

An Empirical Study of Factors Influencing Drone Terrorist Attack Casualties

Taeyoung Kim

National Institute of Protection and Security (Presidential Security Service), South Korea

Jeongwan Park

 <https://orcid.org/0009-0001-6623-039X>

Korea Research Institute for Defense Technology Planning and Advancement, South Korea

Julak Lee

 <https://orcid.org/0000-0002-1798-8671>

Chung-Ang University, South Korea

ABSTRACT

Recognizing the pivotal role of casualties as a metric for assessing the success of terrorist acts, this study endeavors to unravel the underlying factors shaping the casualty count in drone terrorist attacks across the globe. By applying Zero Negative Binomial Regression Analysis on data sourced from the Global Terrorism Database, we discern significant factors influencing the number of terrorist casualties. Our findings reveal the paramount importance of the target facility's significance, the attack type, the utilization of remote-controlled drones, the deployment of suicide drones equipped with explosive payloads, and the audacious strategy of swarming drone attacks.

KEYWORDS

National Security, Drone Terrorism Attacks, Situational Crime Prevention, Target Factors, Weapons Factors

INTRODUCTION

Drones, which are formally referred to as unmanned aircraft systems (UASs) or unmanned aerial vehicles (UAVs), have instigated a technological revolution with sweeping implications for public safety (Patel & Rizer, 2019). Despite their initial acclaim for their diverse potential applications, the rapid integration of artificial intelligence (AI) has paradoxically positioned drones as a substantial menace to public safety, giving rise to instances of terrorism, criminal activities, and warfare on a global scale (Wang et al., 2021). In his seminal work *Drones and Terrorism: Asymmetric Warfare and the Threat to Global Security* published in 2018, N. Grossman coined the phrase democratizing smart bombs to underscore the cost-effective empowerment of nonstate actors in the Third World, including terrorist organizations and irregular forces (Grossman, 2018).

Recent developments have underscored the pressing nature of this issue. In 2022, the UN Security Council Counter-Terrorism Committee officially recognized drones as a significant, new terrorist threat to Western nations (UNOCT, 2022). Moreover, the 2023 “Terrorism Outlook” from the Counterterrorism Institute at the U.S. Military Academy at West Point highlighted the transformative role of Russian suicide drones, typified by the Iranian-manufactured Shahed-136 and the Turkish-produced Ukrainian TB-2, in the Ukraine–Russia conflict, colloquially known as “drone warfare” (Hoffman & Ware, 2022). According to the Global Terrorism Index (GTI) for

DOI: 10.4018/IJCWT.350049

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

2023, as analyzed by the Institute for Economics and Peace (IEP), a staggering 113 countries and 65 terrorist organizations, including Houthi rebels, ISIS, and Boko Haram, have incorporated drones weighing between 200 g to 50 kg into their arsenals as illicit tools for antiterrorism endeavors (IEP, 2023). In 2023, the world witnessed a notable surge in terrorism, with incidents increasing by 22% compared to the previous year, reaching levels not seen since 2017. Among these incidents, drone attacks played a significant role, resulting in casualties and drawing attention to the evolving threat landscape (IEP, 2024).

Drones have transcended their conventional roles encompassing search, surveillance, and filming, morphing into highly precise lethal instruments (Gaines & Kappeler, 2019; Enemark, 2019). Striking instances include a swarm drone assault in Colombia in August 2018, which claimed the lives of seven soldiers during an assassination attempt on President Maduro. Similarly, in November 2021, a drone-borne explosive device targeted Iraqi Prime Minister Haider al-Abadi, leading to the unfortunate demise of six security guards. The Ukraine–Russia conflict of 2022 witnessed a multitude of drone strikes, with casualty figures remaining undisclosed. Particularly noteworthy is the employment of a suicide drone in Ukraine in May 2023 intended to target the Russian Kremlin and assassinate President Putin. This event, triggering significant geopolitical tensions, exemplifies the capacity of drone-related incidents to instill fear and shock, thereby enhancing the effectiveness of terrorist organizations in advancing their political objectives (IEP, 2023). Despite the escalating global menace posed by lethal drone terrorism, empirical research on this subject remains limited. The primary challenge lies in deciphering terrorism patterns in affected regions and devising effective counterterrorism strategies.

As a response to this profound knowledge gap, this study seeks to empirically analyze global drone terrorism trends and forecast the factors influencing the number of terrorist casualties by adopting the framework of situational crime prevention (SCP), a well-established theory within the realm of criminology (Gill et al., 2020). In this study, we aimed to analyze the rational decision-making process of terrorists for drone terrorist attacks against the theoretical background of SCP. In particular, we analyzed what physical factors are considered in the decision-making process of drone terrorism in terms of human casualties. In the end, the research question was *What are the factors that influence the number of casualties in drone attacks?*

Through this empirical exploration, the study can provide invaluable insights for cultivating a deeper comprehension of the evolving global security predicament posed by drone terrorism. In pursuit of the study's objectives and to ascertain the factors influencing drone terrorism attacks from the vantage point of SCP, we conducted a comprehensive literature review. This section begins by scrutinizing existing studies to elucidate the concept of drone terrorism attacks and subsequently expounds on the tenets of SCP with a specific emphasis on the rational choice theory.

UNDERSTANDING THE CONCEPT OF DRONE TERRORISM ATTACKS

The expansion of drone threats from primarily military security to nonmilitary domains like terrorism and crime can be attributed to the unique attributes of drones, distinguishing them from traditional modes of attack (USCISA, 2020). Several contemporary instances of terrorism perpetrated using drones are outlined in Table 1.

The threat posed by Iran's drone capabilities at the global level has increased significantly in recent years, posing a major security challenge to the United States and its allies. The urgency of this threat was dramatically demonstrated by the 14 September 2019 attack on Saudi Arabia's Abqaiq oil processing facility and Quraysh oil field, and the 2023 Hamas terrorist attack. In particular, Saudi Arabia and Israel have been exposed as vulnerable to drone terrorist attacks despite the deployment of sophisticated air defense systems (JINSA, 2023).

