UAS in Urban Attacks

Red Teaming Exercise Report

by
Kerry Chávez

sponsored by

weTHINK.
THE SOCIAL NETWORK FOR STRATEGY

in partnership with

UN

The Center for
Advanced Red Teaming
University at Albany
State University of New York

UWE Bristol
University of the West of England

DRONE SEC

About the Author

Kerry Chávez, PhD, is an instructor in the Political Science Department and project administrator at the Peace, War, and Social Conflict Laboratory at Texas Tech University. She is also a two-time nonresident research fellow with the Modern War Institute at West Point. Her research focusing on the politics, strategies, and technologies of modern conflict and security has been published in several venues. As part of her work on how violent nonstate actors exploit drone technologies, she collaborates with several security providers and policymakers.

About *we*THINK.

Based out of Austria, *we*THINK. facilitates an online network of innovative people to analyze and strategize current challenges and opportunities. Through education, networking, and curation of diverse and talented strategy groups, it explores salient, pressing topics. *we*THINK. also regularly hosts events and disseminates knowledge it has helped to generate and refine.

About the Center for Advanced Red Teaming

The Center for Advanced Red Teaming (CART) is an interdisciplinary research center within the College of Emergency Preparedness, Homeland Security and Cybersecurity at the University at Albany. As the first academic center devoted to advancing the art and science of red teaming, it seeks to address a conspicuous need for both research and education in this growing area of security studies.

Acknowledgements

The "UAVs and Near Future Conflicts" working group values its growing repertoire of partners across industry, academic, and governmental institutions that make this project and its aftereffects in security possible. In particular, we wish to thank Gary Ackerman, Anna Wetzel, and other affiliates at CART at the University of Albany; Chris Church with INTERPOL; Mike Monnik and the DroneSec team; the University of the West of England Bristol; the University of Piraeus; and the United Nations Peacekeepers. We extend special gratitude to all participants in the red teaming exercise, without whom this insight would not be possible.

Executive Summary

This study aims to enhance understanding of how terrorists might employ commercial unmanned aerial systems (UAS) in planning and executing attacks. It focuses on urban settings, recognizing their vulnerability with dense critical assets and populations combined with limited aerial defense infrastructure. As civilian UAS technologies mature, making advanced aerial platforms more accessible to malicious groups, this report emphasizes the need for properly scaled security frameworks to anticipate and intercept harmful uses while preserving legitimate applications.

The study utilizes red teaming, a simulation technique to explore adversary behaviors, to generate synthetic data on how violent nonstate actors may use UAS in urban attacks. The exercise was conducted online from November 2022 to January 2023, yielding 110 high-quality responses. Participants agreed to role-play as terrorists, select targets, and plan hypothetical attacks. Randomly assigned terrorist profiles—extreme left, extreme right, or jihadist—provided background narratives and immersive exercises prompted players to assume characters' motivations and perspectives. The profile-based subsamples exhibited different attack priorities, extremists prioritizing symbolism and civil disruption while jihadists emphasized casualties and property damage.

The exercise examined three categories of urban targets: energy, critical infrastructure, and population-centric sites. Infrastructure, particularly communication networks, was the most common target (50%), followed by population-centric locations (28%), and energy production (22%). Participants described hypothetical attack plans, most sketching courses of action involving drones for intelligence, surveillance, and reconnaissance (ISR). A substantial portion of respondents also articulated plans to use drones for kinetic attack, either to drop explosives or activate them upon purposeful collision with a target. Some also considered using drones as diversions, for propaganda, or for filming the attack.

Finally, participants ranked UAS features for planning and attack. The sample most valued the ability to penetrate secured areas and the aerial vantage point for ISR. Features that lowered risks and costs, such as performing ISR anonymously and evading detection, were also highly rated. In contradiction to existing literature, respondents de-emphasized UAS affordability. Overall, the study sheds light on the potential uses of commercial UAS by violent nonstate actors in urban attacks and underscores the importance of understanding their motivations and priorities for effective countermeasures.

Contents

About i

Acknowledgements ii

Executive Summary iii

Motivation 1

Methodology 3

Profiles 5

Extreme Left 5

Extreme Right 6

Jihadist 7

Target Trends 9

Most Likely Targets 11

Communications 11

Airports 11

Electrical Grid 12

Sports Arenas 12

Threat Vectors 13

Omission and Planning 13

Attacking 14

Most Likely and Black Swan COAs 15

UAS Features 16

Conclusion 19

Appendix 21

Motivation

Violent nonstate actors commonly exploit commercial unmanned aerial systems (UAS) for planning, smuggling, and attack. Attempted as far back as 1995,[1] prescient observers began expressing concern about the allure and implications of UAS for terrorist attacks by 2005.[2] Urgency increased around 2013 as the commercial industry matured, offering ever more advanced yet affordable models that militant organizations can repurpose to advance a violent agenda.[3] By the end of 2019, approximately 9% of active terrorist groups (6% if including groups that became defunct by this time) were deploying UAS.[4] With exponential diffusion through networks and stunning demonstration points of their utility (i.e., Syria, Myanmar, and Ukraine), this percentage is doubtlessly much higher by now.

Several nations, institutions, researchers, and stakeholders have recognized the risks of terrorist UAS in conflict zones and for domestic security. In particular, NATO,[5] the United Nations,[6] the Global Counterterrorism Forum,[7] and INTERPOL[8] are avidly conducting research, crafting guidance and best practices, and seeking solutions to regulate, disrupt, and mitigate emerging threats stemming from UAS misuses. Policymakers and security providers are challenged, though, to garner insights from

[1] Don Rassler, *Remotely Piloted Innovation: Terrorism, Drones, and Supportive Technology* (West Point, NY: USMA Combating Terrorism Center, 2016), 13-14, https://ctc.westpoint.edu/remotely-piloted-innovation-terrorism-drones-and-supportive-technology/.

[2] Jay Mandelbaum, James Ralston, Ivars Gutmanis, Andrew Hull, and Christopher Martin, *Terrorist Use of Improvised or Commercially Available Precision-guided UAVs at Stand-off Ranges: An Approach for Formulating Mitigation Considerations* (Alexandria, VA: Institute for Defense Analyses, 2005), https://apps.dtic.mil/sti/pdfs/ADA460419.pdf; Eugene Miasnikov, "Threat of Terrorism Using Unmanned Aerial Vehicles: Technical Aspects," *Center for Arms Control, Energy and Environmental Studies*, 2005, http://www.armscontrol.ru/UAV/rus/report.htm.

[3] Jackie Alkobi, "The evolution of drones: From military to hobby & commercial," *Percepto*, January 15, 2018, https://percepto.co/the-evolution-of-drones-from-military-to-hobby-commercial/.

[4] Kerry Chávez and Ori Swed, "The Empirical Determinants of Violent Nonstate Actor Drone Adoption," *Armed Forces & Society* (2023), first view online, https://doi.org/10.1177/0095327X231164570.

[5] James Rogers and Dominika Kunertova, "The Vulnerabilities of the Drone Age: Established Threats and Emerging Issues out to 2035," *NATO Science for Peace and Security Programme*, 2022, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/NATO_VDA_Policy_Report.pdf; Matthew Willis, André Haider, Daniel C. Teletin, and Daniel Wagner (eds). "A Comprehensive Approach to Countering Unmanned Aircraft Systems," *Joint Air Power and Competence Centre*, 2021, https://www.japcc.org/wp-content/uploads/A-Comprehensive-Approach-to-Countering-Unmanned-Aircraft-Systems.pdf.

[6] United Nations Office of Counter-terrorism, "Protecting Vulnerable Targets From Terrorist Attacks Involving Unmanned Aircraft Systems (UAS)," *UNOCT*, 2022, https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2118451e-vt-mod5-unmanned_aircraft_systems_final-web.pdf.

[7] Global Counterterrorism Forum, "Berlin Memorandum on Good Practices for Countering Terrorist Use of Unmanned Aerial System," *GCTF*, 2022, https://www.thegctf.org/LinkClick.aspx?fileticket=j5gj4fSJ4fI%3D&portalid=1.

[8] "Project Courageous," *INTERPOL*, https://www.interpol.int/en/How-we-work/Innovation/Project-Courageous.

a mosaic of limited empirical data. Furthermore, at this juncture empirical evidence is accumulating faster than practitioners can collect, systematize, and process it.

This study comes alongside these efforts to clarify, forecast, and edify "blue teams" the world over. Its purpose is to better understand how terrorists might use commercial UAS in urban attacks. Urban settings are especially vulnerable to novel attack approaches, being dense with critical and precious assets yet limited in defense architectures. The malign UAS threat is novel and increasing in breadth, frequency, variety, and lethality.[9] Furthermore, regulation of civilian UAS technologies is difficult and in many ways undesirable. This places greater pressure on security frameworks to anticipate, identify, and intercept harmful uses amid a great variety of good ones.

A key factor in overcoming novel, evolving, and complex threats like this is understanding how adversaries make decisions. This report leverages red-teaming data to excavate terrorist thought and decision processes related to urban UAS attacks. It aims to increase the resilience of NATO and EU member states' critical infrastructure and civilian populations by enriching scientific, technical, and policy communities to understand and adapt to how terrorists might leverage UAS.

[9] Kerry Chávez and Ori Swed, "Off the Shelf: The Violent Nonstate Actor Drone Threat," *Air & Space Power Journal* 34, no. 3 (2020), 29-43, https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-34_Issue-3/F-Chavez_Swed.pdf.

Methodology

Red teaming can be defined as “any activities involving the simulation of adversary decisions or behaviors, where outputs are measured and utilized for the purpose of informing or improving defensive capabilities.”[10] It is a technique to explore emerging threats, identify vulnerabilities, and raise awareness. Ideally, practitioners at all levels would proactively mitigate threats rather than react to real attacks. To keep pace with ever innovating adversaries, red teaming (and wargaming more generally) provides novel insights to white (analysts) and blue teams (security providers) to engineer practical, sustainable solutions; best practices; and standard operating procedures.

This exercise employed red teaming to generate synthetic data on how violent nonstate actors might deploy UAS in urban attacks. Specifically, participants were asked to play the role of a terrorist, select a target given one’s objective, and plan an attack given one’s resources. It was conducted online through the Center for Advanced Red Teaming at the University of Albany using Qualtrics from November 7, 2022 to January 22, 2023. Results discussed in this report reflect “high-quality” responses, or those in which participants completed the survey and evidenced appropriate attentiveness throughout. Fifty-one responses, failing to meet these criteria, were culled leaving 110 high-quality observations.

