



The Impact of an Autonomous Drone System in Providing Security for the Satish Dhawan Space Centre (SHAR), Andhra Pradesh

Geda Kyathi Sri¹, Dr. Thota Chandrasekhar Yadav²

¹ 2400560144

kyathisrigeda1205@gmail.com

Department of Management, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India

² KL Business School, Koneru Lakshmaiah Education Foundation (KLEF), Green Fields Campus, Guntur District, Andhra Pradesh, India.

handrasekharyadav.t@gmail.com

ORCID: 0009-0001-4694-9954

ABSTRACT :

Autonomous drones are increasingly considered for guarding large, sensitive and hard-to-patrol installations. This pilot study examines how stakeholders of the Satish Dhawan Space Centre (SHAR), Sriharikota, Andhra Pradesh, perceive the potential of an autonomous drone system to strengthen security at the spaceport. The study combines secondary data (published literature, a parliamentary reply, official drone regulations and news reports on SHAR) with primary data collected through an online structured questionnaire from 43 respondents, comprising employees, local residents, a security professional and other stakeholders, using convenience sampling. Responses were analysed with descriptive statistics, Cronbach's alpha, one-sample t and Wilcoxon signed-rank tests, Spearman correlation, the Kruskal–Wallis and Mann–Whitney U tests and chi-square goodness-of-fit tests. 65.1% of respondents agreed or strongly agreed that autonomous drones could significantly improve security at SHAR, and 74.4% agreed that drones could improve monitoring of restricted areas. The composite Drone Security Perception Index (mean = 3.33 on a 5-point scale; Cronbach's alpha = 0.79) was significantly above the neutral midpoint ($t(41) = 3.29$, $p = 0.002$). Perception did not differ significantly by familiarity with drone technology, respondent role, or concern about hacking. Adverse weather was the most frequently cited implementation challenge (34.1%), 72.1% favoured constant human supervision, and 51.2% were concerned about cyber-attacks. The findings indicate conditional optimism and support a phased, human-supervised, cyber-secured pilot deployment. Because of the small non-probability sample, the results are indicative rather than generalisable.

Key words: *Autonomous drones; Unmanned aerial vehicles; Security surveillance; Critical infrastructure; SHAR; Sriharikota; Perception study; Pilot study*

Introduction of the Study

1.1 Background of the study

Unmanned aerial vehicles (UAVs), commonly called drones, have moved from military use into a wide range of civil applications such as real-time monitoring, infrastructure inspection, search and rescue, and security and surveillance (Shakhatreh et al., 2019). Their appeal for security work is practical: an aerial platform can observe terrain that is slow, costly or risky for personnel to cover on foot or by vehicle. When a drone can also fly a stored route, sense its surroundings and send alerts with limited human input, it is described as an autonomous drone system, and this capability is what makes continuous or scheduled patrolling of very large sites conceivable.

The Satish Dhawan Space Centre (SDSC SHAR) at Sriharikota is India's spaceport and one of the lead centres of the Indian Space Research Organisation. The site is a spindle-shaped island in Tirupati district of Andhra Pradesh, lying between the Pulicat Lake backwater and the Bay of Bengal; it covers about 175 square kilometres with a coastline of about 50 kilometres (IANS, 2025). Such a large, water-bound and strategically important installation presents a demanding surveillance problem. Public information indicates that its protection already rests on layered arrangements on land and along the coast (Rajya Sabha, 2014), and recent readiness exercises and a hoax threat in 2025 show that security agencies treat the site as a high-priority asset (Press Trust of India, 2025; IANS, 2025). Table 1 summarises the secondary information used in this study.

Table 1: Secondary data on the setting, security arrangements and regulatory context of SHAR

Attribute	Details reported in the sources	Source
Location	Island in Tirupati district, Andhra Pradesh, between Pulicat Lake and the Bay of Bengal; Buckingham Canal on the western side	IANS (2025)
Size	About 175 sq. km of area; coastline of about 50 km	IANS (2025)

Attribute	Details reported in the sources	Source
History	Site chosen in 1969 and operational from 1971; named Satish Dhawan Space Centre, SHAR on 5 September 2002	IANs (2025); ISRO (2002)
Land-side security (as reported to Parliament)	Double-layer concertina coil on the outer boundary, followed by a power fence and CCTV; access control at critical installations; vehicle surveillance and visitor management; authentication at entry points	Rajya Sabha (2014)
Sea-side security (as reported to Parliament)	CISF watch tower and outposts on the beach, foot and boat patrolling along the shore; additional coverage by the Marine Police of Andhra Pradesh	Rajya Sabha (2014)
Recent readiness events	Mock drill on 10 May 2025 testing preparedness, coordination and response time; hoax bomb-threat call on 16 June 2025 that triggered large-scale searches by CISF, district police and the Coast Guard	Press Trust of India (2025); IANS (2025)
Drone regulation	Drone Rules, 2021 notified on 25 August 2021; airspace divided into green, yellow and red zones; prior permission needed in yellow and red zones; rules do not apply to UAS used by the naval, military or air forces	Ministry of Civil Aviation (2021)

Note: The parliamentary reply dates from 2014, so present arrangements may differ from those described.

