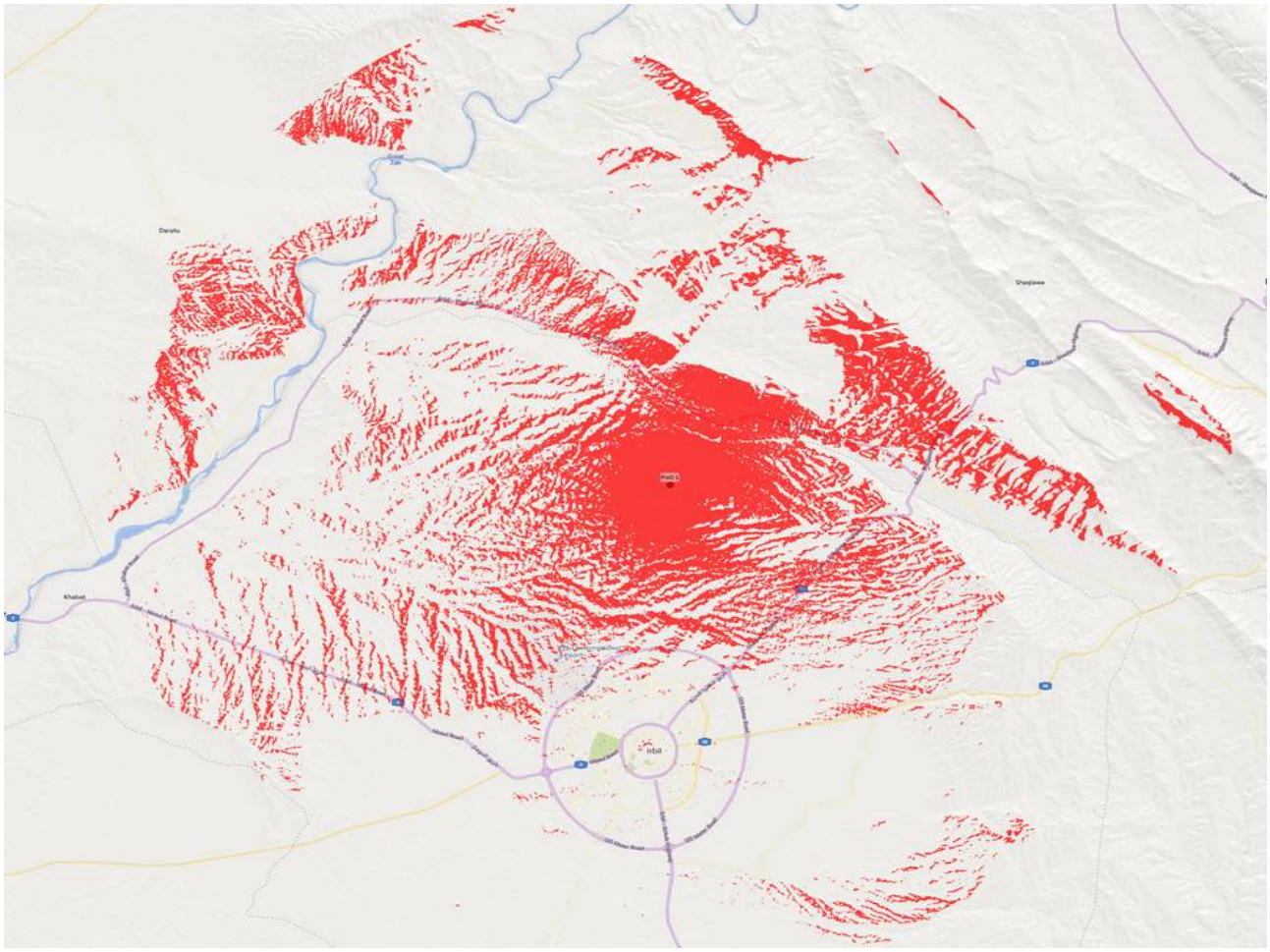
- **Live Video over Cellular link:** with sufficient bandwidth (4G LTE or above, generally) can bridge drone communications to the internet and provide "control from anywhere in the world" capacity for live final control. This technology is already within reach of non-state armed insurgent groups (control hardware can be had for $2,500[2]), though many of the operating areas (such as Iraq) have limited 4G coverage.