The exercise progressed in the following sequence:

1) In a preliminary section, participants were informed of the objectives, process, risks and associated resources, and ground rules. It was emphasized that the exercise is voluntary, and all data are anonymized. Each signaled full understanding by signing a consent form.
2) Participants completed a demographic survey capturing metrics on age, gender, education, and marital status. These measures enable statistical controls allowing analysts to identify the independent effects of the assigned adversarial role regardless of respondents’ backgrounds.
3) One of three terrorist profiles—extreme left, extreme right, or jihadist—was randomly assigned to each participant.
4) While reading their profiles, respondents were prompted three times to pause and write brief notes harnessing their characters’ thoughts and feelings. These immersions were aimed to facilitate appropriate internalization of the characters’ points of view.
5) Once immersed, participants answered a series of questions capturing overall aims in the attack (i.e., property damage, symbolic impact, etc.) and selected a target from a menu of options.
6) Participants then received a text message screenshot simulating contact from a “handler” that suggested commercial UAS as a potential tool. Each inject was designed to dovetail with the terrorist profile, yet was vague on possible

[10] Center for Advanced Red Teaming (CART), “Towards a Definition of Red Teaming,” *CART* White Paper, 2019, https://www.albany.edu/sites/default/files/2019-11/CART%20Definition.pdf.

applications of UAS. Participants were given optional time to perform cursory online research on this topic.

7) Based on all previous steps, players submitted a proposed attack plan. Following submission, each answered a series of questions capturing if / how UAS would be used in the planning or execution of the attack.

Profiles

Extreme Left

Thirty-two (29.10%) participants were assigned the extreme left profile. This narrative sketched a teacher fatigued by increasing demands and fewer resources amid a deteriorating, divisive society. The character reflected on the tensions between progress in social justice and resistance from the perceived alt-right, determining that demonstrations featuring damage have the greatest impact. Following a major policy reversal, the character responded to a social media call from a local activist to get more involved in efforts that coalesce in an attack on a major city.

> *And the administration...DON'T GET ME STARTED. I am only one person! There is not enough hours in the day to get everything done or taken care of.*

> *The system has been keeping us all low for so long...The housing zones, the income taxes, the sectioning based on how much we make, all designed to keep those who are down already nailed to the floor.*

> *We need to make a shock that shakes this world to change...If we want to see change, we have to make it, force it into being with real, raw action.*

The profile narrative unfolded across multiple screens in digestible segments. Participants performed three immersion exercises throughout to increasingly enter the headspace of the character. First, players were prompted to write a brief email to a fellow teacher about the struggles they were experiencing. Many tapped into the multiple pressures, stress, and exhaustion this character evinced, mentioning quitting and breaking points. At the same time, several emphasized the passion of teaching, showing engagement with the character's persona. Second, players were encouraged to write to their sympathetic colleague about the social injustice that most irks them. Despite the profile speaking of injustices vaguely, the most cited frustration was racial discrimination, followed by systemic barriers to equity of opportunities or income. Finally, participants were urged to write a note convincing the somewhat resistant colleague that action must be taken to remedy injustice. Most participants manifested the character's sense of urgency and impact. Overall, recipients of the extreme left profile demonstrated good engagement.

These players prioritized symbolism and civilian disruption in their attacks, rankings for both averaging at 3.4 on a 1 to 5 Likert scale. This is also shown in the kernel density plots in Figure 1, the black and bright blue lines piling around rankings of 4 and 5 clearly indicating their value. Meanwhile, extreme left profile recipients showed lower preferences for property damage (mean of 2.7) and the lowest for casualties (mean ranking of 2.4).

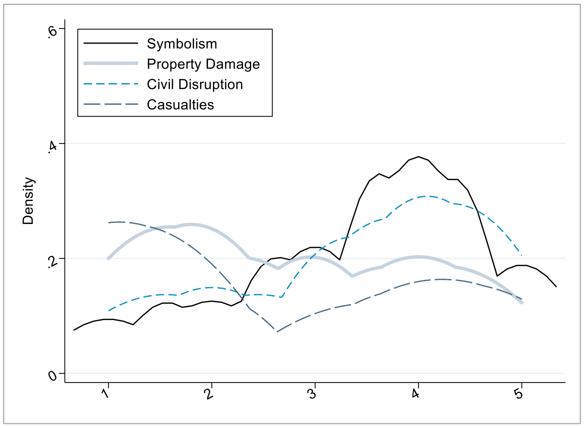


Figure 1.

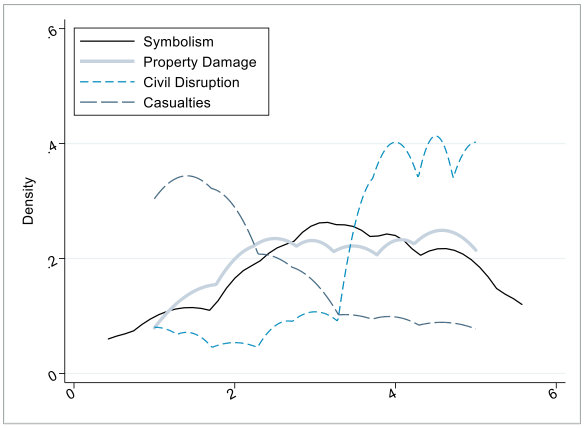
Extreme Right

Thirty-nine (35.45%) participants were assigned the extreme right profile, featuring a disillusioned veteran struggling to adjust to civilian life while working at a big box store. Feeling disconnected, this character joined an online forum where grievances were shared and stoked by a like-minded few. Citing past sacrifices and protection of the nation, the small group opted to capture attention and demonstrate the frailties of current policies by perpetrating an attack on a major city.

Again, the profile was delivered in discrete pieces to maintain attentiveness, with immersion exercises designed at intervals. First, players were prompted to author a brief post in the forum about their struggles. Most highlighted the meaninglessness and monotony of civilian life compared with the purpose of former service. Many also mentioned alienation, especially the dearth of understanding of the difficulty of the transition. Second, participants were urged to post about the grievance that bothered them most. The most common theme was a lament for the restriction of freedoms / intensification of governmental control, especially considering this character fighting for freedom. This occasionally coincided with frustration over increases in crime. Finally, individuals were asked to encourage a member of the core group that remained hesitant, emphasizing the need for action to correct what is broken. Many participants referenced oaths of office to protect the nation from threat. Like the extreme left pool, participants in the extreme right subset showed thoughtful immersion.

> *Hey brother, I know it's rough to transition back to the civ life...Now that we're out here doin bullshit work, jumpin through hurdles, payin bills, I really miss that feeling of purpose, drive, and belonging.*
>
> *The way the country's leadership has weaponized the pandemic to create an opportunity for them to gain more and more power over everyone by seizing their freedoms from them is ridiculous...Freedoms that we fought for.*
>
> *If we do this, we will preserve America as we know and love her. Of course it is not easy to come to this, but what must be done, must be done. This is our duty, This We'll Defend!*

Figure 2.



Turning to attack priorities, players who received the rightwing profile showed comparable rankings for symbolism (mean of 3.3, -0.1), but considerably higher rankings for property damage (3.4, +0.7) and civil disruption (3.9, +0.5). Conversely, this group ranked casualties lowest of all priorities (mean of 2.2, -0.2 compared to extreme left and -1.4 compared to jihadists). In absolute terms, the extreme right appears to place the highest value on civil disruption, illustrated in Figure 2.

Jihadist

Thirty-nine (35.45%) participants were assigned to the final group featuring jihadist ideology. This narrative articulated disillusionment at the menial, unfulfilling nature of life working at a technology store. Facing depression, the character's cousin offered answers and hope in religion that transcends dull reality and infuses meaning. Yet this new meaning contradicts what society upholds as valuable and true. With resentment and a renewed mission to correct the cosmic record, participants with this character planned an attack in league with their cousin linked to a foreign group.[11]

> *Life has taken so many turns that I didn't plan or even agree to. Work is a life sucking black hole...My life has no meaning and I am just a drone fulfilling required functions. How do I get off this hamster wheel to nowhere?*

> *This notion of "freedom" is a cancer. The world dies because the few believe the freedom to consume everything is the pinnacle of human existence. It isn't. I call it what it is: an imperialist dogma that makes Columbus look like a Girl Scout peddling a hypocritical book.*

> *Allah holds the key to true happiness...People do not deserve to live unhappy and depressing lives as I once did. Society will no longer hold them down, as I will help spread the message that jihad had spread to me.*

The immersion exercises for the jihadist profile began with participants receiving space to write a brief email to the character's cousin about their struggles. Many reported confusion and depression that formulas for success did not pan out or yield happiness, respondents seeking advice on how to attain both. Second, players identified the discrepancy / hypocrisy between Western scripts and spiritual truths that most trouble them. Responses centered on the tension between political and religious notions of freedom, often criticizing wealth and consumerism, democracy, and superficiality. Last, participants crafted a note to ensure their cousin of their conviction and trustworthiness to carry the banner of jihad in the attack. Several made compelling rallying cries on behalf of jihad, a good signal that players internalized the characters' world view even if initially distant. Like the other two profiles, the open-ended immersions engender high confidence that the profiles were taken seriously.

The most distinct departure from past profiles was how highly jihadist players ranked civil disruption (mean of 4.3, +0.9 from leftists and 0.4 from rightists), shown in Figure 3. Although this outstripped other priorities, jihadists also ranked casualties the highest of the groups, the mean ranking reaching 3.6 (+1.2 from left, +1.4 from right). While this might not stand out in the figure comparing only jihadist rankings, it is stark in Figures A4 and A5 in the Appendix that chart priorities for all groups in a

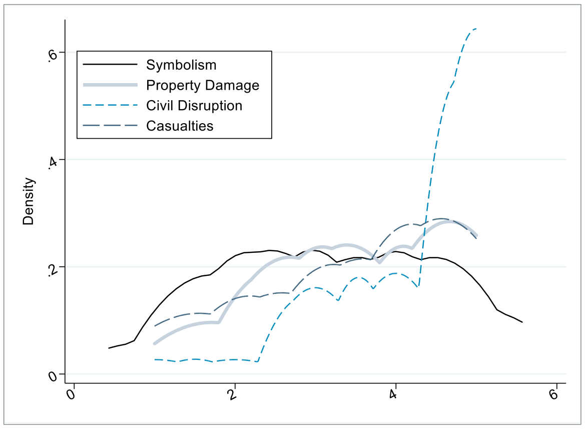


Figure 3.

[11] All participants are informed that they have the same resources: "some rifles and handguns, ammunition, 10kg of explosives, and 50K in currency."

comparative format. Furthermore, jihadist participants lodged the highest prioritization of property damage (3.7 relative to 2.7 for the leftists and 3.4 for rightists). The only criterion on which jihadists yielded a lower average ranking was symbolism, having an average score only 0.1 to 0.2 less than the others, respectively. The upshot is that jihadists might be more radical across the boards, ambitioned to cause damage and signal resolve however possible.[12] The Appendix provides more comparative descriptive statistics, graphing the rankings of each attack priority side-by-side, disaggregated by profile in Figures A1 to A4 and each profile group's mean prioritization of attack priorities in Figure A5.