Against this background, the present pilot study asks a simple question: do people connected with SHAR believe that an autonomous drone system could make a meaningful contribution to its security, and what reservations do they hold? Understanding stakeholder perception is a sensible first step before any technical trial, because acceptance, perceived usefulness and concern about risks shape whether a technology is adopted and used well.

1.2 Review of Literature

1.2.1 Drones for civil security and surveillance

Shakhatreh et al. (2019) surveyed civil UAV applications and identified security and surveillance among the fast-growing areas, noting that smart UAVs promise reduced risk and lower cost in civil infrastructure work. The same review lists charging, collision avoidance, swarming, networking and security as the main open challenges. Motlagh, Taleb and Arouk (2016) reviewed low-altitude UAV-based Internet of Things services, which frame the drone as a flying platform that carries sensors and communicates with ground systems. Kim, Mokdad and Ben-Othman (2018) discussed the design of UAV surveillance frameworks for smart cities and extensive ocean areas, a pairing of urban and maritime concerns that is relevant to a coastal installation such as SHAR.

1.2.2 Real-time sensing and edge processing

Motlagh, Bagaa and Taleb (2017) proposed a UAV-based IoT platform and demonstrated a crowd-surveillance use case built on face recognition. Their testbed compared processing video on board the drone with offloading it to a mobile edge computing node, and reported that offloading conserved the drone's limited energy, shortened recognition time and supported prompt detection of suspicious persons. This work is useful for the present study because it links two of the survey themes, real-time alerts and data-processing capability, to measurable system performance.

1.2.3 Cyber-security and vulnerability of drone systems

A parallel body of work warns that drones are themselves targets. Yaacoub, Noura, Salman and Chehab (2020) analysed attacks on drone systems, examined vulnerabilities in communication links and connected devices, and described experiments in which a drone was detected, intercepted and hijacked through de-authentication or jamming, which they took to show how readily communication channels can be compromised. Abualnaja, Javed and Alasmay (2019) and Mekdad et al. (2023) also surveyed security and privacy issues of UAVs. For a facility with sensitive assets, these studies imply that the protection of communication links, data and control access is a design requirement rather than an optional extra.

1.2.4 Regulatory and site context in India

In India, civil drone operations are governed by the Drone Rules, 2021, notified by the Ministry of Civil Aviation on 25 August 2021 (Ministry of Civil Aviation, 2021). The rules classify airspace into green, yellow and red zones on an airspace map published on the Digital Sky platform, and require prior permission for operations in yellow and red zones. They do not apply to unmanned aircraft used by the naval, military or air forces. Any drone-based security system at a space launch range would therefore have to be planned with airspace permissions and the competent security authorities in mind. On the site itself, the reply given in Parliament described a multilayer arrangement of fencing, CCTV, access control and coastal patrolling (Rajya Sabha, 2014), while news reports of the 2025 mock drill and hoax call show the range of agencies that respond to a threat (Press Trust of India, 2025; IANS, 2025).

1.2.5 Synthesis

Taken together, the literature shows that drones can extend observation, that real-time sensing and edge processing improve responsiveness, that the systems bring their own cyber risks, and that deployment depends on regulation and on integration with existing security layers. What the reviewed

sources do not provide evidence on how the people connected with a specific Indian space installation view these possibilities.

Research Gap

Most of the sources reviewed are technical surveys, prototype demonstrations or security analyses of drone hardware and networks. Within the literature examined by the authors, no study was found that reports stakeholder perceptions of autonomous drone surveillance for SHAR or for a comparable Indian space launch facility. Technical feasibility alone does not guarantee adoption; the views of employees, security staff and the surrounding community on usefulness, supervision, weather limits and cyber risk are needed to plan a workable deployment. This pilot study addresses that gap by combining secondary information on the SHAR setting with a first set of primary perception data.

Objectives of the Study

1. To describe the security setting of SHAR and the regulatory context for drone use from secondary sources.
2. To assess stakeholder perceptions of the usefulness of an autonomous drone system for surveillance, patrolling, real-time alerts and security response at SHAR.
3. To identify the benefits, capabilities and success factors that respondents consider most important.
4. To identify the challenges and concerns, namely weather, technical failure, communication, cyber-security and the need for human supervision.
5. To test whether perception differs with familiarity with drone technology, respondent role and concern about hacking.
6. To suggest a practical direction for a phased implementation and for a larger follow-up study.

Hypothesis

The following null hypotheses were tested at the 5 per cent level of significance. The Drone Security Perception Index (DSPI) is defined in Section 5.4.

- **H01:** The mean agreement of respondents that autonomous drones could significantly improve security at SHAR (and the mean DSPI) does not differ from the neutral midpoint of 3.
- **H02:** There is no significant relationship between familiarity with autonomous drone technology and the DSPI.
- **H03:** There is no significant difference in the DSPI between SHAR employees and other respondents.
- **H04:** There is no significant relationship between concern about drones being hacked and the DSPI.

Research Methodology

5.1 Research design

The study is descriptive and cross-sectional and is designed as a pilot. It uses a mixed evidence base: secondary data drawn from published literature, a parliamentary reply, the Drone Rules, 2021, and news reports, together with primary data from a structured online survey. A pilot design was chosen because the aim is to test the questionnaire, obtain first estimates of perception and identify variables worth pursuing in a larger study.