Now we will discuss some notable drone-related incidents in 2023. In 2023, there was an increase in deadly drone terrorist attacks. On May 3, two suicide drones were shot down over the Kremlin in Russia. This incident was believed to be an attempt to assassinate President Putin. Additionally, on

Table 1. Drone terrorism cases resulting in casualties

Years	Drone terror cases resulting in casualties
2016–2019	In 2016, ISIS used suicide drones in a terrorist attack that resulted in the deaths of 4 special forces members and civilians. In 2018, an unidentified group in Colombia attempted to assassinate the Venezuelan President during a speech using a drone bomb attack, which led to the deaths of 7 soldiers. In 2019, illegal drones appeared at ports in various European countries, causing flight disruptions and posing security concerns. In 2019, Houthi rebels in Yemen launched drone attacks targeting Saudi Arabian oil facilities, resulting in a halt in facility operations and a 50% reduction in oil production.
2020–2023	In 2020, a Taliban drone bomb attack targeted a forward operating base of Afghan security forces, injuring 2 personnel. In 2021, an armed group believed to be operating near the Pakistan–India border conducted a drone bomb attack on an Indian r Force base, damaging buildings within the airbase. In 2022, a drone terror attack occurred at the official residence of the Prime Minister of Iraq in Baghdad, injuring 7 security personnel. In 2022, North Korea engaged in drone provocations. In 2023, a Ukraine (allegedly) drone terror attack on Kremlin Palace in Moscow (Russia). In 2023, a Nationalist drone terror attack on Syria military college graduation ceremony, killed 100 soldiers and civilians. In 2023, Hamas drone attacks on Israeli military bases

May 10, a drone attack targeted a graduation ceremony at a Syrian military academy, resulting in 240 casualties, including 89 soldiers. Remarkably, this attack ranked as the third deadliest globally in 2023 (IEP, 2024). Furthermore, on October 7, the Hamas terrorist organization carried out a drone attack on an Israeli military base, which escalated into a war. These incidents underscore the evolving threat posed by weaponized drones and highlight the need for effective countermeasures in conflict zones.

Recent drone terrorist attacks exhibit distinct characteristics from traditional forms of terrorism, which has prompted the application of SCP theory to analyze the environmental, physical, and situational factors that influence terrorists' decision making regarding drone attacks.

CHARACTERISTICS OF DRONE-BASED TERRORISM

According to the academic discourse, recent terrorist attacks involving drones have exhibited several notable characteristics. First and foremost, drones operate remotely, utilizing radio waves for control and thereby maintaining a significant physical separation between the operator and drone (Cordesman, 2017; Espinoza & Afxentiou, 2018). This distinctive feature enables precise and lethal strikes while maintaining an elusive and concealed profile. Unlike conventional military weaponry, this method diminishes the risk of terrorists themselves being apprehended or targeted during the assault, thus obviating the need for direct self-sacrificial acts, such as suicide bombings (Pledger, 2021). Additionally, it proves challenging for response forces to swiftly pinpoint and disrupt these drones, particularly if they relocate postattack. Furthermore, attackers can alter their position during an assault while maintaining consistent equipment and behavior patterns. This complexity in tracking and identifying operators poses substantial hurdles in preventing future attacks, as evidenced by numerous reports of unidentified drone pilots in various countries. In instances where a pilot with terrorist or criminal intent hastily changes location or flees, detection and apprehension become virtually impossible.

Second, drones possess remarkable aerial maneuverability, including the capability to form swarms, facilitating effective attacks and mass destruction (U.S. Department of Homeland Security, 2020; Kallenborn, 2022). Equipped with precise sensors, drones can accurately target objectives and execute various forms of attacks by capitalizing on their high-speed mobility and hovering abilities, with the choice of attack methods contingent upon the carried equipment or materials (Haugstvedt & Jacobsen, 2020). These swarms of drone strikes quickly create a sense of fear throughout the country, which is the most serious feature of terrorism (Korstanje, 2018).

Moreover, international terrorist organizations have recently assessed that deploying swarms consisting of five to ten drones within a maximum flight range of 1,500 kilometers enables pinpoint precision attacks on multiple targets (MIT Lincoln Laboratory, 2018; IEP, 2023). This assessment is substantiated by an illustrative case in January 2018, when Syrian rebels employed 13 swarm drones to assault a Russian military base (RUSI, 2022). Despite efforts in the realms of technology, legality,

and doctrine, strategies to counter the threat posed by armed swarm drones remain inadequately developed and ineffective.

Finally, drone technology is constantly evolving and enabling a variety of tactical applications. In the early stages, simple drone reconnaissance was used to explore areas and gather intelligence, and Starlink-linked surveillance or strike: Drones relayed real-time intelligence, conducted strikes, identified drone locations, and guided artillery fire. The current phase involves drones following the flight paths of civilian aircraft, swarming (fake) drones attacking anti-aircraft radars or drone bases, and using tactics to drain enemy ammunition. The future will see drones using stealth technology to avoid radar detection, and drones equipped with AI to conduct attacks autonomously. Interconnected drone networks are expected to evolve, utilizing communication technologies such as satellite, LTE, and 5G (IEP, 2023; Blakcori et al., 2024).

APPLICATION OF SITUATIONAL CRIME PREVENTION (SCP)

SCP, as formulated by Clarke and Newman (2006), emphasizes that physical, situational, and environmental factors influence criminal behavior, assuming that offenders are rational actors (Block, 2016). SCP theory recommends that law enforcement agencies focus on modifying or eliminating opportunity factors exhibiting specific situational characteristics to prevent crime effectively (Clarke & Newman, 2006). Terrorists with diverse ideological affiliations and operating within a variety of organizational structures consistently employ rational assessments when evaluating security and risk factors. The study sought to analyze the rational decision-making process that underpins terrorist acts of aggression. How is the cost-benefit decision for a single terrorist attack made? How do terrorists select targets? Finally, the research analyzes what different physical environments are considered in the decision-making process (Gill et al., 2020). This perspective prioritizes reducing crime opportunities and related harms rather than focusing solely on individual offender characteristics (Weisburd et al., 2020).

OPPORTUNITY FACTORS IN DRONE-BASED TERRORISM

Target Factors

Not all potential targets are equally attractive to terrorists. Identifying and prioritizing vulnerable targets are crucial for effective counterterrorism (Martin, 2018). This study concentrates on identifying targets susceptible to chemical and biological terrorism, enabling tailored prevention strategies (McCartan et al., 2008; Haywood, 2017).