[12] Asal and Rethemeyer (2008) demonstrate that terrorist groups with a "supernatural audience" are more lethal in their attacks. Victor Asal and R. Karl Rethemeyer, "The Nature of the Beast: Organizational Structures and the Lethality of Terrorist Attacks," *Journal of Politics* 70, no. 2(2008), 437-449, https://doi.org/10.1017/S0022381608080419.

Target Trends

One of the primary interests of this study is to ascertain likely targets and rationales. Urban settings are dense with valuable and critical assets. Striking or disrupting certain targets can yield greater lethality, costs, and reverberations to other areas, even from a small-scale attack. Yet defending all urban sites all the time is uneconomical and logistically infeasible. Security providers face the daunting task of allocating scarce resources and attention to mitigate probabilistic attacks. The recent advancement and diffusion of commercial UAS has increased the number and type of actors in the air, a vector against which few stakeholders have secured or even considered. The combination of these factors implies a disquieting vulnerability that states and localities must promptly address.

This study focused on three areas of high concern in urban environments: energy, critical infrastructure, and population-centric sites. Surprisingly, 50% of participants selected infrastructure as the final target. More surprising, this was strongly driven by the selection of communication networks (31.8%), although airports were the second most chosen target (12.7%). Respondents selected energy production targets 22% of the time,[13] the electrical grid being the most likely at a similar frequency to airports (11.8%). Participants opted to target population-centric locations 28% of the time, but this is largely a jihadist choice as shown in the rightmost bar in Figure 4.[14] This pattern epitomizes how much target selection varied by terrorist profile, even within categories. In fact, this is a prominent analytical and policy takeaway from this study. Each political space harbors distinct societal cleavages, grievances, and terrorist tendencies. Nations with higher concerns over radicalized factions on the left might emphasize different assets or attack logics and courses of action than those concerned about the radicalized right or jihadist groups.

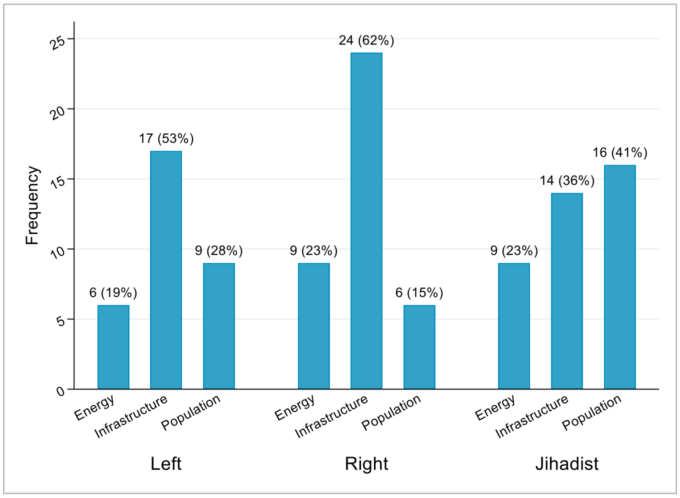


Figure 4

[13] The infrastructure and population categories have four target options while the energy category has only three, possibly underestimating its relative ranking.

[14] A detailed display of final target selections, listed alphabetically within energy, infrastructure, and population categories, is available in the Appendix in Figure A6.

The variation in target selections by terrorist profile is most apparent in Figure 5. For energy targets, participants assigned extreme left profiles homed in on oil / gas sites while those with extreme right and jihadist profiles most often selected the electric grid.[15] The large finding for infrastructure in general and communications in particular is a function of the radicalized poles,[16] yet jihadists are much more prone to target airports.[17] Jihadist characters emphasized population-centric targets most, focusing on mass gatherings at concerts and sporting events rather than lower but regular foot traffic and occupancy at malls and hospitals.[18]

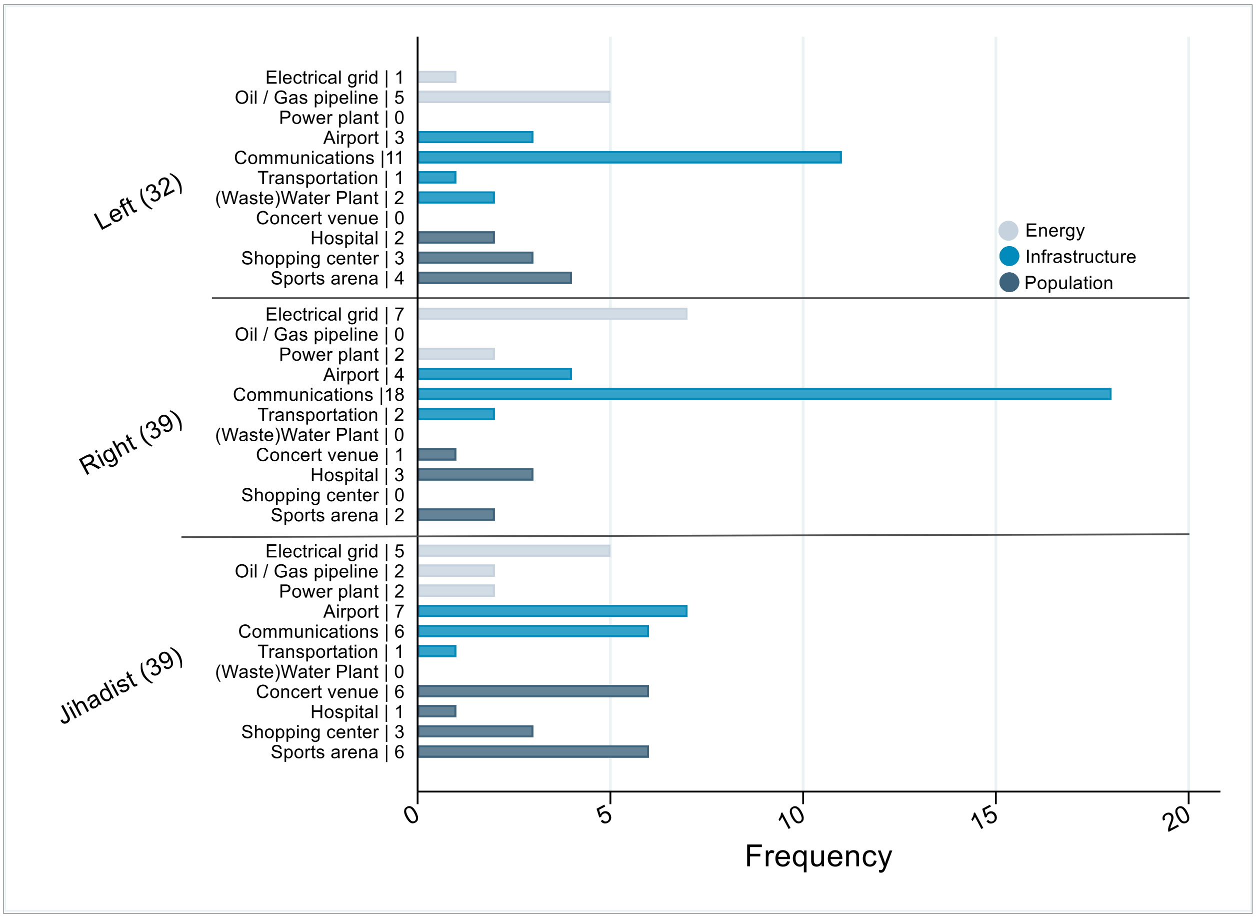


Figure 5

[15] Only 1 participant who selected the energy grid was given a leftist profile (8%), this stemming mainly from rightist players (50%) and jihadist characters (39%).

[16] 31.5% of participants who chose communications as the final target were assigned to the extreme left profile, 51.5% received the extreme right profile, and only 17% came from the jihadist profiles.

[17] 50% of those who selected airports as the final target were jihadist characters, 21% being extreme left and the remaining 29% coming from extreme right players.

[18] The fourth most popular target was sports arenas. Of the twelve individuals who selected it, 50% were assigned jihadist profiles, 33% extreme left, and 17% extreme right profiles.

Most Likely Targets

Communications. A surprising outcome of the study is the high frequency at which participants targeted communications networks. Not only was it the most common final target chosen, but it was highly ranked by many other players who opted for a different final choice. Figure A7 in the Appendix shows that an additional 34 participants ranked communications as their second or third choices, a remarkable 63.6% of the full sample considering this target in their top three. Participants provided their rationales in an open-ended text box entry upon making final selections. The handful of players with jihadist profiles were almost universally motivated by maximizing chaos and damage, especially limiting the provision of emergency services, repairs, and intelligence to coordinate a response.

Justifications for participants with extreme left and right profiles were more nuanced. Both sides emphasized undercutting misinformation, fake news, and government or mainstream media propaganda. Both sides also reasoned that disrupting communications would garner the most attention from the mass public, reliance on this network being deep in the digital age. Indeed, two thirds of players targeting communications highly ranked civil disruption as a priority in the attack. Respondents with the extreme right character also emphasized that this target would have a large impact, but with the fewest casualties. This coincides with priorities individuals expressed prior to selecting this target, 51% ranking casualties at the lowest level and 23% ranking it as only slightly important. Finally, a vivid theme from rightist players emphasizes the symbolism of the communication network medium (51% ranked symbolism as a high priority). Several referenced a supposed monopoly of information flows by government and progressive actors that an attack would disrupt. Some also cited difficulty having their voices heard in the political environment and the opportunity to directly deliver a message without censorship or spin.

> *A COMMUNICATIONS NETWORK SYMBOLIZES THE TRANSFER OF PROGRESSIVE IDEOLOGIES AND OTHER SYSTEMATIC GOVERNMENT OPERATIONS THAT MY CHARACTER DISAGREES WITH.*

Airports. This was the second most likely target, selected by 12.7% of participants. Given precedents of terrorist attacks on the aviation industry, this is an intuitive finding. Indeed, practitioners and security providers already focus on airport defense and security, including in response to the expansion of commercial UAS. For instance, INTERPOL conducted a live technology assessment of counter-drone solutions at Oslo Airport Gardermoen in 2021 to better understand their effectiveness in operation in a live, dynamic environment.[19] Jihadist characters were most likely to target airports, and rationales given are exclusively about maximizing casualties: “number of people located in one place,” “it would cause numerous casualties,” “most amount of people in it,” “crowd.” The number of players from left and right profiles who selected airports are fewer, so rationales are more scattered and anecdotal. Nonetheless, the extreme

[19] INTERPOL, “Drone Countermeasure Exercise Report: Technology Assessment of C-UAS within an Airport Environment,” *INTERPOL Innovation Centre*, 2022, https://cuashub.com/content/interpol-drone-countermeasure-exercise-report/.

left profiles commonly emphasized logistical ease, such as “large area so easy to move around” and “large, sprawling relatively easy to hit.”