5.2 Sample design

The population of interest is people connected with SHAR: its employees, security personnel, local residents and other stakeholders. A non-probability convenience sampling method was used, and the questionnaire link was circulated online. The form recorded 44 submissions. One early submission dated 24 August 2026, made before the questionnaire was finalised and containing mostly unstructured or ‘don’t know’ entries, was excluded, leaving a valid sample of 43 respondents. Sample sizes of roughly 12 or more per group have been suggested as a rule of thumb for pilot studies (Julious, 2005); the two largest role groups here meet this guideline, while the smaller groups do not, and this is treated as a limitation.

5.3 Data collection

Primary data were collected through Google Forms on 28 September 2026 (submissions received between about 10:30 and 16:30). Participation was online and no names or contact details were requested. Secondary data were collected from peer-reviewed surveys on UAV applications and security, the Drone Rules, 2021, a reply recorded in the Rajya Sabha, an ISRO announcement, and news agency reports on SHAR; all are listed in the References.

5.4 Questionnaire preparation and measurement

The questionnaire contained 20 structured, closed-ended items (Annexure A). Two items captured respondent profile (role and familiarity with drone technology). Eleven items used five-point ordinal response scales, such as strongly disagree to strongly agree (Likert, 1932), or not useful to extremely useful. The remaining items were single-choice questions on preferred patrol frequency, most important benefit, major challenge, most valuable capability and most important success factor, plus one four-point item on concern about hacking and one four-point item on reduction in assessment time. Ordinal responses were coded 1 to 5 (Annexure B).

A composite Drone Security Perception Index (DSPI) was formed as the mean of nine five-point items: monitoring of restricted areas, overall security

improvement, usefulness of automated patrols, effectiveness of aerial observation, assistance in covering large areas, improvement in security response, importance of predefined routes, usefulness of real-time alerts, and reduction in routine physical inspection. Higher values indicate a more favourable perception. The items on weather, human supervision and hacking were kept outside the index because they describe reservations rather than perceived benefit.

5.5 Reliability and statistical tools

Internal consistency of the DSPI was acceptable (Cronbach's alpha = 0.79, n = 42, nine items; Cronbach, 1951). Analysis was carried out in Python using pandas and SciPy. Tools were frequencies and percentages, means and standard deviations, the one-sample t test with the Wilcoxon signed-rank test as a non-parametric check, Spearman rank correlation, the Kruskal–Wallis test, the Mann–Whitney U test and chi-square goodness-of-fit tests. Because Likert responses are ordinal and the sample is small, non-parametric results are treated as the primary evidence wherever they differ in emphasis.

5.6 Ethical considerations

Participation was voluntary and anonymous, and no sensitive operational details of SHAR security were requested or are reported. The study uses only publicly available secondary information. The DSPI could be computed for 42 of the 43 retained respondents because one person left several rating items blank.

Data Analysis

6.1 Profile of respondents

Table 2: Profile of respondents (n = 43)

Variable	Category	n	%
Role in relation to SHAR	Employee	12	27.9%
Role in relation to SHAR	Local resident	6	14.0%
Role in relation to SHAR	Security personnel	1	2.3%
Role in relation to SHAR	Other stakeholders	24	55.8%
Familiarity with drone technology	Not familiar	7	16.3%
Familiarity with drone technology	Somewhat familiar	15	34.9%
Familiarity with drone technology	Familiar	10	23.3%
Familiarity with drone technology	Very familiar	11	25.6%

Table 2 shows that 55.8% of respondents described their role as 'other' without specifying it, 27.9% were employees, 14.0% were local residents and one respondent was a security professional (Figure 1). Familiarity with autonomous drone technology was spread across the scale: 16.3% were not familiar, 34.9% somewhat familiar, 23.3% familiar and 25.6% very familiar (Figure 2). Roughly half of the sample (48.8%) therefore reported at least a working familiarity with the technology.

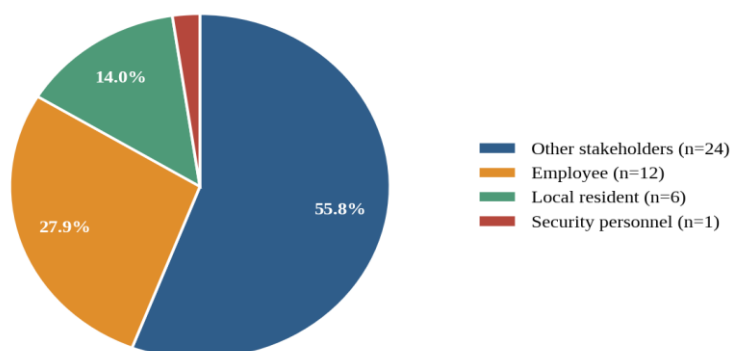


Figure 1: Respondents by role in relation to SHAR (n = 43)

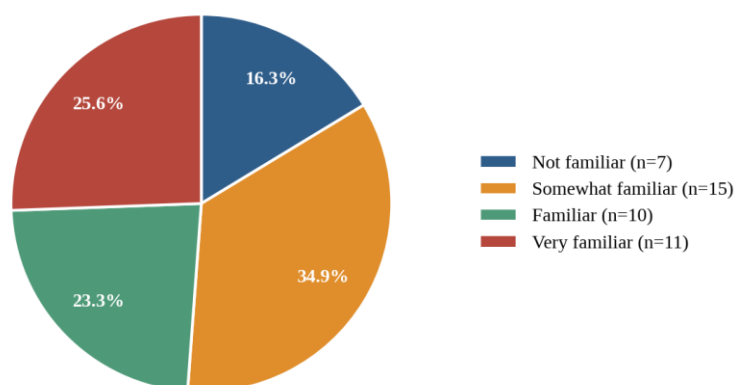


Figure 2: Familiarity with autonomous drone technology (n = 43)