Weapons Factors

The choice of weapons significantly influences the nature of terrorist attacks. Weapon selection depends on the available resources within the terrorist organization and the level of expertise. The accessibility of weapons is also a critical factor, with chemical agents being relatively easy to obtain.

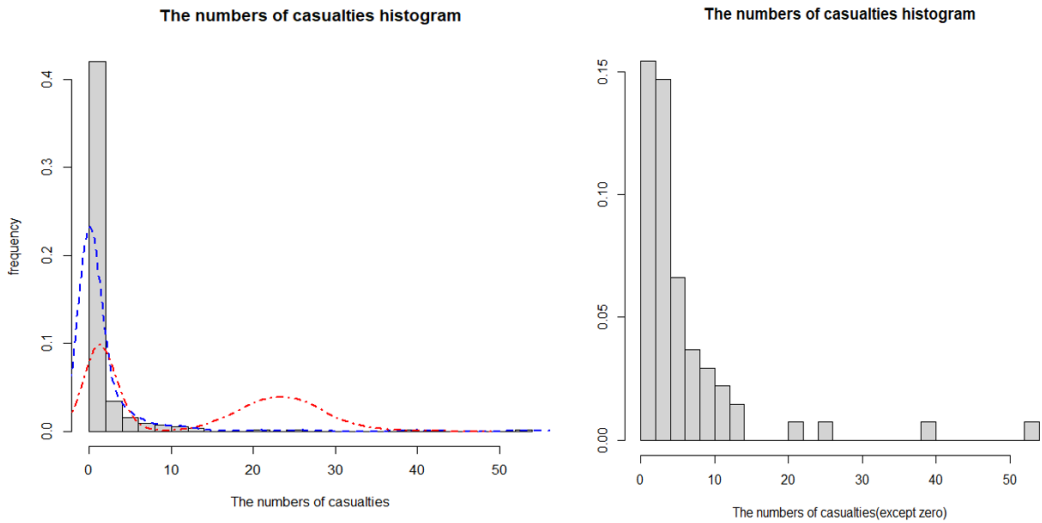
Main variables in this study: Applying SCP theory to analyze drone terrorism, this study considers two main variables to understand the factors influencing terrorists in conducting drone attacks.

Target factors: importance of the target facility, importance of the target person, multiple terror attacks (space complexity), seasonal considerations.

Weapons factors: attack patterns (4), swarm drone attacks

This study aims to provide insights into terrorists' decision-making processes in conducting drone attacks through the SCP framework. Understanding these factors is essential for the development of effective counterterrorism strategies tailored to address the evolving threat of drone-based terrorism.

Figure 1. The numbers of casualties histogram



RESEARCH METHODS

In this study, we aimed to analyze the rational decision-making process behind drone terrorists' attacks. In particular, we were interested in analyzing the cost-benefit decision making of drone strikes in terms of casualties. We aimed to analyze how terrorists choose their targets and methods of attack in order to cause casualties. In the end, the research analyzed how different physical environments are considered in the drone terrorism decision-making process. This study aims to answer the research question: *What are the factors influencing the number of casualties in drone attacks?*

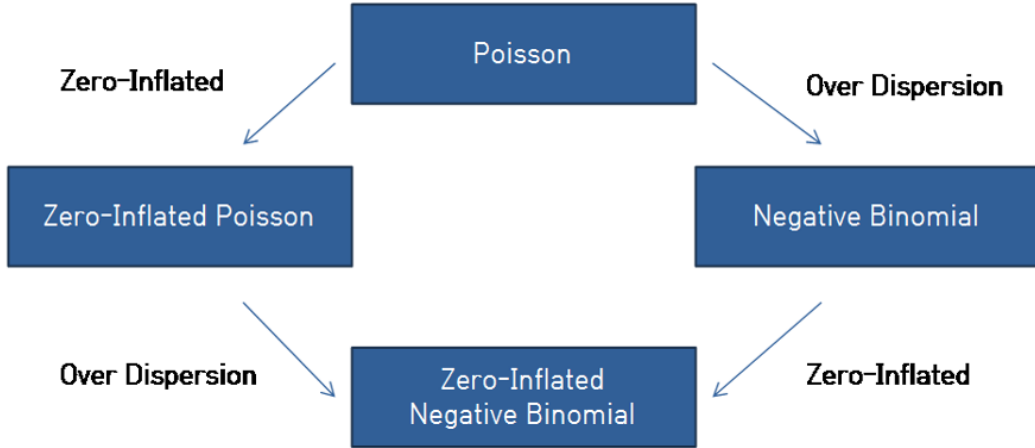
To address this research question, we applied the statistical method of zero-inflated negative binomial regression (ZINB). When determining the statistical analysis technique to identify the factors affecting the number of casualties in drone attacks, it is appropriate to conduct probability and count-based analysis. Typically, when dealing with count data, such as casualty counts, researchers resort to Poisson regression or negative binomial regression. Additionally, casualty numbers are a count data type that cannot be negative, are discrete in nature, and exhibit a skewed distribution.

In cases like this, linear regression models do not satisfy the assumptions and may yield unreliable results. First, the distribution of casualty counts as shown in Picture 1 appears to resemble a Poisson or negative binomial distribution. However, upon calculating the mean and variance of the casualty counts, it is evident that the variance (23.457350) is much larger than the mean (1.433898), indicating overdispersion. Considering these characteristics and the presence of many zeros in the data, we chose to conduct the analysis using ZINB regression.

ZINB regression is used when the standard negative binomial regression is constrained due to excess zeros in discrete probability distributions and when the mean and variance are not equal. The model makes the several assumptions because, when dealing with zero-inflated data, using Poisson or negative binomial models results in an underestimation of the zero-inflated portion: ZINB regression is a mixed model that simultaneously analyzes the count (count model) portion for the group where events occur and the zero-inflated portion for the group where events do not occur, thereby increasing the explanatory power of the overall model. This model achieves this by utilizing techniques such as logistic regression to explain the zero-inflated component.

First, we determined which of the two models to use using a Bernoulli trial, as shown in Equation 1.

