Fragile States, Technological Capacity, and Increased Terrorist Activity

Ore Koren[a]* and Sumit Ganguly[a] and Aashna Kahnna[a]

[a]*Department of Poltical Science, Indiana University, Bloomington, USA*

*corresponding author: okoren@iu.edu.

Fragile States, Technological Capacity, and Increased Terrorist Activity

Research on terrorism disagrees on whether terrorist activity is at its highest in collapsed states, which are more hospitable to such activities, or whether terrorism increases in more capable states. We revisit this discussion by theorizing an interactive relationship: terrorists prefer to operate in politically-hospitable states, but their attack frequency within these states increases with greater technological capacity, which allows them to expand their military, recruitment, and financing operations. We analyze 27,018 terrorist incidents using regression and causal inference models, conduct a case study, and find robust support for this interactive logic. Our conclusions outline implications for policy and academic work.

Keywords: terrorism; state capacity; War on Terror; technology; rogue states

Does terrorist activity increase in all hospitable states equally or is it prevalent in more technologically advanced states? Recent research provides divergent answers to this question, with some studies emphasizing the role of failed states as breeding grounds for terrorists,[1] while others arguing that terrorists cannot effectively operate in such states.[2] Yet, to our knowledge, no study has approached this question by assuming a *moderated* relationship, where the physical infrastructure and development aspects intensify terrorism within politically-hospitable countries, or tested such a relationship empirically on a cross-national sample using causal inference methods.

In this study, we do exactly that. Building on past research on the motivations of terrorists to conduct attacks in territories with given characteristics,[3] we emphasize how conditions that enable terror groups to operate in a particular country intersects with factors that improve their capacity to conduct large-scale, complex operations to intensify the level of terrorist activity in these locales. Rather than focusing just on conditions of state weakness or failure, we highlight the role of technological infrastructure and capacity in facilitating and enabling terrorist activity.

In particular, we identify and validate three specific mechanisms linking technological capacity with higher rates of terrorist activity within hospitable states. First, we emphasize the role of technology in improving the group's *ability to muster more resources*, including procuring better military equipment, gaining access to international banking services, etc., which allow it to wage a more effective fighting effort. Second, we argue that access to more technology improves the group's ability to *mobilize supporters*, both at home and abroad, including elites and even military personnel. Third, we note that access to more technology allows terror groups to *more effectively identify and attack* both "soft" (e.g., schools, hospitals) and "hard" (e.g., military installation) targets, as well as resist counterterrorism efforts. We then move on to discuss the interactive logic of our argument in more detail. We build on this logic to draw our key empirical hypothesis, namely that terrorist activity within politically-hospitable states will rise where and when technological capacity increases.

To evaluate these interactive effects, we create a detailed indicator of terrorist activity within all countries worldwide since 2001 using information from the Global Terrorism Database (GTD) managed by the National Consortium for the Study of Terrorism and Response to Terrorism (START).[4] We then examine whether and to what extent the level of technological infrastructure within a given country moderates the number of terrorist attacks in politically-hospitable states targeted by a major international counterterrorism attack during a given year. To ensure any effects identified are causal, we also estimate generalized method of moment (GMM) models, which ensure that endogeneity – especially between the number of terrorist attacks and the targeting of such states by counterterrorism coalitions – and serial correlations are accounted for using a set of internal instruments, alongside ordinary least squares (OLS) models.

In deriving a moderated empirical expectation and testing it on cross-national data spanning 17 years (2001-2016), we illustrate that indeed, attempting to understand terrorist groups' incentives to be active within a given country necessitates taking into account not only their willingness to conducts attacks in these locales, which designates the latter as politically-hospitable states, but also how local development, infrastructure, and access to technology allows these organizations to do so effectively. The results are also robust to a battery of additional sensitivity analyses, reported toward the end of the empirical section.