6.2 Perceived effectiveness of autonomous drones

Table 3: Descriptive statistics of perception items (5-point scales, 1 = lowest, 5 = highest)

Item	n	Mean	SD	Median	% rating 4 or 5
Drones can improve monitoring of restricted areas	43	4.05	0.90	4.0	74.4
Drones could significantly improve security at SHAR	43	3.81	1.07	4.0	65.1
Usefulness of automated patrols	43	3.14	1.08	3.0	39.5
Effectiveness of aerial observation	42	3.19	1.17	3.0	40.5
Help in covering large areas	42	3.10	0.96	3.0	35.7
Improvement in security response	42	3.17	1.01	3.0	38.1
Importance of predefined routes	42	2.90	1.03	3.0	28.6
Usefulness of real-time alerts	42	3.38	1.10	3.5	50.0
Reduction in routine physical inspection	42	3.26	1.17	3.0	42.9
Drones should always be human-supervised	43	4.00	0.82	4.0	72.1
Weather could affect drone operations	43	4.00	0.93	4.0	72.1

Note: “% rating 4 or 5” is the share choosing agree/strongly agree, or the two highest levels of usefulness, effectiveness, importance, extent or improvement.

The two broad statements attracted the strongest support. 74.4% agreed or strongly agreed that drones can improve monitoring of restricted areas (mean = 4.05), and 65.1% agreed that drones could significantly improve security at SHAR (mean = 3.81); 25.6% were neutral and 9.3% disagreed (Figure 3). Ratings of specific functions were more moderate, with means between 2.90 and 3.38 (Figure 4). Real-time alerts received the highest function rating, with half of the respondents calling them very or extremely useful, whereas the ability to follow a predefined route received the lowest mean, which sits slightly below the neutral midpoint. On time saved in visually assessing a large area, 12 of 42 respondents (28.6%) expected very little reduction, 31.0% a moderate reduction, 33.3% a significant reduction and 7.1% a very significant reduction.

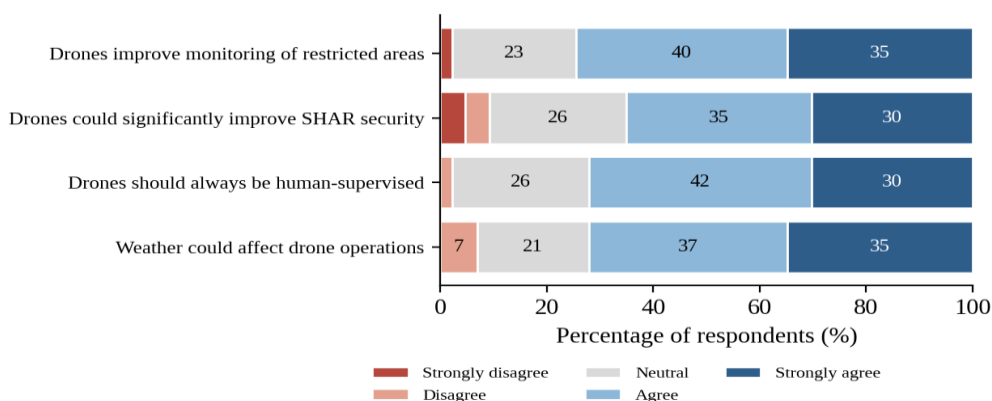


Figure 3: Agreement with selected statements (% of respondents, n = 43)

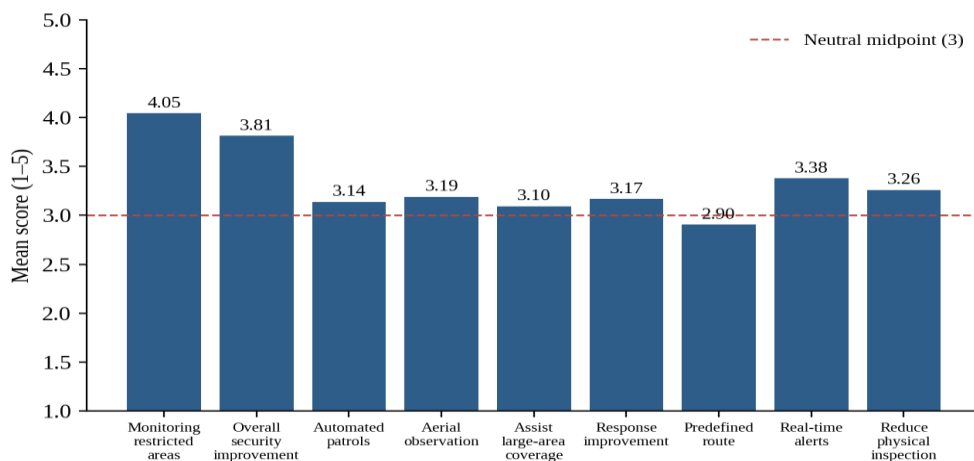


Figure 4: Mean scores of the nine DSPI items (1 = lowest, 5 = highest)

6.3 Preferred patrol frequency

Of the 41 respondents who answered, 36.6% preferred patrols several times a day, 26.8% once a day, 22.0% continuous patrolling and 14.6% patrols only in high-risk situations (Figure 5). About 58.5% thus wanted patrolling at least several times a day, although the distribution was not significantly different from an even spread across the four options (Table 4).