Figure 2. Relationship between Poisson and negative binomial regression



$$Y_i \sim \begin{cases} 0 & \text{with probability } \pi_i \\ g(y_i) & \text{with probability } 1 - \pi_i \end{cases} \quad (1)$$

In this study, $g(y_i)$ follows a negative binomial distribution, and the probability of observing $g(y_i)$ is $1 - \pi_i$. π_i represents the excess probability starting from 0. The probability mass function for the zero-inflated model with independent variables can be expressed as shown in Equations 2 and 3.

$$P(y_i = 0|x_i) = I(y_i = 0)\pi_i + (1 - \pi_i)(1 + \alpha\mu_i)^{-\alpha^{-1}} \quad (2)$$

$$P(y_i | x_i) = (1 - \pi_i) \frac{\Gamma(y_i + \alpha^{-1})}{\Gamma(\alpha^{-1})\Gamma(y_i + 1)} \left(\frac{\alpha^{-1}}{\alpha^{-1} + \mu_i} \right)^{-\alpha} \left(\frac{\mu_i}{\alpha^{-1} + \mu_i} \right)^{-y_i}, \quad y_i = 1, 2, 3, \dots \quad (3)$$

In Equations 2 and 3, π_i represents the excess probability starting from 0 and can be modeled using a logistic link function (logit transformation) as shown in Equation 4.

$$\pi_i = \frac{\exp(Z_i' \gamma)}{1 + \exp(Z_i' \gamma)} \quad (4)$$

In Equation 4, $Z_i' = (z_{i1}, z_{i2}, z_{i3}, \dots, z_{ik})'$ represents the independent variable vector for zero-inflated probabilities, and $\gamma_i' = (\gamma_{i1}, \gamma_{i2}, \gamma_{i3}, \dots, \gamma_{ik})'$ represents the vector of coefficients for zero-inflated probabilities. Model fit was evaluated considering the log-likelihood, Akaike Information Criterion (AIC), and Bayesian Information Criterion (BIC). A higher log-likelihood and lower AIC and BIC values indicate a better fit for the model, making it a preferable choice.

DATA

In this study, the data were sourced from the GTD, compiled by the National Consortium for the Study of Terrorism and Response to Terrorism (START) in the United States. The GTD contains

information on terrorist incidents worldwide and relies primarily on publicly available sources, notably internet-based media reports.

This study's scope encompassed 295 drone terrorism incidents across 13 countries. The data range considered was from January 2016 to June 2021, coinciding with the first appearance of drone terrorism incidents in the GTD data set. To augment the data set and include variables not covered in the GTD, additional information was derived from various global drone terrorism-related research papers and major media sources. This supplementary information was then aligned with the basic data structure provided in the GTD codebook (START, 2021).

OPERATIONALIZATION OF VARIABLES

Dependent Variables

Number of casualties: To quantify the number of casualties resulting from drone terrorism, the study examines the total count of deaths and injuries. The number of casualties, including both fatalities and injuries, ranged from 0 to 54 (START, 2021).

Independent Variables

The independent variables related to terrorist targets and weapons were informed by previous research.

Season

The season variable was adapted from prior studies, and it indicates the significant influence of seasonal factors on terrorist attack casualties. The study categorizes the time of year when the incidents occurred into two seasons: summer (March to September) and winter (October to March). This dichotomy reflects the hypothesis that terrorist attacks are more frequent during the active, warmer summer months; accordingly, we coded this variable as 1 for attacks that have occurred during warm seasons and 0 for cold seasons (Kim et al., 2022).

Importance of Target Facility

This variable was influenced by the findings from Cordesman (2017), Korstanje (2021), and Kim et al. (2021), which highlighted that highly symbolic public facilities, including those of national significance, are more prone to drone terrorist attacks and casualties. Accordingly, government facilities, military bases, police stations, and less-exposed public facilities were coded as 1, while generally less-protected and exposed civilian facilities received a code of 0 (START, 2021).

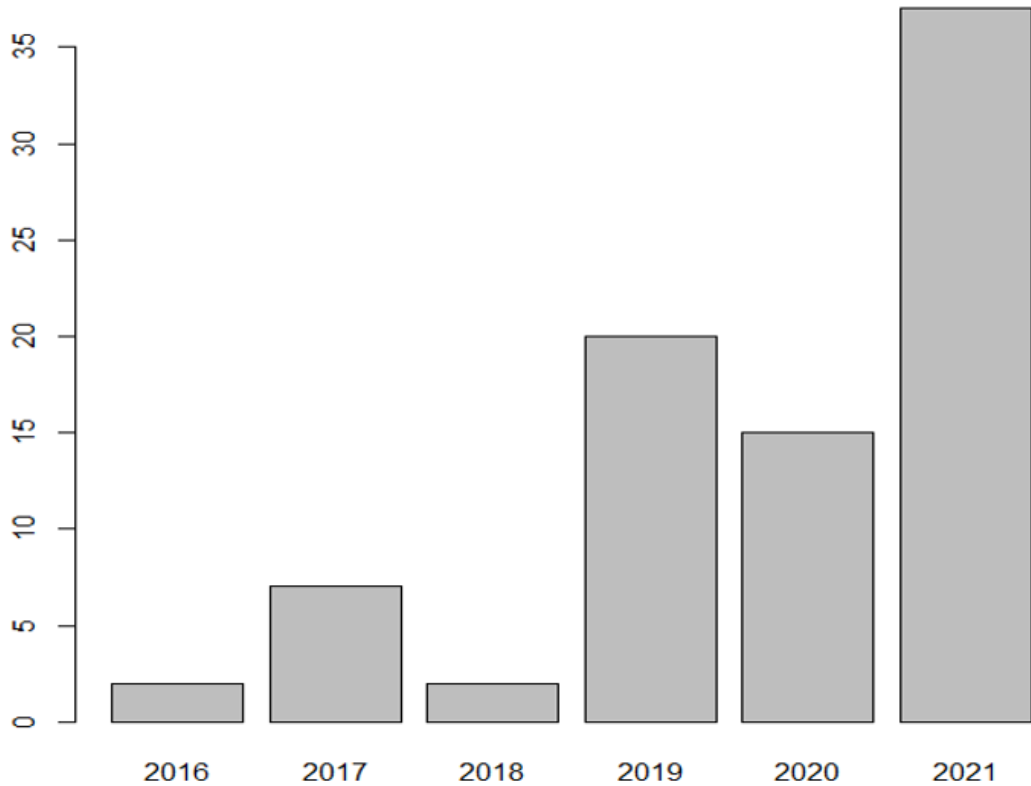
Importance of Target Person

Incorporating research by Kim et al. (2021), which associated higher-profile national figures with an increased likelihood of drone terrorism casualties, we assigned 1 when the target of an attack was a government or public institution official such as heads of state, high-profile people, military personnel, police, or diplomats, and we assigned 0 in the case of unspecified civilians, as guided by the criteria outlined in the GTD coding book's target type classification (START, 2021).