Electrical Grid. This target was selected at a similar rate to airports, ranking in the top three target choices at an even higher frequency. Across the boards, rationales for this target rest on civil disruption. Figure 6 depicts the attack priorities for those who opted to hit the electrical grid. The rankings for civil disruption in the bottom left pane are highly skewed toward this feature, having no values at 1 (not at all important) or 2 (slightly) and most of them at the maximum value of 5. For all other attack traits, the distributions are more uniform and uninformative. This priority comes through in the open-ended text responses as well. Most respondents emphasized how disruptive it would be if the grid went down, including spilling over to other sectors that depend upon it (i.e., transportation, communication). One unique theme surfacing from jihadist characters was the symbolism of cutting off power users. For example, one mentioned how satisfying it would be to stop society from plastering “unrealistic thoughts through social media,” while another suggested that electricity consumption symbolizes indulgence, overuse, and hypocrisy. For various reasons, the electrical grid seems a moderately attractive option for urban terrorist attacks.

> *EVERYTHING RUNS OFF OF THE ELECTRICAL GRID. HOSPITALS, EMERGENCY SERVICES, TRAFFIC LIGHTS, FUEL PUMPS, COOLING SYSTEMS, PHONES, COMMUNICATIONS, AND LITERALLY EVERYTHING ON THIS PLANET.*

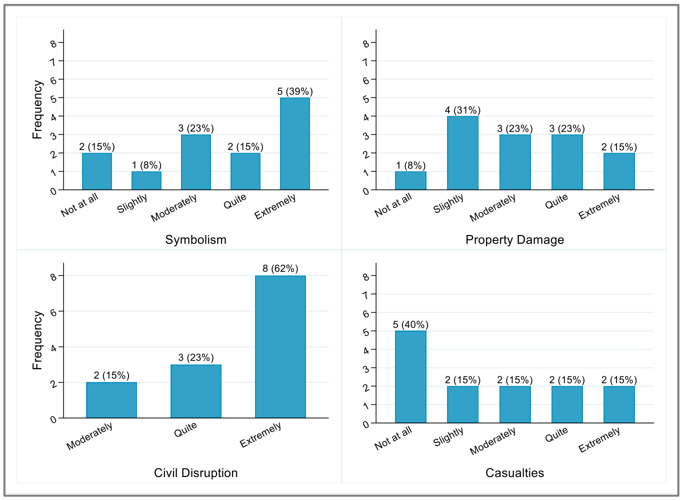


Figure 6

Sports Arenas. With 10.7% of participants opting to target a sports arena, this was the fourth most likely option. Jihadist characters gravitated toward it more, namely for the large crowds and high amount of instant publicity an attack would garner. Players with leftwing profiles also emphasized the allure of impacting large crowds onsite and through television. Other reasons respondents cited included the lack of defensive countermeasures (jihadist); that sports are a distraction from more important endeavors (left); and that arenas would disproportionately impact the affluent owners, players, and attendees (left and right).

Threat Vectors

Omission and Planning

Despite the upfront description of the study's focus and the strength and timing of the inject promoting participants to consider using UAS, 19 (17.27%) individuals opted not to use drones in any portion of the planning or attack. This is a vital takeaway for analysts and practitioners. UAS use in terrorist attacks is not a story of technological determinism, but one of human agency and affordance.[20] It is also a function of relative utility and reliability. Five of the players who did not turn to drones described attack plans using simple firearms, three selected emplaced or suicide explosives, and seven described cyberattack strategies. Depending on the goal and the site, UAS are not always the most obvious or appropriate tools. In fact, seven of the attack plans pertaining to communications targets omitted drones, meaning that the attention this sample paid to the target does not imply it is solely vulnerable to aerial threats.

This logic was reinforced by the plans that elected to use drones only for planning purposes. Indeed, ISR efforts are the primary ways that violent nonstate actors deploy UAS. Seventeen players articulated plans to gather ISR on site layouts, access or weak points, security measures, and foot traffic prior to waging a more conventional attack with firearms or explosives. The choices to overlook UAS or use it more passively for pre-attack observation and planning were not specific to any target or terrorist profile. Illustrated in Figure 7, that approximately one third of participants (32.7%, 36 respondents) designed courses of action without weaponized drones in a study that soundly primed this is quite instructive.

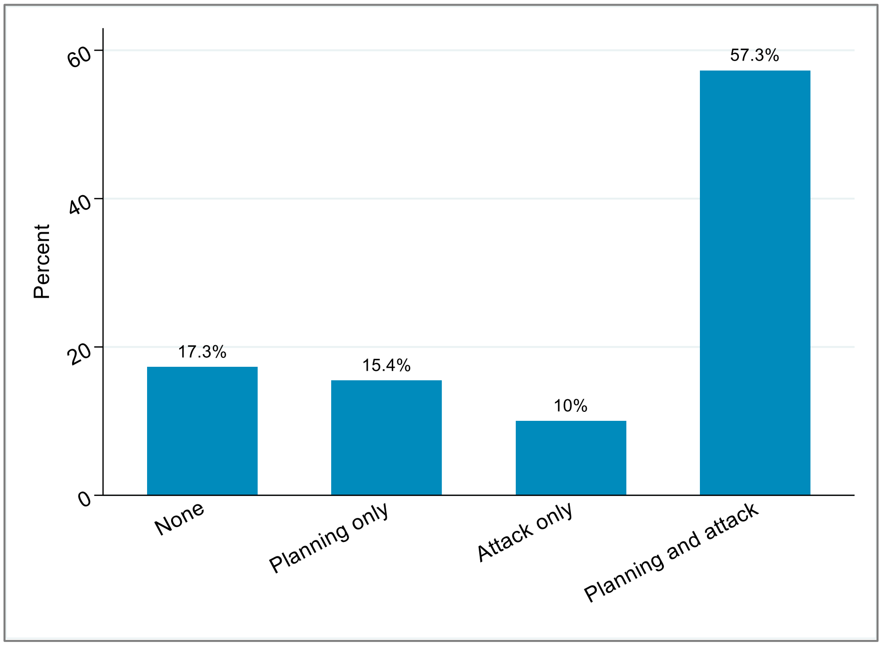


Figure 7

[20] Affordance refers to the action potential a user sees in a given technology, which may or may not coincide with the uses intended by a manufacturer. See Samer Faraj and Bijan Azad, "The Materiality of Technology: An Affordance Perspective," in *Materiality and Organizing: Social Interaction in a Technological World,* ed. Paul M. Leonardi, Bonnie A. Nardi, and Jannis Kalliniko (Oxford University Press, 2012), 237-258.

Attacking

The second main interest of this study is attack courses of action (COAs) using UAS. After submitting detailed attack plans in open-ended text boxes, participants answered a series of questions related to how drones would figure in the operation: to deliver materials discreetly or to areas of limited access, as a diversion, to film the attack for public consumption, for ISR, to deliver an explosive payload, or other. Table 1 provides a breakdown of the frequency of applications. None of the plans entailed using a drone to transport materials to a target site for delayed or real-time reception by the attack team. In all cases involving cargo, teams either brought it on their persons or drones delivered payloads directly without going through human hands for assembly or placement. This was somewhat surprising given the high frequency with which criminals transport contraband into prisons and in smuggling schemes. It is possible that the intensive terrorism priming precluded respondents from considering habits more common to criminal and cartel actors.

Table 1

UAS Attack Deployment	
Cargo / Delivery	0 (0.0%)
Diversion	9 (12.2%)
Film / Propaganda	11 (14.9%)
ISR	42 (56.8%)
Explosive payload	57 (77.0%)
Other	7 (9.5%)

Nine individuals sketched plans to use drones as a diversion. The majority (5) intended to distract security officials and first responders from the substance of a conventional attack with firearms and explosives. Two described plans to deploy a cluster of UAS to overwhelm mitigation efforts so that at least one armed platform penetrates defenses. The final two discussed using drones to probe security responses to calibrate the attack. A small margin of more players indicated that they would use drones to film the attack for a publicity or propaganda angle. That said, only four participants explicitly cited this in the attack plans, such as “I would focus on drones producing images, recording video, documenting the attack to be used for propaganda purposes.” The others appeared to see filming the attack as an add-on feature that UAS offer but not the main thrust of their purpose. Furthermore, many shied away from filming to minimize the risks of being tracked and caught.

In well over half of the attack plans, players expressed intent to rely on drones for sustained aerial ISR to monitor unfolding attacks. Given the empirical precedent for this and the penchant among participants to use ISR drones for planning, this is an intuitive finding. The most popular application of UAS in the attack plans was weaponization with explosives, over ¾ of respondents who included drones in the attack using them this way. Five players described specific plans to use them as loitering munitions. For those who sketched plans to drop munitions, 21 explicitly named property damage as the goal while 17 designated humans and crowds as the target. Of the latter, nine of these were jihadist characters targeting population-dense locations: concert venues (2), shopping centers (1), and sports venues (6). For the remainder, four extreme left characters also focused on malls (2) and sporting arenas (1) while the last sketched a plan to target a hospital. Two extreme right players also opted to send weaponized drones to a hospital, and two expressed a targeting focus on casualties at an airport.

> *There will be C4 attached to 3 of the drones and a Molotov cocktail attached to the other. We will fly the drones in, Kamikaze style, and blowup the main control hub disrupting the whole grid.*

Most respondents calibrating drone attacks for property damage focused on communications or energy targets. Many were careful to emphasize casualty avoidance in their narratives, seeking disruption and attention but not death. Sixteen described plans to disable communications networks using UAS, eleven of these being extreme right profiles. A separate group of eleven participants focused on attacking the electrical grid with drones, only one being leftist and the remainder being split between rightist and jihadist characters.

> *A drone will be used to target telephone lines and internet cables. Upon reaching their targets, the drones will deploy a device…able to explode, causing damage to the lines but resulting in no direct casualties. The goal is to instill fear and panic, not violence.*

> *Explosives will be strapped to the drone and will dive into the identified vulnerable parts of the electrical grid.*

> *We will try to attack [the power plant] during shift change in an attempt to lesser the number of human casualties as we are aiming for the facility, not the civilians.*

Respondents who developed "other" means to employ UAS in the attack evidenced considerable creativity and ambition. One suggested that drones be outfitted with electronic warfare capacities to disable critical operations. Another planned to drop smoke bombs to obscure attackers' exit from the site. A third planned to disrupt the electrical grid by dangling carbon filaments over key areas, a COA that is not without precedent. A final example involved towing tablecloths with quotes displaying the terrorists' ideology over a crowd at a sports' stadium, not unlike an advanced (being unmanned) yet antiquated (being table linens) skywriter.