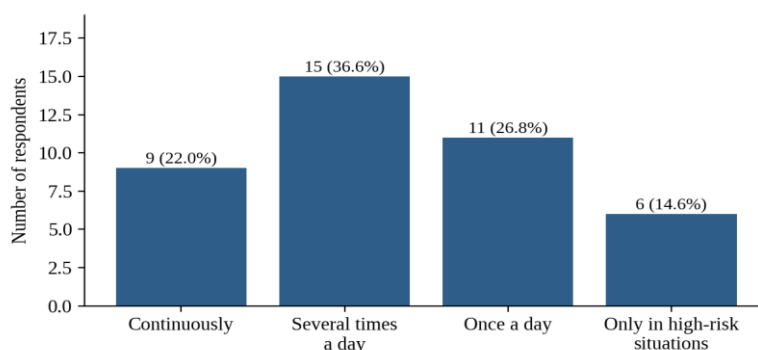


Figure 5: Preferred frequency of autonomous drone patrols (n = 41)

6.4 Benefits, capabilities and success factors

Improved surveillance was the most valued benefit (42.9%), followed by wider security coverage (26.2%), faster threat detection (14.3%), reduced human risk (11.9%) and reduced operational costs (4.8%) (Figure 6). Cost saving was thus the least emphasised benefit. Preferences for the most valuable capability were spread out: real-time video monitoring (26.2%), object or activity detection (23.8%), a combination of capabilities (23.8%), automated route navigation (14.3%) and night-time surveillance (11.9%) (Figure 7). For the factor contributing most to effectiveness, communication reliability (26.2%) and data-processing capability (23.8%) led, ahead of camera and sensor quality (19.0%), integration with existing security systems (16.7%) and autonomous navigation (14.3%) (Figure 8).

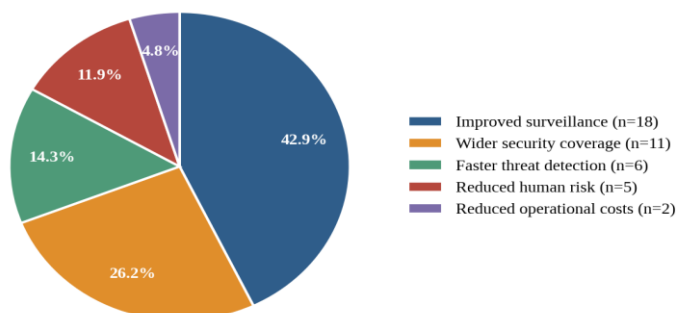


Figure 6: Most important benefit of autonomous drones at SHAR (n = 42)

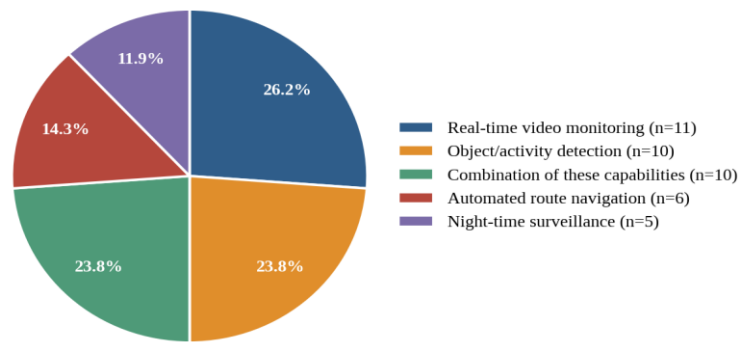


Figure 7: Most valuable capability of an autonomous security drone (n = 42)

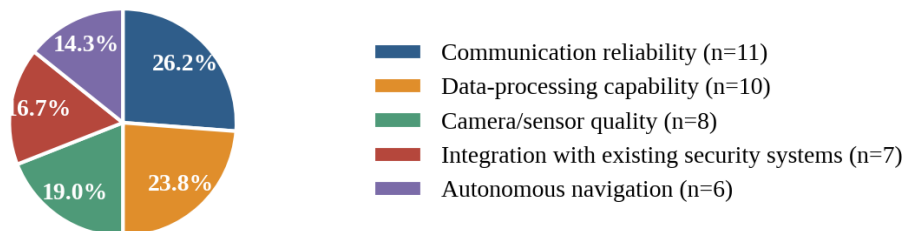


Figure 8: Factor contributing most to effectiveness of drone surveillance (n = 42)

Table 4: Chi-square goodness-of-fit tests on single-choice items (H0: equal preference across options)

Item	n	χ^2	df	p	Significant	Most chosen option
Preferred patrol frequency	41	4.17	3	0.244	No	Several times a day
Most important benefit	42	18.71	4	< .001	Yes	Improved surveillance
Major challenge	41	11.83	5	0.037	Yes	Weather conditions
Most valuable capability	42	3.48	4	0.482	No	Real-time video monitoring
Key success factor	42	2.05	4	0.727	No	Communication reliability

Two of the five distributions departed significantly from an even spread. The concentration on improved surveillance as the main benefit was strong, and the concentration on weather as the main challenge was moderate. Preferences for patrol frequency, capability and success factor were not significantly different from an even spread, which suggests that respondents see several needs as comparably important rather than one dominant priority.