We follow up on these quantitative analysis with a case-based evaluation of two Pakistani-based groups, Jaish-e-Mohammed (JeM) and Lashkar-e-Taiba (LeT), to illustrate the viability of the quantitative findings and the underlying mechanisms we hypothesize. In the conclusion we outline the implications of our findings to both scholars studying the determinants of terrorism and policymakers concerned with mitigating its impacts.

Terrorist Attacks, Politically-Hospitable States, and Technology

In this section, we develop our detailed theory regarding the role of technological capacity in facilitating terror group activity within politically-hospitable states. We begin by providing a short discussion of existing research on the link between weak states and terrorism followed by a short discuss of the relevant concepts used in this paper, before proceeding to discuss our theory and its underlying mechanisms.

Background Discussion: Failed States and Terrorism

Do weak, failing or collapsed states serve as breeding grounds for domestic as well as transnational terror? The question is of considerable significance as both policymakers and scholars have

suggested that such states may be ideal sites for terrorist havens. In particular, the lack of formal governance capacity and the inability of a state to meet the basic Weberian standard of maintaining a monopoly of legitimate violence could make them attractive to terrorist groups as they could act with impunity.

Rem Korteweg and David Ehrhardt provide an effective illustration of this claim.[5] They contend that weakening of state structures provides opportunities for terrorists to establish a base of operation. Although particular terrorist groups may differ based on goals and structures, these groups all share in common the necessity to establish a strategic advantage in particularly weak areas, which Korteweg and Ehrhardt call 'black holes':

> Similar to the astronomical objects (and) consist of territories of limited size with significant impact on the system as a whole. They are centers of gravity in which destructive forces are at play, where transparency is limited and finding out what goes on inside them is difficult. … Black holes provide the terrorist group with freedom of operations, and therefore become staging grounds for various types of activities in support of the non-state actor/terrorist group[6]

C.C. Brafman Kittner makes a similar claim, arguing that weak governance provides an attractive setting for terrorists for a number of compelling reasons.[7] Since these states have limited sovereignty within their borders, they can ward off external interference and counter terrorist measures from foreign actors. The argument also states that, territorially speaking, weak governance need not have to be widespread throughout a country for terrorists to exploit it. Relying on quantitative cross-national analysis, James Piazza similarly finds "that failed and failing states do indeed disproportionately contribute to transnational terrorism" and, moreover, that such states, "irrespective of the type of state failure experienced, are more likely to be targeted by terrorist attacks."[8]

Other studies, however, argue that the focus on state weakness as linearly correlated with higher incidence of terrorism is misguided. For instance, Stewart Patrick adds a caveat to the weak-

state and terrorism argument. [9] In particular, he argues that failing states may serve as incubators of terrorism as well as transnational threats, but that this relationship is by no means universal. He further argues that not all weak or failing states are terrorist havens, and that a variety of other factors rendered certain collapsed states attractive to terrorist groups. Most importantly, he claims that terrorists may prefer *functioning* states, all else being equal.

The claim that state-weakness is insufficient, in-and-of itself, in explaining terrorist activity, is echoed by other scholars. For example, Ken Menkhaus argues that collapsed states in effect do not constitute attractive safe havens for terrorists. [10] In regions where state authority completely collapsed, terrorist cells and their bases are far more susceptible to counter-terrorist actions. Such areas may also attract other, often hostile violent nonstate actors, such as pro-government militias,[11] making these groups vulnerable to threats that they themselves pose, e.g., kidnapping, extortion, blackmail or assassination. Operating under these anarchic conditions, terrorist organizations might find it extremely difficult to remain neutral and must pick sides among other feuding forces. Indeed, some scholars[12] go further in finding no clear causal links between failed states and increased terrorist activity.

More recent work by Elizabeth Grimm Arsenault and Tricia Bacon tries to focus on and explain the particular mechanisms that affect linkages between fragile states and politically-hospitable conditions for terrorism. [13] In particular, the authors argue that while weak or failing states could provide terror groups with some form of sanctuary, their ideal option is to base their operations in a sub-category of semi-failed states that *actively enable their operations*. We draw on this logic to further argue that collapsed or failed states that are also underdeveloped are hardly ideal locations for terrorists, for a number of compelling reasons, which we discuss below; but that

such politically-hospitable states that have higher level of technological infrastructure and improved levels of development are exactly where terrorism will rise.