Most Likely and Black Swan COAs

From this study, the most common COA overall was utilizing drones for ISR during planning, then dropping explosives on key communications or energy targets at points of vulnerability (nearly one third of all respondents). This was also the most likely outcome for extreme right players, their consistency influencing the broader finding to a degree. Players assigned to the extreme left exhibited high variability in their COAs, using them for weaponized attack only one third of the time against both property and human targets and deploying them for propaganda, in tandem with conventional attack formats, and in other uses more widely than other profiles. Leftist players were also the least likely to use UAS in general, just over half using them for planning and exactly half using them in attacks in some manner (only 19% for strikes). The jihadist characters were most likely to use UAS during the planning phase, only two individuals opting to use them only during attack. The most likely jihadist attack COA was to drop munitions at crowded venues, especially sports arenas. In fact, this was the sole COA described for all jihadist characters who targeted a sports venue.

The two plans depicting the most catastrophic results (if successful) both focused on stadiums. In the first, a jihadist character described an initial explosive delivered by drone into the stadium and detonated near fans, causing some casualties but more chaos. A second fleet of armed drones would then drop explosives at all exits and in concentric rings in the walkways and parking lots. In the second plan, a leftist profile sketched a strategy to preprogram several agricultural UAS toward an arena center that would disperse lethal chemicals en route, within, or if shot down.

UAS Features

Following descriptions of the attack plans and potential UAS deployment, participants ranked ten features of drones purported to be meaningful in coercive uses. The two reported to be most valuable were the ability to penetrate secured areas and the aerial vantage point for ISR, shown in Figure 8. Sixty percent ranked penetrative reach at its maximum value labeled "extremely important" and an additional 22% considered it "very important."[21] The skewed favorability for aerial view is smaller, but still distinctive with 42% considering it extremely important, 29% very important.

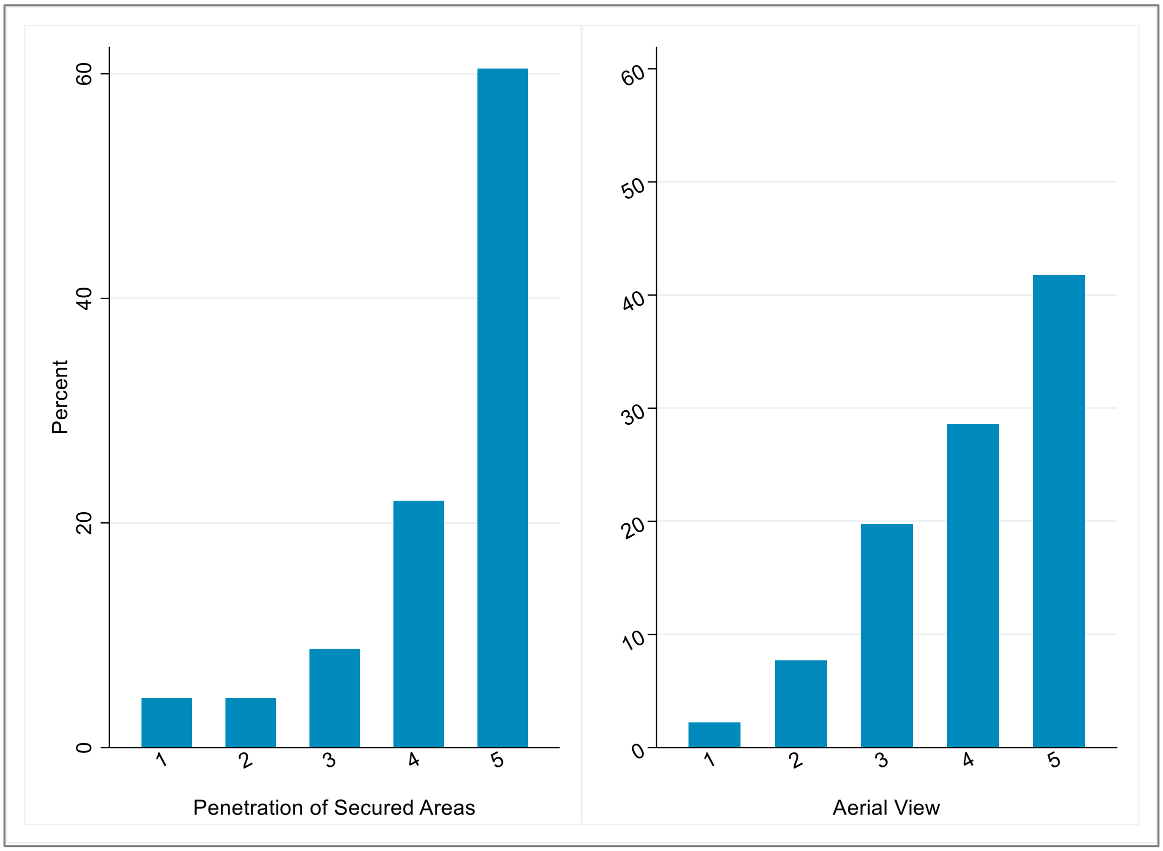


Figure 8

Of the broad UAS properties that diminish risks and costs, two were ranked well and two were discounted. Displayed in Figure 9, the ability to perform ISR and attack more anonymously with UAS (upper left panel) was highly valued by nearly half of the respondents but not as uniformly popular among the rest. The same pattern obtains at more muted levels for a team's ability to evade detection (upper right panel). Players did not place as much value on drones' ability to lower overall risks and on their

[21] Percentages for the first six feature rankings are calculated from the subsample of participants who chose to use UAS in the exercise in planning and attacking activities, including 91 observations.

affordability. This contradicts the scholarly literature analyzing why violent nonstate actors exploit commercial UAS.[22] It might be the case that the red teaming exercise biased against this by depicting a one-shot attack with ample currency to wage it ($50K). Most armed nonstate organizations wage a continuous stream of attacks, making them more inherently and acutely aware of resource constraints.

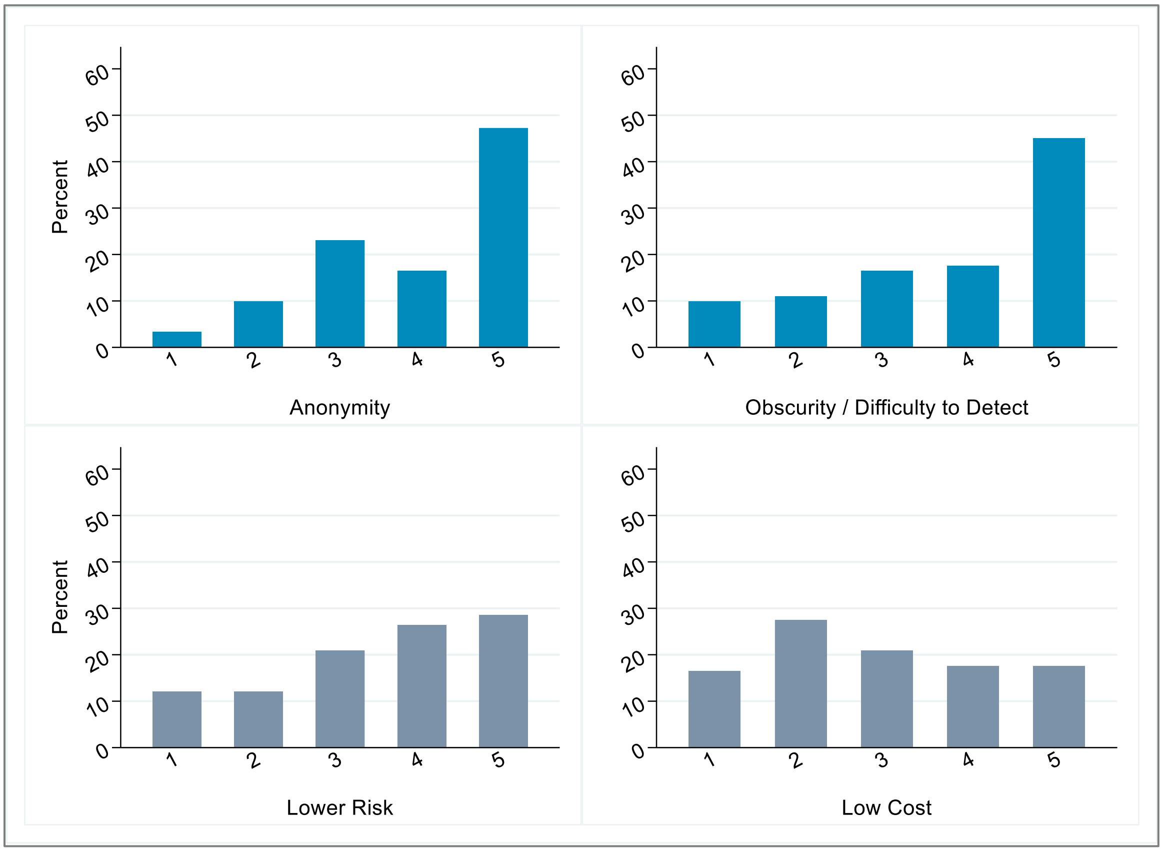


Figure 9

Finally, respondents ranked four drone attributes useful primarily in attack, depicted in Figure 10. Half of the players who employed UAS in the attack (not solely for planning) evaluated speed as extremely important and nearly 40% considered it moderately to very important.[23] Many also appeared to appreciate the ability to attack from the air, 42% ranking this at the highest value and an additional 45% indicating it is moderately to very important. The distributions of rankings for the flexibility of commercial UAS to perform multiple tasks (i.e., ISR, filming, payload delivery) and for the novelty of attacking from a civilian unmanned platform were uniform, suggesting a mix of considerations with no clear trend. Overall, the exercise affirmed some empirical patterns and revealed others that might indicate new trends or nuances that merit further research.

[22] Kerry Chávez and Ori Swed, "The Proliferation of Drones to Violent Nonstate Actors," *Defence Studies* 21, no. 1 (2021), 1-24, https://doi.org/10.1080/14702436.2020.1848426.
[23] Percentages for the final four feature rankings are calculated from the subsample of participants who chose to use UAS in the exercise in attacking activities, including 74 observations.