6.5 Challenges and concerns

Weather conditions were named most often as the major challenge (34.1%), followed by technical failures (22.0%), communication or network problems (14.6%), and battery limitations, cybersecurity threats and high implementation cost (9.8% each) (Figure 9). The rating item on weather points the same way: 72.1% agreed or strongly agreed that heavy rain, strong wind or poor visibility could affect drone security operations, and the same share (72.1%) held that drones should always work under human supervision. Concern about hacking or data compromise was widespread: 23.3% were very concerned and 27.9% concerned, making 51.2% in all, while 44.2% were neutral and only 4.7% were not concerned (Figure 10).

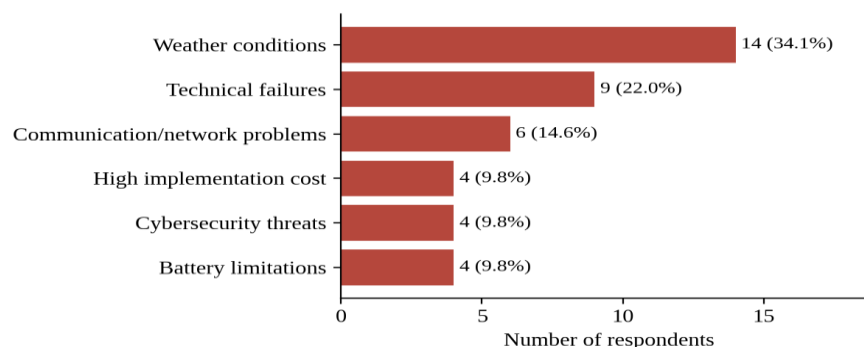


Figure 9: Major challenges in implementing autonomous drones at SHAR (n = 41)

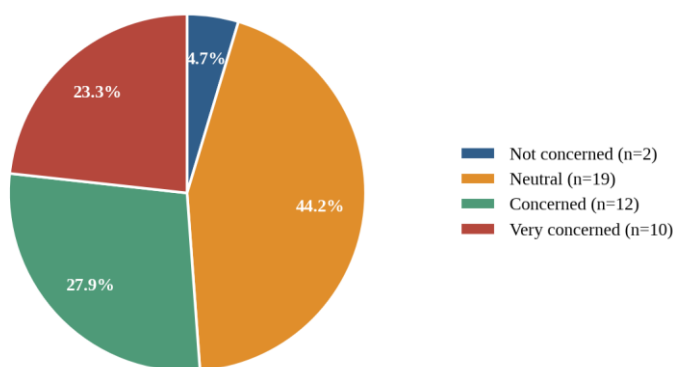


Figure 10: Concern about hacking or data compromise (n = 43)

6.6 Testing of hypotheses

H01. For the single item on overall improvement, mean agreement was 3.81 (SD = 1.07), above the neutral value of 3 (one-sample $t(42) = 4.97$, $p < .001$; Wilcoxon $W = 68$, $p < .001$). For the DSPI ($n = 42$), the mean was 3.33 (SD = 0.65); it was also significantly above 3 ($t(41) = 3.29$, $p = 0.002$; Wilcoxon $W = 211$, $p = 0.004$), with a medium effect size (Cohen's $d = 0.51$). H01 is rejected.

Table 5: Mean DSPI by familiarity with drone technology

Familiarity level	n	Mean DSPI	SD
Not familiar	6	3.50	0.53
Somewhat familiar	15	3.27	0.53
Familiar	10	2.94	0.60
Very familiar	11	3.67	0.76

H02. The Spearman correlation between familiarity and the DSPI was negligible ($\rho = 0.06$, $p = 0.708$, $n = 42$), and the Kruskal–Wallis test across the four familiarity levels was not significant ($H(3) = 5.83$, $p = 0.120$) (Table 5, Figure 11). H02 is not rejected. Group means did not rise steadily with familiarity: the ‘familiar’ group had the lowest mean and the ‘very familiar’ group the highest.