Multiple Terror: Spatial Complexity

Several studies, including Deloughery (2013), Crenshaw(2007), Parkin and Freilich (2015), and Kim et al. (2021), indicated that the number of casualties and the scale of terrorist attacks tend to rise in multiple-target scenarios as opposed to single-incident attacks. We captured this concept by coding simultaneous terrorist attacks as 1 and single, one-time attacks as 0, following the GTD coding book's multiple classification (START, 2021).

Figure 3. Histogram by year of terror occurrence using swarm drones



Attack Patterns

Informed by the research of Grossman (2018) and Farlík and Gacho (2021), which highlighted the precision and versatility of drones in executing attacks, this study examines the types of attacks performed using drones. Four attack types—remote trigger, projectile, device drop, and firearms—were identified according to the GTD coding book's attack type classification criteria.

Swarm Drones Attacks

Building on the analysis presented in IEP (2023) and ACLED (2023), which emphasized that recent drone terrorism patterns increase the likelihood of casualties through swarm maneuvers rather than single drone attacks, we coded swarm drone terrorist attacks as 1 and single drone terrorist attacks as 0.

Control Variables

Area: Region of occurrence of drone terrorism was categorized according to the country and region codes outlined in the GTD coding book. Specifically, the Middle East was assigned a code of 0, which encompassed the Middle East and North Africa, Sub-Saharan Africa, and South Asia. Conversely, the West was designated a code of 1, incorporating North America, East Asia, Southeast Asia, Central America, and the Caribbean, as well as Eastern and Western Europe (START, 2021).

Table 2. Operationalization of variables

Dependent variables	Casualties	0–54 person(s)	
Independent variables	Drone terrorism target factors (5)	Season	Summer, March to October (1)
			Winter, November to February (0)
		Importance of the facility	National critical infrastructure (1)
			Private facilities (0)
		Importance of the person	High-profile people (1)
			Unspecified civilians (0)
		Multiple terror attack	Multiple terror (1)
			Single terror (0)
	Drone terrorism weapon factors (4)	Attack pattern	Projectile, remote trigger, device drop, firearms
		Swarm drones	Swarm drone attack (1)
			Single drone attack (0)

FINDINGS

Table 3 presents the descriptive statistics for the independent variables. The total number of casualties resulting from drone terror incidents is 423, with an average of 1.43 casualties per incident. The incident with the highest number of casualties, 40 in total (seven military fatalities and 21 injuries), occurred on August 13, 2020, in the Marib region of Yemen. This incident was a suicide drone bombing attack by Houthi extremists, a terrorist organization, targeting a military base (Yaacoub et al., 2020).

First, in terms of seasons, the numbers of terror incidents and total casualties are relatively higher in the summer season (March to October), accounting for 211 incidents (71.53%) and 261 casualties (61.7%), respectively. However, in terms of the average casualties per incident, the winter season has a higher average of 1.93 casualties per incident compared to 1.23 in the summer season.

Second, in terms of the importance of the target facilities, public facilities (such as presidential offices, major government buildings, military bases, and police stations) show a relatively higher frequency of terror incidents, totaling 192 cases (65.08%) compared to nonspecific private facilities. Furthermore, in terms of the total number of casualties and the average casualties per incident, public facilities (192 casualties/1.56 casualties per incident) have relatively higher numbers than private facilities (103 casualties/1.2 casualties per incident). This suggests a somewhat distinctive result from the general trend of terrorist attacks targeting nonspecific private facilities more often, highlighting a difference in the pattern of typical terrorist attacks.

Third, considering the importance of the target individuals, attacks on politically influential figures and leaders involved in crucial state affairs show a higher frequency of incidents, totaling 206 cases (69.83%) compared to attacks on nonspecific civilians. Furthermore, in terms of the total number of casualties and the average casualties per incident, attacks on prominent figures (311 casualties/1.51 casualties per incident) have a relatively higher count than attacks on nonspecific civilians (112 casualties/1.26 casualties per incident). This indicates that attacks on important figures are more prevalent both in terms of frequency and casualties compared to attacks on nonspecific civilians.

Fourth, multiple terrorist attacks, where terrorist incidents occurred continuously and simultaneously, are relatively less frequent compared to single incidents, accounting for 75 cases (25.42%). Consequently, the total number of casualties resulting from these complex attacks is lower (110 individuals, 26%), and the average casualties per incident are similar to that of single-attack incidents.

Table 3. Descriptive statistics of independent variables

Category	Total casualties	Percentage (%)	Number of terrorist incidents	Percentage (%)	Average number of casualties
Season	423	100	295	100	1.43
Summer, March–October	261	61.7	211	71.53	1.24
Winter, November–February	162	38.3	84	28.47	1.93
Attack patterns	423	100	295	100	1.43
Projectile	19	4.49	25	8.48	1.36
Remote trigger	322	76.12	237	80.34	1.17
Device drop	75	17.73	27	9.15	2.78
Firearms	7	1.65	6	2.03	1.43
Multiple terror attack	423	100	295	100	1.43
Multiple terror	110	26	75	25.42	1.47
Single terror	313	74	220	74.58	1.42
Importance of the target facility	423	100	295	100	1.43
National critical infrastructure	299	70.69	192	65.08	1.56
Private facilities	124	29.31	103	34.92	1.20
Importance of the person	423	100	295	100	1.43
High-profile people	311	73.52	206	69.83	1.51
Unspecified civilians	112	26.48	89	30.17	1.26
Swarm drone attack	423	100	295	100	1.43
Swarm drone attack	231	54.61	83	28.14	2.78
Single drone attack	192	45.39	212	71.86	0.91

Note. Percentage rounded to 3 decimal places.