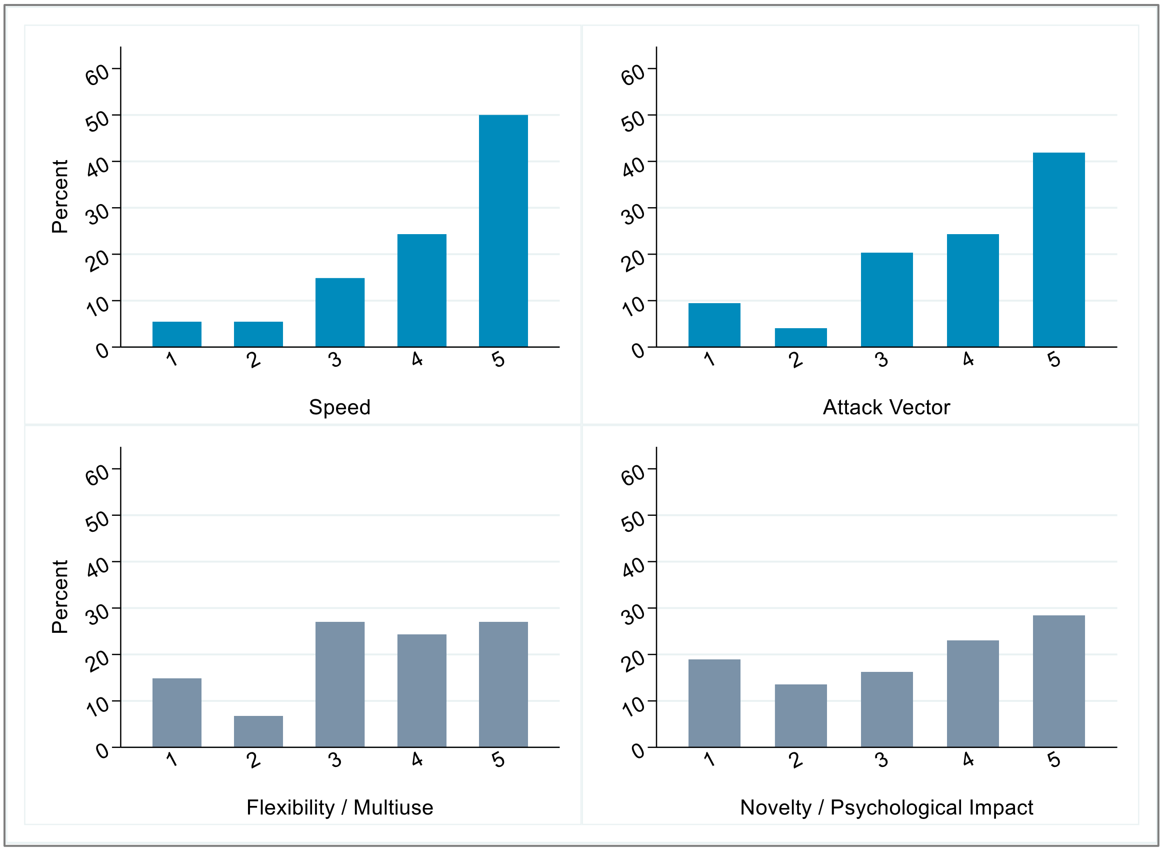

Percent
0
10
20
30
40
50
60
1
2
3
4
5
Speed
Attack Vector
Flexibility / Multiuse
Novelty / Psychological Impact

Figure 10

Conclusion

This study, and the working group mounting and supporting it, set out to gain insight into how terrorists might leverage commercial UAS technologies against urban targets. Ultimately, it aims to enrich the development, coordination, and implementation of best responses to defend sensitive and precious assets. By simulating and analyzing how adversaries consider UAS platforms in their arsenals, it furthers understanding of this diverse, growing threat. Furthermore, it will help practitioners to discern between licit and malicious agendas with drones so that the former can be maximized for societal gain, the latter mitigated.

The findings in this report are based on synthetic data, generated through a carefully designed red teaming exercise. Valid, reliable data are vital to develop prudent policies and pointed security frameworks. There are ample precedents, demonstration points, and a growing list of threats of terrorist UAS deployment. Yet given the emerging nature of the threat and evolving nature of the technologies, systematic empirical data remain limited. Rather than wait for more instances to accumulate and data collection efforts to be fielded, we leveraged red teaming techniques to simulate them to stay on the leading edge of the threat.

While synthetic data are valuable, especially amid high stakes and a dearth of empirical evidence, they are limited. They should be used conservatively, wisely, and in conjunction with empirical data for any trend forecasting or policy formulation. In addition to its reliance on synthetic information, this study is limited in other ways. First, it has a relatively small *N* of 110 high-quality responses. Consequently, it is low in statistical power and possibly skewed from the population average. Second, it features only three terrorist profiles. Given the heterogeneity of responses among profile subsamples, stakeholders should be cautious about extrapolating patterns to other terrorist types. Third, all participants were assigned the same resources (cash, weapons, UAS) whereas terrorist resources vary dramatically in reality. Future studies should examine how different levels and types of resources influence affordance and drone use among violent nonstate actors.

Finally, the study is limited in external validity in a few ways: 1) conducted in a one-shot experience while radicalization and cultivation of illicit ingroup trust is long-term and incremental, 2) conducted in a brief time slot to maximize participation whereas attack planning takes much longer, 3) conducted online and alone whereas these processes often occur in person and in small groups; and 4) conducted with a diverse demographic sample whereas individuals prone to select into terrorism tend to exhibit narrower demographic markers. In sum, we are transparent about these tradeoffs but enthusiastic about leveraging all approaches, resources, and knowledge to equip blue and white teams.

There are three key takeaways that blue teams should regard from this report and its inferences. First, target selections and COAs are a strategic human choice stemming from agendas, opportunities, and constraints. Political spaces vary across nations and localities. Insofar as terrorist organizations tend to construct and dwell in their own bubbles of reality, the way they observe, internalize, and interpret affordance for UAS varies. Consequently, there is variation in the degree to which groups deem them attractive or useful, appropriate for a given task or setting, and preferable relative to other platforms and weapons. Blue and white teams should partner to take stock and keep tabs on the social and political landscape to isolate prominent grievances, dark networks, and demonstration points to discern if and how UAS might constitute a security threat in the first place.

Second, not all targets are equally vulnerable. Given that security resources are finite and security threats are many and diffuse, it would not be appropriate to transfer them toward defending assets of nominal risk. Defense must abide by a vulnerability vs. value logic (not unlike insurance) that protects the most probable and catastrophic targets. The results of the red teaming exercise suggest that communications, airports, sports arenas, and the electrical grid are most likely to be attacked and that if successfully black swanned, sports arenas would involve the most casualties while the electrical grid would have the largest civil disruption. This should be squared with empirical evidence and additional wargame exercises and simulations. From these, stakeholders should develop a taxonomy of targets to harden against aerial attack, then map responsibilities and coordinate resources across industry, local, and federal levels.

A third implication, crystallized based on the courses of action, is that defense of a given asset should be shrewdly tailored and scaled. Security provisions at a high-attendance sports match should look drastically different from any permanent installations on the electrical grid. Furthermore, if aerial defense is merited, solutions must account for and integrate with existing security systems, perhaps even economizing costs by building upon or embellishing extant infrastructure whenever possible. The upshot is that perpetrating an attack with a commercial off-the-shelf drone is quite inexpensive and adaptable, so defending against this threat must be similarly cost-effective and agile to be feasible and remain sustainable. As global partners continue to address the emerging threat of terrorist UAS attacks on Western and urban targets, we hope this report makes a substantive contribution.

Appendix

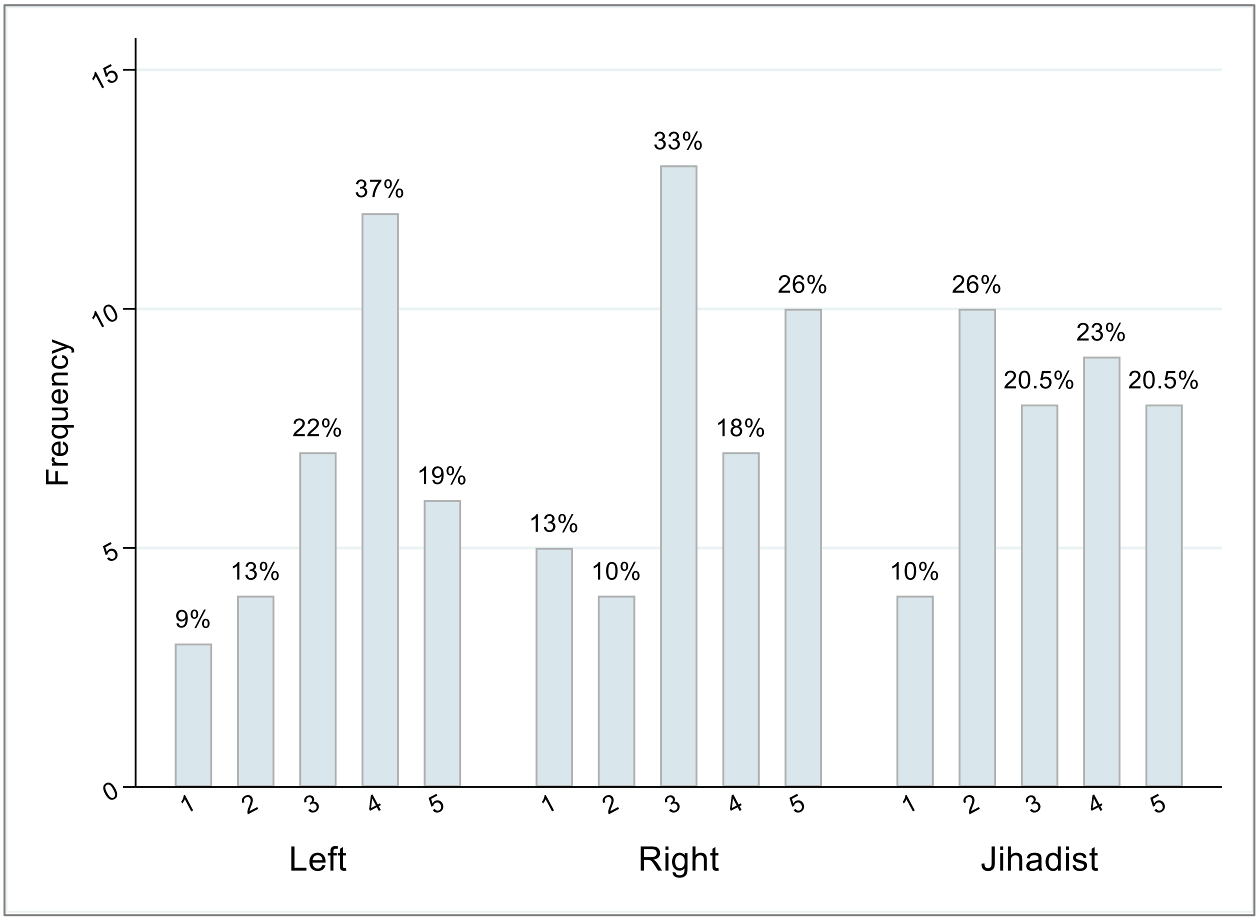


Figure A1. Rankings of **symbolism** as an attack priority, disaggregated by profile. Percentages are calculated within each profile category.