Relevant Concepts

In this study, we use different theoretically and empirically relevant concepts, which we define in this subsection. First, we define what we mean by "politically-hospitable states." For our purposes, a politically-hospitable state is a country where the government enables – either actively or passively – the activity of a terrorist group. This does not mean that the state has to sponsor the group, although sponsoring states are a subcategory of politically-hospitable countries,[14] but merely to provide conditions where the group can operate without interruptions and – also important for our purposes – take advantage of any technological or other advantage provided within or by the state unhindered. Fragile and failed states as defined by, for instance, by Menkhaus, Korteweg and Ehrhardt, and Piazza,[15] could fit – and often fall under – the category of politically-hospitable states, although a failed state could still, at least in theory, oppose terrorism and try to hinder the terrorists' activity. Often such states simply do not have the capacity to oppose terrorist groups and their activities. Nevertheless, the actual physical ability to thwart terror groups is related to the capacity aspect (as discussed below); a government may prefer not to fight terrorists even if it has the capacity to do so, and vice versa. From a theoretical perspective, political-hospitability serves as a proxy for whether terror groups will be generally *willing* to operate in the country. If the climate is inhospitable, groups could still conduct attacks, but they will have a reduced willingness to fester in the state, compared with other locations in the regions which might be more hospitable.

A second key feature of our argument relates to local capacity and its impact on improving groups' ability to operate in a given country. Primarily, our argument emphasizes *technological capacity*, namely the degree of development, communications, financial services, and other factors that are dependent on whether a state has sufficient technological means and infrastructure to enable this activity. Accordingly, for our purposes, technological capacity relates to level of access of technology available to individuals within a given state, particularly with respect to electrification, which is a necessary perquisite for sophisticated technological activities.[16]

A third relevant concept we use here is international counterterrorism. As we explain below, political-hospitability is often hard to observe directly. But some host countries enable terrorism to such a degree that they attract the attention of international actors, namely other (affected) states, the UN, etc. In such cases, one or more states, sometimes backed by the international community or as part of a coalition of several countries, will invade this country in an organized effort to eliminate terrorist activity therein.[17] As we discuss in the empirical section, we define (international) counterterrorism as such an observed major effort and use it – in the lack of a better tool – as a visible empirical proxy of politically-hospitable conditions. We do recognize that using such a proxy introduces potential endogeneity concerns into the data, namely that counterterrorism could directly affect the level of terrorist activity in the region. Accordingly, we both discuss this concern theoretically below (especially in Figure 1), and account for it empirically using relevant models (discussed in detail in the empirical section), and indeed, in doing so find an even stronger evidence for our hypothesized relationship.

Technology and Terrorism: Three Relevant Mechanisms

Importantly, modern terrorist organizations are heavily dependent on technological capacity for recruiting troops, maintaining operations, securing funding, and coordinating attacks globally.[18] Although past research often emphasized the link between state weakness and terrorism (as we discussed above), low-technological capacity countries do not offer adequate infrastructure for conducting such operations because they lack, for example, banking facilities that enable the transfer of funds, or regular access to communication technologies, among other factors. Consequently, we argue that often, it is actually more developed states that are the most effective in enabling – either actively or passively – terrorism. Accordingly, higher terrorist activity is a feature of two distinct, although related factors.