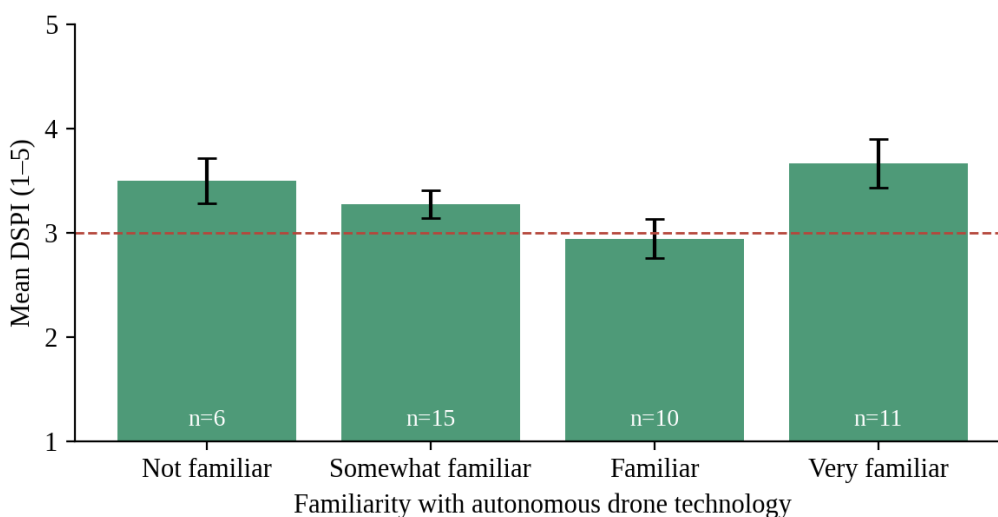


Figure 11: Mean DSPI by familiarity level (error bars show standard error; dashed line = neutral midpoint)

H03. Employees ($n = 12$) had a mean DSPI of 3.19 (SD = 0.50) and all other respondents ($n = 30$) a mean of 3.39 (SD = 0.70). The difference was not significant (Mann–Whitney $U = 149$, $p = 0.394$). H03 is not rejected. The single security professional's index (2.44) was the lowest in the sample, but one case cannot support any inference.

H04. Concern about hacking was unrelated to the DSPI ($\rho = 0.04$, $p = 0.814$, $n = 42$). H04 is not rejected. Respondents who were worried about cyber-attacks were, on average, as favourable towards the technology as those who were not. In addition, overall agreement was positively correlated with agreement on improved monitoring ($\rho = 0.54$, $p < .001$), with expected improvement in security response ($\rho = 0.36$, $p = 0.020$) and with familiarity ($\rho = 0.34$, $p = 0.026$).

Table 6: Summary of hypothesis tests

Hypothesis	Test	Statistic	p	Decision
H01 (overall item)	One-sample t; Wilcoxon	$t(42) = 4.97$; $W = 68$	$< .001$	Rejected
H01 (DSPI)	One-sample t; Wilcoxon	$t(41) = 3.29$; $W = 211$	0.002	Rejected
H02 Familiarity	Spearman; Kruskal–Wallis	$\rho = 0.06$; $H = 5.83$	0.708; 0.120	Not rejected
H03 Employees vs others	Mann–Whitney U	$U = 149$	0.394	Not rejected
H04 Hacking concern	Spearman	$\rho = 0.04$	0.814	Not rejected

Note: Tests are exploratory and no correction for multiple comparisons was applied; with $n = 43$, power to detect small differences is limited.

Interpretations

The results describe conditional optimism. A clear majority accepts the general proposition that autonomous drones would help SHAR's security (65.1% agreement) and would improve monitoring of restricted areas (74.4%). This matches the literature, which presents surveillance as a natural use of UAVs (Shakhatreh et al., 2019). But enthusiasm cools when respondents judge concrete functions: most function items average close to 3.1 to 3.4, meaning that many respondents expect useful but not transformative gains. The pattern suggests that people accept the idea more readily than they are convinced of specific operational payoffs, which is plausible for a technology that is not yet in use at the site.

Real-time alerts were the most highly rated function. This is consistent with Motlagh et al. (2017), who tie the value of aerial sensing to prompt detection, and it agrees with the finding that communication reliability and data-processing capability were the two success factors chosen most often. Together they imply that the perceived value of a drone lies less in the airframe than in how quickly and dependably information reaches decision-makers. The lower rating for predefined routes may indicate that respondents prefer adaptive, event-driven flights to rigid patrol loops, though this study cannot confirm that reading.

The reservations are as informative as the support. Weather was the leading challenge (34.1%) and 72.1% agreed that it could disrupt operations; given the island-and-coast setting described in Table 1, a reliable system would need weather limits and a fallback to conventional patrols. The same proportion wanted permanent human supervision, so acceptance appears to be for supervised autonomy, not for unattended decision-making. Cyber concern was widespread, as the literature on hijacking and jamming would predict (Yaacoub et al., 2020); yet concern was unrelated to the DSPI, so worry about hacking does not seem to reduce respondents' belief in the technology's usefulness. It is better read as a condition to be met than as a reason for rejection.

Perception did not vary significantly with familiarity, role or hacking concern. One reading is that views are shaped by general expectations of technology rather than by technical knowledge, but the small groups and low statistical power mean that modest real differences may have gone undetected. The very small number of security personnel, who would be the day-to-day users, is the most important gap in the evidence.

Findings, Suggestions and Conclusion

8.1 Findings

1. 65.1% of respondents agreed or strongly agreed that autonomous drones could significantly improve security at SHAR, and 74.4% agreed that they can improve monitoring of restricted areas.
2. The composite DSPI (mean 3.33) was significantly above the neutral midpoint, but ratings of individual functions were moderate (means 2.90 to 3.38).
3. Real-time alerts were the highest-rated function (mean 3.38); predefined route following was the lowest (mean 2.90).
4. Improved surveillance (42.9%) and wider coverage (26.2%) were the most valued benefits; reduced operating cost was chosen least (4.8%).
5. Weather was the main perceived challenge (34.1%), followed by technical failures (22.0%).
6. 72.1% favoured permanent human supervision of drones, and 51.2% were concerned about hacking or data compromise.
7. Communication reliability and data-processing capability were the success factors chosen most often.
8. Perception did not differ significantly by familiarity, role (employee versus others) or concern about hacking.