Fifth, in terms of attack types, remote-controlled attacks predominate with a significantly higher proportion (237 cases, 80.34%), followed by suicide bombings and explosive device drops (27 cases, 9.15%), projectile attacks (25 cases, 8.48%), and firearm attacks (6 cases, 2.03%). However, the average number of casualties per incident varies by attack type, with suicide bombings and explosive device drops having the highest average (2.78 individuals), followed by firearm (1.43 individuals), projectile (1.36 individuals), and remote-controlled attacks (1.17 individuals).

Sixth, cluster drone attacks account for a total of 83 casualties, representing 28.14% of the distribution. Notably, among all incidents, there are 11 cases where more than 10 casualties occurred, and all these incidents are attributed to swarm drones. Furthermore, there has been a significant increase in such incidents since 2019, rising from two cases to 20 cases, a 1,000% increase. The average number of casualties in cluster drone attacks is 2.78 individuals, significantly higher than the average of 0.91 individuals in single drone attacks.

Table 4 presents the results of ZINB regression conducted to identify the factors influencing the number of casualties in drone terror incidents.

First, regarding target factors, we found that, regionally, the Middle East has a statistically significant impact on the number of casualties in drone terror attacks compared to non-Middle East regions. Additionally, regarding the importance of the target facility variable, nationally important facilities have a statistically significant positive effect on the number of casualties compared to

Table 4. Results of zero-inflated negative binomial regression analysis

Category	Count model				Zero-inflation model			
	<i>B</i>	SE	<i>Z</i>	<i>Pr(> z)</i>	<i>B</i>	SE	<i>Z</i>	<i>Pr(> z)</i>
Intercept	−0.3164	0.4758	−0.665	0.50626	1.2164	0.2619	4.645	3.39e-06 ***
Area	0.9282	0.2850	3.257	0.00113 **				
Importance of the target facility	0.6251	0.2149	2.909	0.00363 **	0.6009	0.3072	1.956	0.0505.
Multiple terror attack	−0.6288	0.2102	−2.991	0.00278 **	−1.4294	0.3177	−4.499	6.82e-06 ***
Attack patterns								
Remote trigger	0.9933	0.3692	2.690	0.00714 **				
Device drop	0.9007	0.3992	2.256	0.02405 *				
Firearms	0.1520	0.6583	0.231	0.81744				
Swarm drone attack	0.6470	0.2309	2.803	0.00507 *				
Log (theta)	1.3037	0.3303	3.947	7.93e-05 ***				

$p < 0.1$, * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$.

Theta = 3.683

Number of iterations in BFGS optimization: 18

Log-likelihood: −310 on 12 Df

civilian facilities. In other words, relatively well-defended and symbolic nationally important facilities influence the occurrence of casualties. Finally, multiple attacks are statistically associated with a negative impact on casualties.

Second, in terms of weapon factors, we observed that remote-controlled attacks and suicide drones (explosive device drops) have a statistically significant positive impact on the number of casualties, while cluster drone attacks are also positively associated with the number of casualties. Particularly, the remote trigger variable has the highest influence among the independent variables on the number of casualties. Furthermore, we found that multiple cluster drones have a statistically significant impact on the number of casualties compared to single drones.

Zero-inflated Poisson (ZIP) regression analysis was also conducted, as shown in Table 5, for the purpose of comparison. The results are similar to those obtained from the ZINB regression analysis. As presented in Table 6, we can conclude that considering both overdispersion and excess zeros, ZINB regression analysis is more suitable than the ZIP model. It is worth noting that negative binomial and Poisson analyses were also performed, but no significant results are obtained.

DISCUSSION AND CONCLUSIONS

This study is rooted in the criminological theory of SCP, which posits that criminals make rational decisions on the basis of situational factors and conditions when selecting their criminal activities. In the context of drone terrorism, it is assumed that terrorists choose their targets and methods according to specific characteristics that increase the likelihood of success. Accordingly, this study focuses on two dimensions, target and weapon, and employs these variables to assess their impact on drone terrorism casualties using descriptive statistics and zero-inflated regression. Here are the summarized results:

First, within the weapon variables, remote trigger is the most frequently used method, with remote-control and drone attacks involving explosives showing a statistically significant positive effect

Table 5. Result of zero-inflated Poisson regression analysis

Category	Count model				Zero-inflation model			
	<i>B</i>	<i>SE</i>	<i>Z</i>	<i>Pr(> z)</i>	<i>B</i>	<i>SE</i>	<i>Z</i>	<i>Pr(> z)</i>
Intercept	−0.4069	0.3335	−1.220	0.222425	1.2666	0.2562	4.943	7.69e-07 ***
Area	0.9669	0.1965	4.922	8.58e-07 ***				
Importance of target facility	0.6686	0.1201	5.567	2.59e-08 ***	0.5583	0.2992	1.866	0.062
Multiple terror attack	−0.5848	0.1311	−4.461	8.19e-06 ***	−1.3710	0.3060	−4.481	7.44e-06 ***
Attack pattern								
Remote trigger	0.9728	0.2531	3.844	0.000121 ***				
Drop device	0.8702	0.2828	3.077	0.002091 **				
Firearms	0.2922	0.4596	0.636	0.524974				
Swarm drone attack	0.8049	0.1150	6.998	2.59e-12 ***				

$p < 0.1$, * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$.
Number of iterations in BFGS optimization: 16
Log-likelihood: −342.6 on 11 Df

Table 6. Model comparison (ZINB versus ZIP)

Model	ZINB	ZIP
Log-likelihood	−310	−342.6
AIC	644.0159	707.1336
BIC	688.2596	747.6903

on all dependent variables. This suggests that terrorists prefer using remote-controlled or drone-based attacks, where the operator and the drone are remotely separated, over projectile attacks. This finding aligns with previous research indicating that drone terrorism is more likely to result in casualties due to the reduced exposure of operators, eliminating the risk of capture, attack, or self-sacrifice as seen in suicide bombings (Alakoc, 2017; Grossman, 2018; Farlík & Gacho, 2021; Pledger, 2021).