The first feature is whether a country provides politically-hospitable conditions for terrorism. Scholars showed that terror groups often make strategic operational calculations to deduce where it is best for them to operate.[19] Indeed, political hospitability, as defined in the previous subsection, is a central tenet of some of the research discussed in the previous subsection, and in particular, of research that emphasizes the ability of the state to monopolize security uniformly across its entire territory.[20]

Importantly for our purposes, the emphasis in extant research is often on the *willingness* of terror groups to operate in a given country. For instance, Arsenault and Bacon contend that terrorists will be more willing to operate where governments are prone to grant leeway to these groups in not cracking down on them. [21] Similarly, Piazza concludes "the relationship between intensity and pervasiveness of state failure and transnational terrorism is linear." [22] Indeed, this willingness to permit or tolerate terrorist operations has led to military responses on the part of the U.S. and its allies since the September 11, 2001 attacks, with mixed results.[23] As we discuss in the next subsection, we concur with extant research that political hospitability as often defined in the

literature is key in explaining increased terrorist activity, although we believe this relationship is more complex, and in particular, that its strength depends on the capacity of groups to develop, maintain, and increase the scope of their operations.

Accordingly, a second key feature, yet one that received less attention in extant research, is the role of available *capacity* in allowing the group to establish itself and effectively operate within the country and expand its activities locally.[24] Indeed, without effective capacity, a terror group is unlikely to be very successful in expanding its operations or in becoming a viable threat to the state or to international actors.[25] In particular, we emphasize the *physical technological infrastructure* within a given state (as we defined in the previous subsection), which enable capabilities such as banking, telecommunications, and other resources available in more developed states,[26] rather than the government's ability to monopolize violence and deploy coercion within its borders, or lack thereof, highlighted by past studies.[27] This is because the latter is specific to the host country's ability to thwart terrorism and as a result – as we discussed above – falls closer to the willingness aspect discussed above, providing hospitable political conditions where terrorism *could*, but not necessarily *will*, increase. In contrast, technological capacity relates specifically to terror groups and their ability to expand operations within a given space ungoverned by the state. It is important to stress that by relatively high level of technological capacity, we do not necessarily refer to high levels of development or to developed countries. Rather, we mean that, on average, as technological infrastructure levels rise, so does the risk of terrorism within hospitable states (as we discuss below). For example, countries with relatively high degrees of terrorist activity such as Pakistan or Iraq are not fully developed states, but the level of technological infrastructure available per capita within each of these states is higher than, say, in Mali or Niger.

More specifically, developed technological infrastructure can be connected to higher terrorist activity within the right contexts (which we discuss in the next subsection) via three specific pathways, or mechanisms. We discuss these mechanisms here, while providing a detailed evaluation of each one in our case study analysis below.

First, improved technological capacity allows the terror group to improve its overall *resource capacity*. In general, citizens of relatively better developed states enjoy more disposable income, more free time, and generally higher levels of other resources that can be directed toward terrorism activities.[28] Correspondingly, operating within such countries lowers the costs terrorists incur from mobilizing against the government or against a foreign invader, especially as better communication technology also mitigates mobilization costs by promoting information sharing and coordination among potential supporters at home and abroad (see below). In mustering material resources and capabilities, the terrorists can wage a more effective fighting effort, not only including by procuring better equipment and financially rewarding their supporters,[29] but also in gaining access to international banking services, which are necessary for the group to support and maintain its day-to-day operations, mobilizing funds from abroad, etc.[30]

Second, access to more technology improves the group's ability to mobilize supporters, both at home and abroad, via *increased alignment capacity*. In this case, technology allows the terrorists to effectively communicate with their activists and supporters, optimizing troop deployment for specific missions, thereby improving the group's ability to make the most effective use of the resources available to it. Regular access to communication technology also allows terrorists to more effectively spread their message to potential new supporters and recruits, e.g., via social media, as well as using traditional recruitment techniques (face-to-face, local places of worship, etc.).[31] For example, an infamous case of social-media-driven terrorism, the Islamic State

(IS) often relies on such methods in recruiting and mobilizing support. The organization has standardized selection procedures on social media such that, "IS is active to find possible recruits on the social media platforms and before the recruitment it invites them to join in the more private and closed forum for the further instructions."[32] Moreover, in line with the hypothesized mechanism, "tampering of the Internet platforms helps the terror groups to continue their operational discussions on any terrorist incidents or attacks across the world…In many video clips, IS shares its arms, arsenals and other weapons in order to demonstrate its strengths and powers to the international community, which also inspires its supporters and followers."[33]