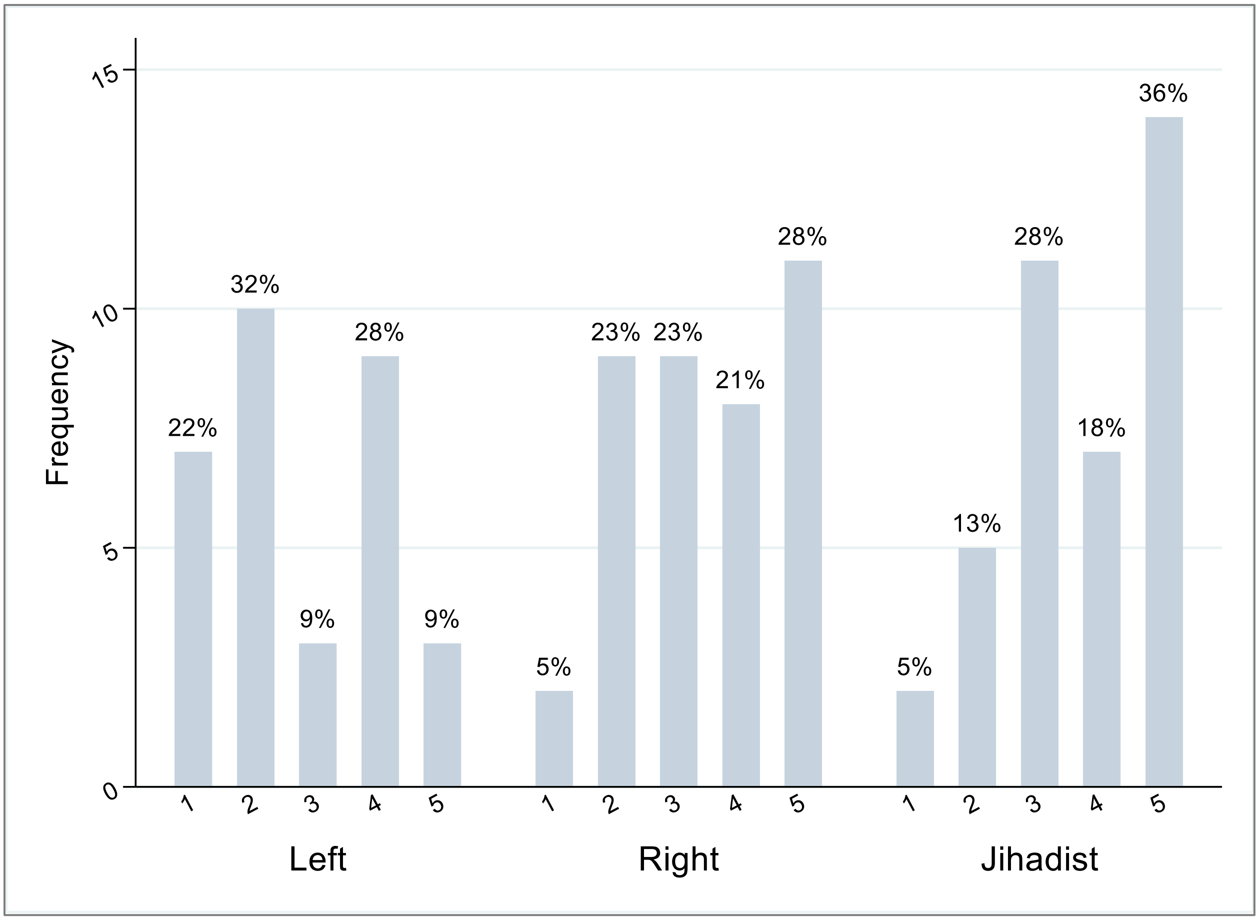


Figure A2. Rankings of **property damage** as an attack priority, disaggregated by profile. Percentages are calculated within each profile category.

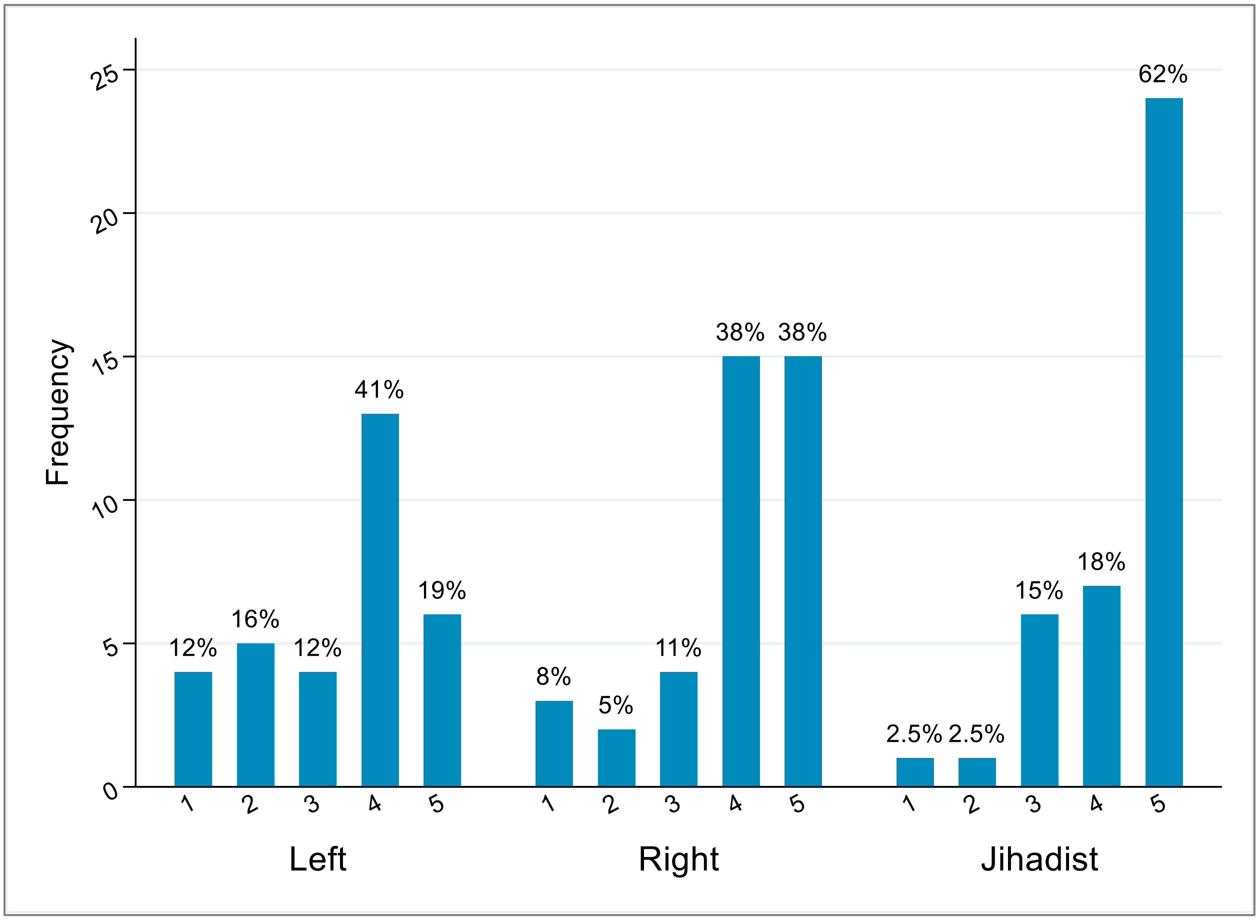


Figure A3. Rankings of **civil disruption** as an attack priority, disaggregated by profile. Percentages are calculated within each profile category.

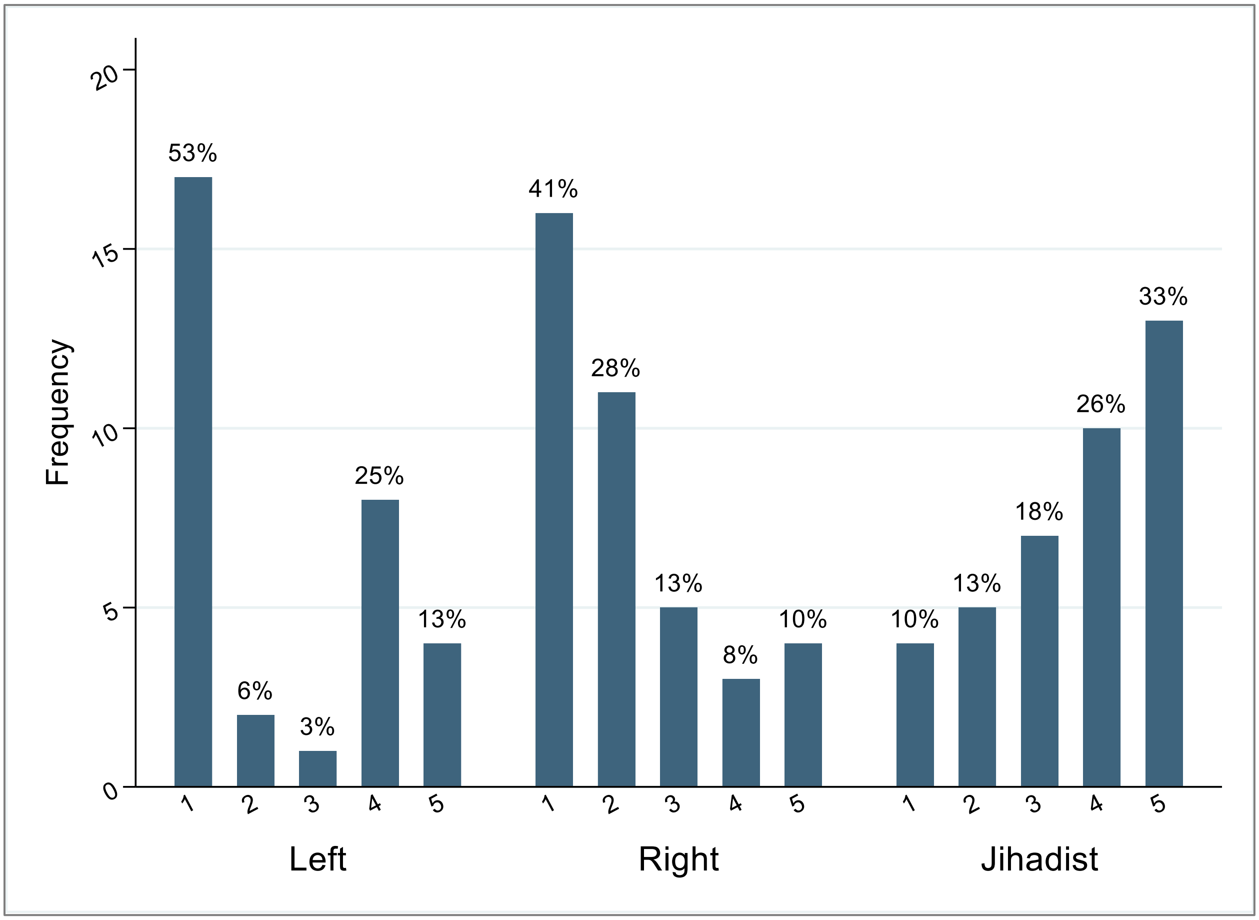


Figure A4. Rankings of **casualties** as an attack priority, disaggregated by profile. Percentages are calculated within each profile category.