8.2 Suggestions

1. Adopt in phases. Begin with a time-bound trial in selected low-risk perimeter and coastal segments, judged against defined indicators such as detection time, false-alarm rate, coverage achieved and system availability, before any wider rollout.
2. Keep a human in the loop. Design for supervised autonomy with control-room monitoring and manual override, in line with the strong preference for human oversight.
3. Plan for weather. Use platforms rated for local conditions, set clear flight-suspension criteria and keep conventional patrolling as a fallback.
4. Build cyber-security in from the start. Use encrypted links, strong authentication, restricted control access, secure storage of footage and resilience against jamming, as recommended by the security literature.
5. Integrate with existing layers. Route drone alerts into the same control room that handles CCTV, access control and coastal patrol, since real-time alerts were valued most.

8.3 Limitations and scope for further research

This is a pilot study with a small convenience sample, so the results are indicative and cannot be generalised to all SHAR stakeholders. More than half of the respondents did not specify their role and only one security professional took part, which restricts subgroup analysis. The data measure opinion, not system performance, and no field trial was conducted. Part of the secondary evidence is drawn from news reports, and the parliamentary description of security arrangements dates from 2014. Ordinal Likert data were summarised with means for readability and complemented by non-parametric tests, and the tests are exploratory. Future work could use a larger stratified sample, include expert interviews and test a drone system in a controlled trial.

8.4 Conclusion

The study finds that the people who responded see autonomous drones as a promising addition to security at the Satish Dhawan Space Centre, particularly for monitoring, wider coverage and real-time alerts, but they attach clear conditions: human supervision, weather-proof operation, dependable communications and protection against cyber-attack. The evidence supports a cautious, phased and well-integrated pilot deployment rather than immediate large-scale adoption. Because this is a first, small-sample study, its main contribution is a tested questionnaire, initial estimates and a set of hypotheses for a larger and more representative investigation.

REFERENCES

- Abualnaja, K. M., Javed, M. A., & Alasmay, W. (2019). Security challenges of unmanned aerial vehicles: A survey. *Journal of Communications and Networks*, 21(5), 429–446.
- Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika*, 16(3), 297–334.
- IANS. (2025, June 16). Bomb threat to Sriharikota Space Centre sends security agencies into a tizzy. *The News Minute*. <https://www.thenewsminute.com/andhra-pradesh/bomb-threat-to-sriharikota-space-centre-sends-security-agencies-into-a-tizzy>
- Indian Space Research Organisation. (2002, September 5). Prime Minister names space centre after Prof Satish Dhawan [Press release]. SpaceRef. <https://spaceref.com/?p=36011>
- Julious, S. A. (2005). Sample size of 12 per group rule of thumb for a pilot study. *Pharmaceutical Statistics*, 4(4), 287–291.
- Kim, H., Mokdad, L., & Ben-Othman, J. (2018). Designing UAV surveillance frameworks for smart city and extensive ocean with differential perspectives. *IEEE Communications Magazine*, 56(4), 98–104.
- Likert, R. (1932). A technique for the measurement of attitudes. *Archives of Psychology*, 22(140), 1–55.
- Mekdad, Y., Aris, A., Babun, L., El Fergougui, A., Conti, M., Lazzeretti, R., & Uluagac, A. S. (2023). A survey on security and privacy issues of UAVs. *Computer Networks*, 224, 109626.
- Ministry of Civil Aviation, Government of India. (2021). Drone Rules, 2021 (Notification dated 25 August 2021). *The Gazette of India*. <https://egazette.nic.in/WriteReadData/2021/229221.pdf>
- Motlagh, N. H., Bagaa, M., & Taleb, T. (2017). UAV-based IoT platform: A crowd surveillance use case. *IEEE Communications Magazine*, 55(2), 128–134.
- Motlagh, N. H., Taleb, T., & Arouk, O. (2016). Low-altitude unmanned aerial vehicles-based Internet of Things services: Comprehensive survey and future perspectives. *IEEE Internet of Things Journal*, 3(6), 899–922.
- Press Trust of India. (2025, May 10). Mock drills held at Sriharikota Space Centre and Tirupati airport. *Business Standard*. https://www.business-standard.com/india-news/mock-drills-held-at-sriharikota-space-centre-and-tirupati-airport-125051000725_1.html
- Rajya Sabha. (2014, February 20). Reply to Parliamentary Question No. 230 on security of vital space installations. Government of India. https://rsdebate.nic.in/bitstream/123456789/631120/2/PQ_230_20022014_U2910_p289_p290.pdf
- Shakhathreh, H., Sawalmeh, A. H., Al-Fuqaha, A., Dou, Z., Almaita, E., Khalil, I., Othman, N. S., Khreishah, A., & Guizani, M. (2019). Unmanned aerial vehicles (UAVs): A survey on civil applications and key research challenges. *IEEE Access*, 7, 48572–48634. <https://doi.org/10.1109/ACCESS.2019.2909530>
- Yaacoub, J.-P. A., Noura, H., Salman, O., & Chehab, A. (2020). Security analysis of drone systems: Attacks, limitations, and recommendations. *Internet of Things*, 11, 100218.