Finally, greater access to technology allows the terror group to *optimize its targeting activities*, assisting in the collection of information and the ability to more effective attach both "soft" (e.g., schools, hospitals) and "hard" (e.g., military installations) targets. From this perspective, terror groups with access to better technology can collect more sophisticated and more specific information on potential targets (e.g., satellite images), conduct covert collection activities (e.g., via deploying drones, hidden cameras), and improve the timing of their attacks (e.g., when during changes of the guard, prayer times). Access to better technological capacity can also improve the group's ability to select across a range of potential targets, investing their resources and manpower where they can get the "biggest bang for their buck".

Technological Capacity and Terrorism in Politically-Hospitable States

It is important to emphasize that these mechanisms are primarily relevant where terror groups have the willingness to operate. Indeed, we contend that, *separately*, neither hospitable political conditions nor relatively high levels of technological capacity, as defined above, should noticeably increase terrorist activity. Relatively high technological capacity is a feature of many strong and

capable states,[34] the vast majority of which do not experience or enable any kind of terrorist activity. Because technological capacity is often an associated feature of high levels of development and state capacity,[35] states with better infrastructure can also effectively combat terrorism instead of allowing it to fester within their borders.

Similarly, as we argue here (and as we show below), focusing on the hospitality of the political environment to terror groups is also insufficient in explaining where such groups will be more or less active. First, as mentioned above, without having sufficient capacity to operate effectively, the terrorist group is unlikely to choose to operate within a politically-hospitable state, or – if it does choose to do so – is unlikely to become a powerful organization. Second, although being a politically-hospitable state is one of the most effective indicators of whether or not terrorists are willing to operate in a given country, such states frequently attract international intervention. For analytical purposes, this feature provides an advantage by allowing us to identify a list of states that clearly provide politically-hospitable conditions for terrorists to grow and fester (pending on technological capacity levels), but such intervention also has an obvious impact on reducing such activities.[36]

In other words, if willingness is the key defining feature of terrorist activity, being the target of a counterterrorism effort by one country or a coalition of states should – simultaneously – strongly and negatively impact said willingness, thereby possibly decreasing overall levels of terrorist activity in the country over both the short and long terms. We therefore make sure to account for such potential endogeneity in our empirical models below. At the same time, technological capacity could actually provide terror organizations with greater capabilities to resist these counterterrorism efforts, thereby making terror groups in these politically-hospitable

countries with relatively developed infrastructure even more effective vis-à-vis the invading state or coalitions of states than their low-development-state counterparts.

For this reason, we believe that examining a *moderated relationship*, where technological capacity should intensify terrorist activity in politically-hospitable countries, and estimating causal models that account for relevant endogeneity concerns (as we do in the empirical section below) are both crucial for improving our understanding of terrorism. Empirically, we proxy political-hospitability using international counterterrorism effort, as we defined under "concepts", under the assumption that the impact of such operations, moderated by technological capacity, on terror group activity should mirror the intersection of willingness and capacity aspects of our theory.

To illustrate this later point, we plot these conceptual relationships inf Figure 1. Here, the top plot (Figure 1a) shows the expected persistence of terrorism within a given country based on our theory along two axes: political hospitability (left-right) and technological capacity (top-bottom). Our theory expects that the highest rates of terror group persistence will take place in countries and regions where both politically-hospitable conditions and relatively higher levels of technological infrastructure exist, that is, in the upper-right quadrant. According to research, countries that fall within this quadrant are states such as Pakistan[37] or Iraq.[38]