Second, among the target variables, there is a high occurrence during the summer months and a preference for hard targets, such as nationally important facilities and political figures. Both the importance of the target facility and the importance of the person variables have a statistically significant effect on the number of terrorist casualties. This corroborates earlier studies indicating that terrorists are drawn to high-value, symbolically significant targets, thereby increasing the likelihood of drone terrorism attacks (Yaacoub et al., 2020; Kim et al., 2022). This is contrary to previous research that suggests that, while classical terrorism targeted critical public facilities, politicians, celebrities, and other high-profile targets, modern terrorism focuses attacks on unspecified civilians and facilities (Korstanje, 2021).

It suggests that terrorists are strategically employing drones as a primary tool to target critical national facilities and key individuals, impacting national security and people's lives across various countries in asymmetrical warfare. This approach maximizes the impact of terrorist attacks by

exploiting the relative weaknesses of air defense systems compared to drone attack technology and tactics (Grossman, 2018).

Third, the multiple terror attack variable, although less frequent, results in relatively higher casualty rates. This indicates that, from the terrorist's perspective, carrying out attacks in a series or simultaneously in multiple locations, as opposed to single attacks or single locations, increases the likelihood of achieving the desired impact. This is consistent with existing research that suggests that if a terrorist's goal is to maximise fear among a large number of people, they will prefer a complex terrorist attack that destroys a large number of facilities and people (Deloughery, 2013; Berkell, 2020; Kim et al., 2022).

Fourth, concerning the target variables, seasonal factors, particularly the winter season, are statistically significant in predicting terrorist casualties. This can be attributed to the seasonal characteristics of the Middle East and North Africa, where most of the data were collected. This finding aligns with recent research suggesting that the summer months may increase the likelihood of mechanical failures in drones and explosives due to high temperatures, dryness, and sandy winds. Additionally, issues like radio interference between drones and explosives can lead to a higher likelihood of failed terrorist attacks during the summer (Kim et al., 2022).

Fifth, the swarm drone attacks variable within the weapon variables demonstrates a statistically significant effect on the occurrence of terrorist casualties. This reflects the rising trend of swarm drone attacks resulting in mass casualties in recent years, with all mass casualty incidents involving the use of swarm drones. This supports the argument that contemporary drone terrorism has shifted from single drone attacks to coordinated, simultaneous multiple attacks using multiple drones. This transformation is linked to advancements in information and communication technology and aligns with existing research findings (ACLED, 2023).

The implications of this study are drawn out. First, this study suggests that terrorists are more likely to conduct drone terrorism attacks against hard targets (such as national critical facilities and key figures) in complex terrorism scenarios, taking into account seasonal factors. Regarding weaponry, this study finds that terrorists are more inclined toward the remote-controlled attack mode of swarm drones for executing terrorist acts.

Second, the threat patterns of major countries such as Saudi Arabia, which have a high frequency of drone terrorism, should be analyzed in depth. This should lead to the development of response manuals for the key players, the military, and the police. Based on these manuals, they should be able to respond to various situations such as crimes, terrorism, and military provocations in a timely manner.

Third, the antidrone response system for national critical facilities should be improved based on the results of the study. The response concepts and equipment should be enhanced from the perspective of integration, redundancy, and multilayering, moving away from the existing ground-based operation concept. Through this, systematic joint drills should be regularized with key relevant agencies.

While this study offers valuable insights by empirically analyzing drone terrorism tendencies and patterns of area successful attacks, it has limitations. First, the majority of the data from the GTD used in the study primarily represents countries in the Middle Eastern and North African regions, limiting the generalizability of the findings to a global analysis of drone terrorism trends. Future research is encouraged to explore the causal relationship between drone terrorism variables and the occurrence of casualties on a broader scale. Additionally, a more in-depth investigation into the influence of seasonal environmental factors, such as temperature, air quality, humidity, and precipitation, on drone terrorism is warranted.

Second, it may reveal the degree to which various indicators influence outcomes, and it fails to pinpoint decisive factors that can be directly controlled or prevented. A comprehensive analysis to identify significant elements that could help prevent terrorism, alongside the collection and pipeline-building of pertinent data, would allow for predicting the likelihood and conditions of terrorism and uncovering direct methods of prevention.

Recent research in biometrics has explored gait recognition as a promising approach to identifying individuals (Parashar et al, 2024). Applying this technology in counterdrone terrorism could help devise a concrete prevention strategy if we collect relevant data systematically and build pipelines to forecast the conditions under which drones might be employed for terrorist purposes. And the issue of ethical and political debates about the threats posed by new digital technologies such as drones should be further explored (Lyon, 2010).

FUNDING

This study was supported by the BK21 FOUR program (Education and Research Center for Securing Cyber-Physical Space) through the National Research Foundation (NRF) funded by the Ministry of Education of Korea (5199990314137).

CONFLICTS OF INTEREST

We wish to confirm that there are no known conflicts of interest associated with this publication and there has been no significant financial support for this work that could have influenced its outcome.

PROCESS DATES

07, 2024

This manuscript was initially received for consideration for the journal on 03/24/2024, revisions were received for the manuscript following the double-anonymized peer review on 07/10/2024, the manuscript was formally accepted on 07/05/2024, and the manuscript was finalized for publication on 07/10/2024.