- **Live Video over Consumer Link (WiFi):** Low cost hardware is amenable to simple modifications for gravity drop munitions which can be accurately targeted[2] over the standard OEM control links provided in most consumer drone packages for precise delivery, but with significant drawbacks including requiring a ground controller within line of sight and typically within 1–3 km, vertical drop final flight paths, and loitering over the target during target acquisition.

2.1 AIR TO GROUND LINKS

In general, point to point radio links, such as ground to drone RF controllers, are limited by the shorter of either the maximum usable range of the link or line of sight. In flat, open terrain, RF signal strength is the primary limitation, and ranges from a few kilometers for consumer hardware to hundreds of kilometers for military hardware.

In many regions line of sight and ground clutter will limit control range well before RF link strength will drop below usable limits. We can perform an viewshed analysis of line of sight from the POI in Jazhnikan assuming a drone operating at 200 m elevation communicating to a ground controller with a 10 m mast using software from Cambium Networks[2].



This analysis is limited by the software used to a range of 30 km but clearly shows that line of sight considerations would drive ground control site selection to a limited set of options increasing operator risk.

2.2 SATELLITE LINKS

Iran is a space-faring nation and has successfully launched a number of communications satellites, two of which are currently reported as live: Noor-2 (NORAD ID: 51954[2]) and the Khayyam (NORAD ID: 53370[2]), which was launched just 105 days before the attack. Of the two, the Khayyam was within range (being somewhat generous to the term) during the approximate reported attack window for about 7 minutes per In-The-Sky.org[2].

Time	Khayyam Latitude	Khayyam Longitude	Elevation at Jazhnikan	Range from Jazhnikan	Elevation at Koya	Range from Koya
00:29	55.1 N	34.2 E	2°	2350 km	1°	2391 km
00:30	51.4 N	32.5 E	5°	2037 km	5°	1999 km
00:33	40.2 N	28.7 E	12°	1533 km	11°	1591 km
00:36	28.9 N	25.7 E	5°	2017 km	5°	2058 km
00:37	25.1 N	24.9 E	2°	2327 km	1°	2361 km

This analysis suggests that with very careful timing, it would have been at least theoretically possible to preposition a drone to visual standoff using GPS and await a satellite link for final targeting via remote video.

Given that remote satellite links to drones are the standard method by which US drones are piloted, it is reasonable to consider the possibility that Iran might do the same, however this analysis makes it clear that military operations benefit greatly from more continuous satellite coverage as would be provided by Starlink or similar LEO direct-to-consumer satellite internet offerings as they come on-line and become widely available.

3 CONCLUSION

While the strike at Jazhnikan appears to have demonstrated accuracy not reliably achievable with simple GPS guidance, concluding that the operation must therefore have implemented more advanced final control mechanisms is not well supported by the limited evidence.

The event does offer an appropriate moment to consider the inexorably advancing military capabilities that consumer technology enables and the degree to which such capabilities tend to destabilize historical power structures that rely on structural capacity asymmetries between wealthy and poor nations or, somewhat more alarmingly, between nation states and non-state armed insurgent groups.

Globally dominant militaries have for more than a century relied on a combination of great wealth and exceptional innovation to establish air superiority, intelligence superiority, and communications superiority to achieve battlefield dominance. The war in Ukraine is the first real test of consumer and "insurgent" military technology being engaged as coequal partner with tier one nation state military capabilities demonstrated by both in Ukraine's Aerorozvidka units and Russia's use of the Герань-2 alongside multi-million dollar hypersonic missiles and yielding nominally equivalent results.

It is clear that we are entering an era where even poorly funded non-state armed insurgent groups will have access to extremely effective munitions capable of reaching deep inside even actively protected territory with deadly precision and the capability of doing extensive damage to critical infrastructure of a scale that might be destabilizing at a cost well below levels that are easily tracked with equipment that is not easily subject to proliferation controls.

This highly asymmetric transition is legitimately disruptive and warrants significant investment in re-symmetrizing technology.