Because we cannot directly observe political-hospitability due to the issues discussed above, we use major counterterrorism efforts to proxy terrorist groups willingness and delineate corresponding expectations in the bottom plot (Figure 1b). Accordingly, we do not expect to see any changes in terrorist activity in locations that have relatively low levels of technological infrastructure, and which did not experience a counterterrorism effort, and we treat them as our baseline of comparison. In countries that do not involve a major international counterterrorism effort which also have relatively improved technological capacity, terrorists can draw on said

capacity to increase the scale of their operations. At the same time, however, even if a major counterterrorism effort involving international actors does not happen, local domestic counterterrorism measures could still induce a change in terrorist activity. This is because in such states terrorists could increase their activities, but the host state could similarly draw on the same technology to combat terrorism. We hence remain agnostic as to whether terrorism will increase or decrease in such states, although our logic suggests that terrorists might be able to better target domestic forces using the technological resources available, and hence that terrorist violence might increase overall, compared with countries low technological capacity that similarly have not been targeted by a major counterterrorism effort.

Most importantly for our theory, in states where terrorists have more developed technological capacity and infrastructure to draw on and where the state does not try to thwart their activity, if not to actively assist them, we expect international counterterrorism efforts to not only be less effective, but actually intensify terrorism. Here, local groups will be able to expand their operations, using violence successfully not only against any targets they may have targeted otherwise, but also against the forces that have engaged in the counterterrorism effort, with brutal efficacy. This in contrast to states with low technological capacity, where counterterrorism efforts should be (very) effective in reducing terrorism activity, as local groups simply cannot muster sufficient capacity to effectively challenge the (far) stronger invading state or coalition.

[Insert Figure 1 about here]

Put simply, we contend that the frequency of attacks is not uniform across states that offer hospitable conditions (willingness), which serves as a key feature in policymakers' decisions as to whether or not to target these states as part of a counterterrorism effort, but rather varies based on

the level of technological infrastructure available within these states (capacity). From this perspective, technological infrastructure gives the terrorists heightened capacity to respond to and target the forces of an intervening power.[39] As such, even during an ongoing intervention (that is, in time *t*), the number of terrorist activity incidents in a politically-hospitable (and internationally targeted) country should be *higher* than in similar targeted states with low infrastructure levels, as groups can take advantage of the more developed technological capacities to coordinate, stage, and carry out attacks more effectively. Accordingly, and building on the logic discussed above, our key hypothesis is:

> **Hypothesis:** *In countries targeted by an international counterterrorism effort the level of terrorist activity should noticeably rise as technological capacity increases*.

Empirical Analysis

Sample, Variables, and Methodology

We test our argument on a global sample of 156 countries for the years 2001–2016.[40] Our dependent variable, *Terrorist Activity*$_{it}$,[41] is operationalized as the number of recorded terrorist attacks in a given country during a given year. For operationalizing this variable, we relied on data from the Global Terrorism Database (GTD) managed by the National Consortium for the Study of Terrorism and Response to Terrorism (START).[42] The GTD systematically collects information on terrorist attacks, including date, location, weapon used, and casualties. To create this variable, we went through the GTD to code any attacks perpetrated by an identified terrorist group against military (either domestic or foreign) or civilians within a given country over the 2001-2018 period.[43] This resulted in a list of 34,855 incidents. We curtailed our period to 2001-2016 to ensure

comparability with our main independent variables, which left a list of 27,018 distinct terrorist incidents. We then aggregated this count variable to the country-year level, by summing the number of terror activity incidents by all groups recorded annually within a given country.[44]

We interact two explanatory variables to test the moderated effect and related expectations hypothesized in the previous section. The first is a continuous proxy for technological infrastructure available within a given country during a given year. The purpose of this indicator is to measure the *capacity* of terror groups to develop and expand their domestic and international operations, emphasizing – again – technological capabilities, specifically, rather than the state's ability to coerce more broadly, as we explained in the previous section. Building on recent research that equates access to electrification and its expansion with technological and economic development,[45] we operationalize this variable as the count of the number of people within a given country with regular access to electricity during a given year. Information on this variable, $Electricity\ Access_{it}$, was obtained from the World Development Indicators (WDI) published by the World Bank, which collects these data from industry, national surveys and other domestic and international sources.[46] Considering the wide range on the number of individuals with access to electricity measured by the data (0 ⇔ 1.379e+09), we log this variable prior to entering it into our models.