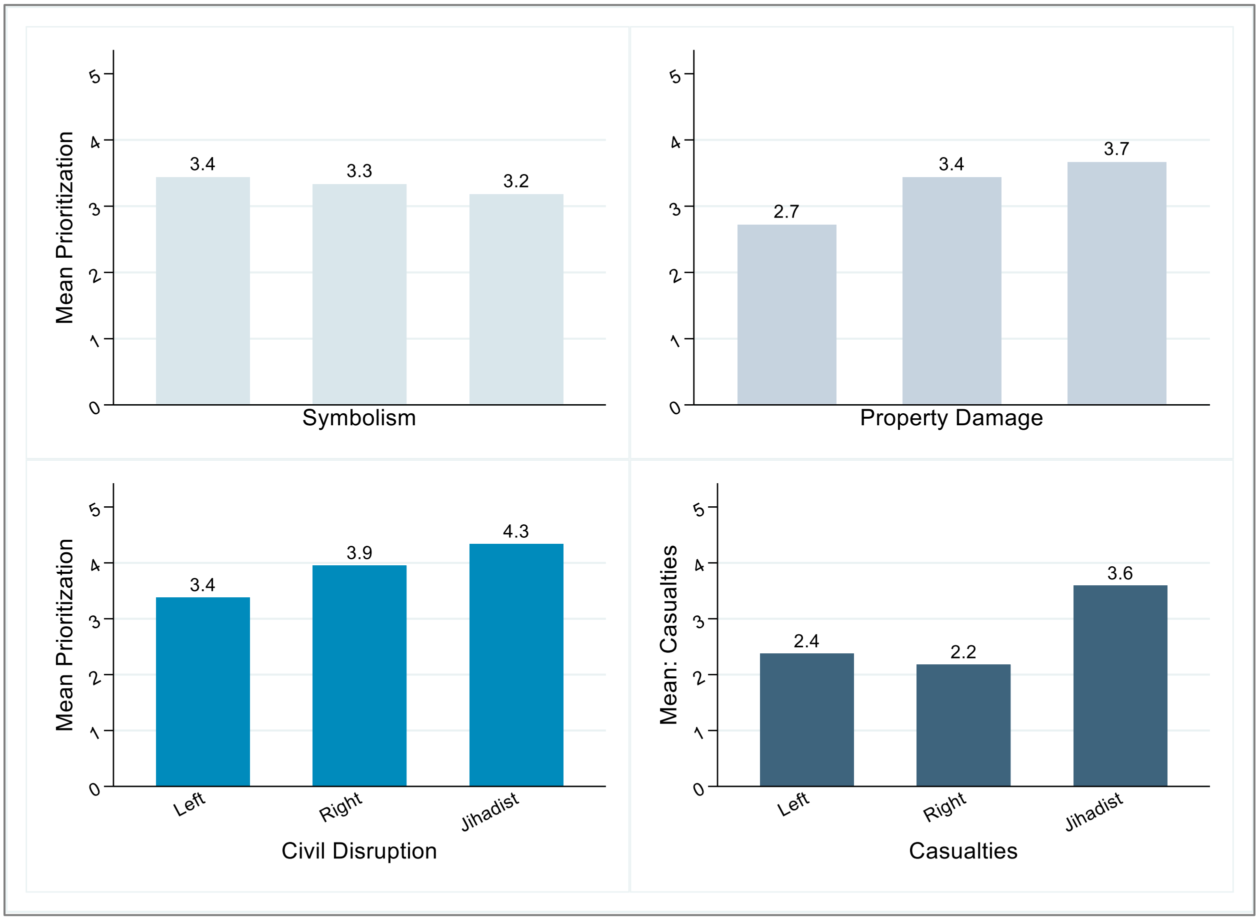


Figure A5. Mean prioritization of each attack priority, disaggregated by profile.

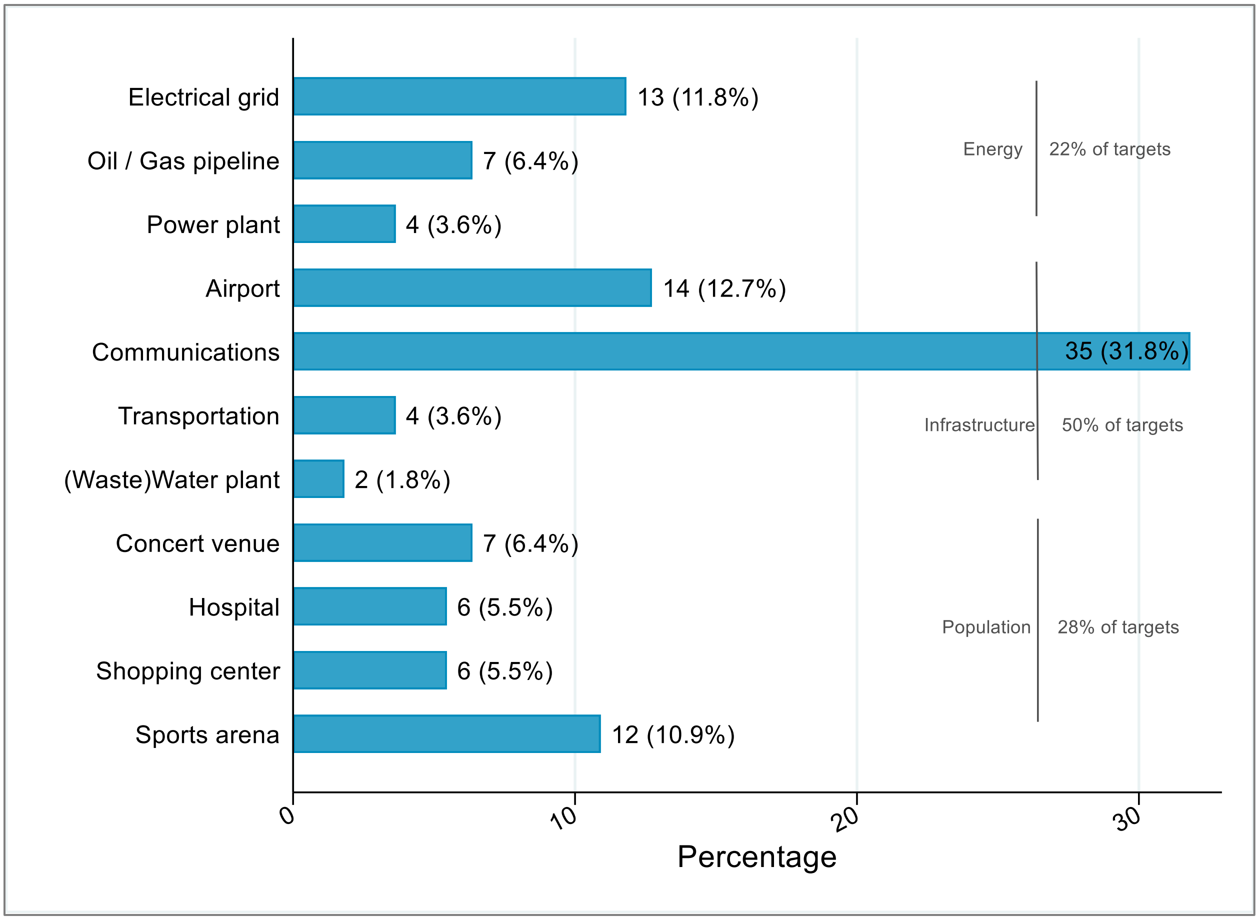
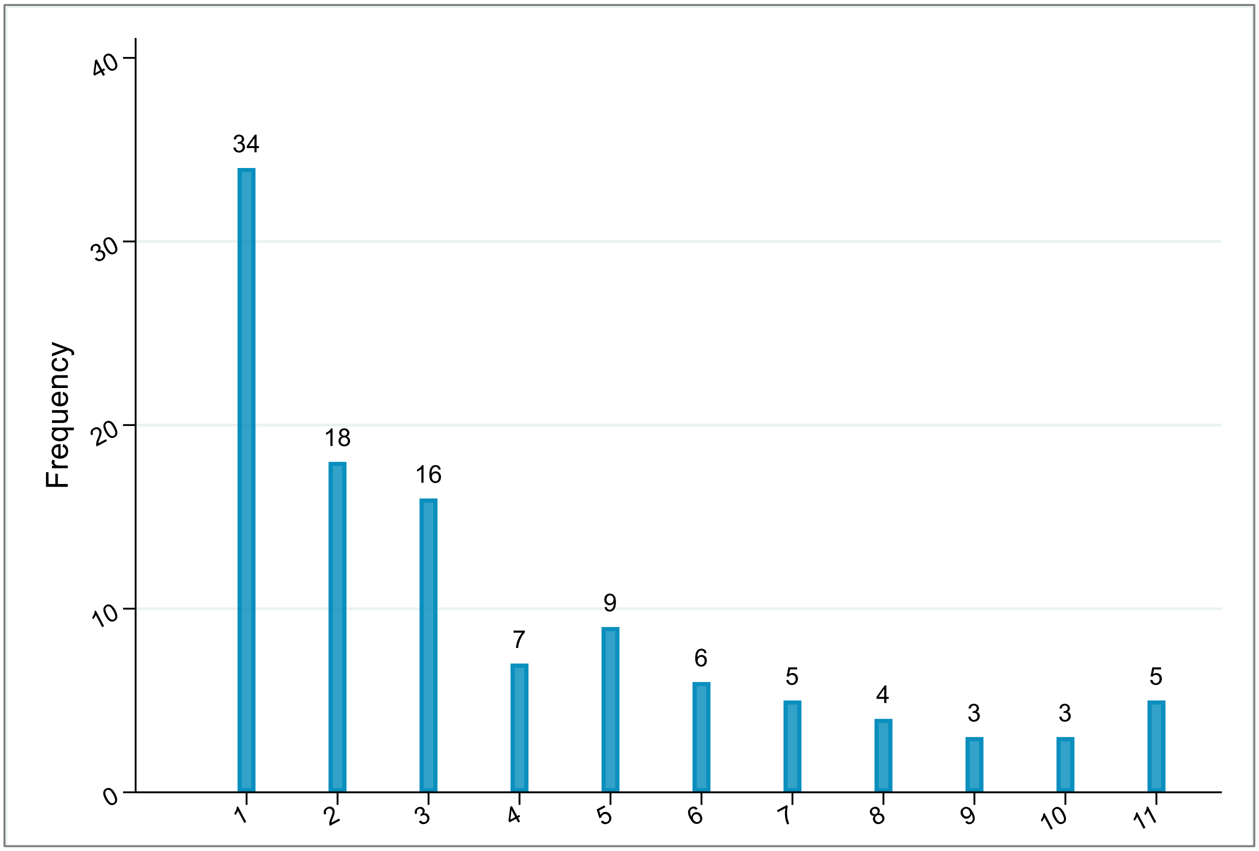


Figure A6. Final target selections, listed alphabetically within energy, infrastructure, and population categories.



A7. Target selection rankings for communication networks.