CORRESPONDING AUTHOR

Corresponding author: Julak Lee (julaklee71@cau.ac.kr)

REFERENCES

- ACLED. (2023). *Beyond Riyadh: Houthi cross-border aerial warfare 2015-2022*. Armed Conflict Location and Event Data Project.
- Alakoc, B. P. (2017). When suicide kills: An empirical analysis of the lethality of suicide terrorism. [IJCV]. *International Journal of Conflict and Violence*, 11, a493–a493.
- Berkell, K. A. (2020). *A criminological approach to preventing terrorism: Situational crime prevention and the crime prevention literature*. International Centre for Counter-Terrorism.
- Blakocok, N., Stathakis, L. I., Koutsoukos, L. D., Kirilov, L. K. (2024). *The evolving UAS threat: Lessons from the Russian-Ukrainian war since 2022 on future air defense challenges and requirements*.
- Block, M. M. (2016). *Applying situational crime prevention to terrorism against airports and aircrafts*. [Doctoral dissertation, University of Louisville].
- Clarke, R. V. G., & Newman, G. R. (2006). *Outsmarting the terrorists*. Praeger Security International.
- Cordesman, G. (2017). *The patterns in global terrorism: 1970-2016*. Center for Strategic & International Studies.
- Crenshaw, M. (2007). Explaining suicide terrorism: A review essay. *Security Studies*, 16(1), 133–162. 10.1080/09636410701304580
- Deloughery, K. (2013). Simultaneous attacks by terrorist organizations. *Perspectives on Terrorism*, 7(6), 79–89.
- Enemark, C. (2019). Drones, risk, and moral injury. *Critical Military Studies*, 5(2), 150–167. 10.1080/23337486.2017.1384979
- Espinoza, M., & Afxentiou, A. (2018). Editors' introduction: Drones and state terrorism. *Critical Studies on Terrorism*, 11(2), 295–300. 10.1080/17539153.2018.1456727
- Farfík, J., & Gacho, L. (2021, June). Researching UAV threat—new challenges. In *2021 international conference on military technologies (ICMT)* (pp. 1-6). IEEE. 10.1109/ICMT52455.2021.9502759
- Gaines, L. K., & Kappeler, V. E. (2019). *Homeland security and terrorism*. Pearson.
- Gill, P., Marchment, Z., Corner, E., & Bouhana, N. (2020). Terrorist decision making in the context of risk, attack planning, and attack commission. *Studies in Conflict and Terrorism*, 43(2), 145–160. 10.1080/1057610X.2018.1445501
- Grossman, N. (2018). *Drones and terrorism: Asymmetric warfare and the threat to global security*. Bloomsbury Publishing. 10.5040/9781350986169
- Haugstvedt, H., & Jacobsen, J. O. (2020). Taking fourth-generation warfare to the skies? An empirical exploration of non-state actors' use of weaponized unmanned aerial vehicles (UAVs—'drones'). *Perspectives on Terrorism*, 14(5), 26–40.
- Haywood, T. (2017). *Determinants of terrorist target selection: A quantitative analysis*. [Master's dissertation, University of Central Florida].
- Hoffman, B., & Ware, J. (2022). The terrorist threats and trends to watch out for in 2023 and beyond. *CTC Sentinel*, 1-9.
- IEP. (2023). *Global terrorism index (GTI)*. Institute for Economics and Peace.
- IEP. (2024). *Global terrorism index (GTI)*. Institute for Economics and Peace.
- JINSA. (2023). *Build it and they will come: A U.S. strategy for integrating Middle East air and missile defense*. Jewish Institute for National Security of America.
- Kallenborn, Z. (2022). InfoSwarms: Drone swarms and information warfare. *Parameters*, 52(2), 87–102. 10.55540/0031-1723.3154
- Kim, T., Jeong, S., & Lee, J. (2022). Factors of mass casualty terrorism. *Security Journal*, 35(1), 133–153. 10.1057/s41284-020-00268-w

- Korstanje, M. E. (2021). Tracing the cultural background of lone-wolf terrorism: Dilemmas, contradictions, and opportunities for the next decade. [IJCWT]. *International Journal of Cyber Warfare & Terrorism*, 11(1), 45–56. 10.4018/IJCWT.2021010104
- Korstanje. (2018). *The challenges of democracy in the war on terror: The liberal state before the advance of terrorism*. Routledge.
- Martin, G. (2018). *Essentials of terrorism: Concepts and controversies*. SAGE Publications.
- McCartan, L. M., Masselli, A., Rey, M., & Rusnak, D. (2008). The logic of terrorist target choice: An examination of Chechen rebel bombings from 1997–2003. *Studies in Conflict and Terrorism*, 31(1), 60–79. 10.1080/10576100701767122
- MIT Lincoln Laboratory. (2018). *Urban counter-UAS operational prototype*.
- Parashar, A., Parashar, A., Shabaz, M., Gupta, D., Sahu, A. K., & Khan, M. A. (2024). Advancements in artificial intelligence for biometrics: A deep dive into model-based gait recognition techniques. *Engineering Applications of Artificial Intelligence*, 130, 107712. 10.1016/j.engappai.2023.107712
- Parkin, W. S., & Freilich, J. D. (2015). Routine activities and right-wing extremists: An empirical comparison of the victims of ideologically-and non-ideologically-motivated homicides committed by American far-rightists. *Terrorism and Political Violence*, 27(1), 182–203. 10.1080/09546553.2014.975649
- Patel, B., & Rizer, D. (2019). *Counter-unmanned aircraft systems technology guide*. U.S. Department of Homeland Security: Science and Technology Directorate.
- Pledger, T. (2021). *The role of drones in future terrorist attacks*. Association of the United States Army.
- RUSI. (2022). *Militants and drones: A trend that is here to stay*. Royal United Services Institute.
- START. (2021). GTD codebook: Methodology, inclusion criteria, and variables. National Consortium for the Study of Terrorism and Responses to Terrorism. University of Maryland.
- UNOCT. (2022). *Protecting vulnerable targets from terrorist attacks involving unmanned aircraft systems (UAS)*. United Nations Office of Counter-Terrorism.
- U.S. Department of Homeland Security. (2020). *United States Secret Service unmanned aircraft systems program*.
- USCISA. (2020). *Protecting against the threat of unmanned aircraft systems (UAS)*. U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency Interagency Security Committee.
- Wang, J., Liu, Y., & Song, H. (2021). Counter-unmanned aircraft system (s)(C-UAS): State of the art, challenges, and future trends. *IEEE Aerospace and Electronic Systems Magazine*, 36(3), 4–29. 10.1109/MAES.2020.3015537
- Weisburd, D., Savona, E. U., Hasisi, B., & Calderoni, F. (2020). *Understanding recruitment to organized crime and terrorism*. Springer. 10.1007/978-3-030-36639-1
- Yaacoub, J. P., Noura, H., Salman, O., & Chehab, A. (2020). Security analysis of drones systems: Attacks, limitations, and recommendations. *Internet of Things : Engineering Cyber Physical Human Systems*, 11, 100218. 10.1016/j.iot.2020.10021838620271