Next, we operationalize the *willingness* of groups to operate within a given country during a given year by capturing a country that provided politically-hospitable conditions for terrorism during a given year (as we defined theoretically in the previous section). To this end, our second explanatory variable measures whether a given country was on the receiving end of a major counterterrorism efforts on the part of the U.S. and/or its allies.[47] We understand that in focusing on such major counterterrorism efforts, we might be omitting from our sample countries that

provide such politically-hospitable conditions, but which have not been targeted by such a campaign. Nevertheless, as we showed in Figure 1, the resulting indicator serves as an effective empirical proxy for the *willingness* of terror groups to operate and perpetrate attacks within a given country – as countries that are targeted by a counterterrorism coalition have, at least passively, enabled terrorist groups to operate within their borders.[48]

Considering that our theoretical argument assumes the two variables should reinforce each other's effects, generating the most terror-group-friendly conditions, i.e., within a state that enables terrorist activity and where technological infrastructure improves the group's ability to operate effectively, we introduce the interaction term *Electricity Access*$_{it}$ X *International Counterterrorism*$_{it}$ into our models, controlling for each individual component.

Our models include several additional variables, also measured at the country-year level, to account for alternative explanations. Because adding too many such "controls" can lead to inferential biases and type II errors, i.e., falsely rejecting the null,[49] we only include the most relevant potential confounders identified by relevant research, while reporting and discussing robustness models that account for a large number of additional confounders toward the end of the empirical section. To this end, we first include indictors accounting for (log) population size and (log) GDP per capital in a given country during a given year, by combining information from the WDI[50] and Gleditsch's 2002 study,[51] which overcomes the prevalent missingness of the WDI-based indicators over most of our period of interest. To account for how political openness within a given state might impact terrorist activity via channels of hospitability to terror groups, we include the ordinal Polity2 indicator from the Polity IV dataset.[52] To account for any deterrent effects the military of a given state might have on terrorist activity in a given year, we include a variable measuring the (log) number of military troops in a given-country year.[53] Summary

statistics for all our variables, including those used in our robustness models, which we discuss below, are reported in Table A.1 in the Appendix.

Considering the wide range of our dependent count variable, *Terrorist Activity*$_{it}$, we treat it as continuous and rely on ordinary least squares (OLS) for estimating our variables' effects. Additionally, recall that one potentially confounding relationship within our data relates to the fact that while being the target of an international counterterrorism effort illustrates a country's viability as a potential hotbed of terrorism, such intervention can also impact the frequency of terrorist attacks, generating an endogenous relationship between the dependent (*Terrorist Activity*$_{it}$) and at least one independent (*International Counterterrorism*$_{it}$) variables. Nevertheless, to ensure that any observed associations are causal and robust to these issues, we additionally estimate generalized method of moment (GMM) models, which rely on past values of the endogenous dependent variable to 'exogenize' its relationship with counterterrorism and development.[54] For both the OLS and GMM models, we also estimate and report additional sensitivity analyses accounting for data and model selection choices below.

In our OLS models, to ensure that the observed relationships are not the particular results of across -or within- country *i* variations, especially considering our argument focuses specifically on within-country impacts, we estimate each model with fixed effects by country as recommended in extant research.[55] To ensure our results are not due to year-specific trends, each model also includes fixed effects by year *t*. To account for heterogeneities within countries, especially considering that the values for some variables are duplicated over time, standard errors in all models are clustered by country. The moderated relationship between access to electricity, counterterrorism efforts, and terrorist activity is hence identified using the following equation:

$$\mathbf{y}_{it} = \beta_0 + \beta_1 e_{it} + \beta_2 w_{it} + \beta_3 e_{it} \times w_{it} + \beta_{4-k} X_{it} + \Theta_t + \Phi_i + \epsilon_i \qquad (1)$$

Here, $\mathbf{y_{it}}$, is a vector of terrorist attacks in country *i* in year *t*; $\mathbf{e_{it}}$ is a vector denoting the (log) number of citizens with access to electricity in a given country annually, $\mathbf{w_{it}}$ is a vector denoting whether or not a country was the target of counterterrorism effort by the U.S. and/or its allies, and $\mathbf{e_{it}}$ x $\mathbf{w_{it}}$ their interaction; $\mathbf{X_{it}}$ is a matrix of control variables; Θ_t and Φ_i are fixed effects by year *t* and country *i*, respectively; and ϵ_i denotes standard errors clustered by country.

Additionally, as mentioned above, terrorism activity may exhibit serial correlations over time and/or endogeneity with counterterrorism (and potentially with technological infrastructure) due to endogenous policy responses, omitted variable effects, or persistent policies due to ongoing conflict. To address this concern, we employ a series of robust system generalized method of moments (GMM) dynamic models where the necessary instruments are 'internal' and rely on lagged values of the potentially endogenous dependent variable, *Terrorist Activity*$_{it}$, to 'exogenize' the relationship between our two independent variables and terrorist activity.[56] The model is specified as a system of (per period) equations, where the instruments applicable to each equation differ because additional lagged values of the instruments exist in later time periods. Accordingly, for these instruments, we include two-to-five-period (year) lags of *Terrorist Activity*$_{it}$, capturing variations in this variable at time *t* based on changes from past periods. In doing so, we are able to account for any potential impacts of our dependent variable (*Terrorist Activity*$_{it}$) on not only one but both independent variables (*Electricity Access*$_{it}$ and *International Counterterrorism*$_{it}$) over the period of analysis. Since we are considering panel models with two-way effects, conflict-dyad and year fixed effects are canceled-out, providing a straightforward instrumental variable estimator. We also estimate two-step robust standard errors, corresponding to country-robust standard errors within the OLS framework, to account for country-level heterogeneities within our GMM models.

Results

Table 1 first reports a baseline OLS model of *Terrorist Activity*$_{it}$, which includes only our interaction term *Electricity Access*$_{it}$ X *International Counterterrorism*$_{it}$ and its constitutive terms, in addition to year and country fixed effects. This baseline model is followed by a full specification, which adds all controls. Attempting a causal, robust-to-endogeneity statement, the next two columns then report the corresponding GMM model estimates.

All results strongly support the hypothesized effect of *Electricity Access*$_{it}$ X *International Counterterrorism*$_{it}$ on terrorist activity. The individual coefficient estimates on *Electricity Access*$_{it}$ are not robust in either sign or significance in the OLS models, suggesting that – in the absence of counterterrorism effort, which captures terrorist groups' willingness to operate in a given country – access to more technology does not noticeably increase or decrease the level of terrorist activity. However, the coefficient is positive and statistically significant in the GMM models, which account for endogeneity, suggesting that even in the absence of an international counterterrorism effort conditions, terrorist groups prefer, on average, states with better technological infrastructure.

Most importantly, the coefficient on our *Electricity Access*$_{it}$ X *International Counterterrorism*$_{it}$ interaction is positive and significant (to at least the $p<.1$ level) across all models, implying that, in support of our hypothesis, increases in technological capacity had caused an *added* terrorism-intensifying effect within a politically-hospitable state in a given year (i.e., during an international counterterrorist intervention), although we must examine our marginal effects below to fully ascertain the significance of this result. Indeed, the results are not only robust, but actually pass a higher statistical significance threshold once endogeneity is accounted for in the GMM models, suggesting a causal impact. Table 1 hence strongly confirms our key hypothesis.

Finally, the coefficient estimates for *International Counterterrorism*$_{it}$ itself is negative and significant in all but one OLS model (to the $p<.01$ level), suggesting that – without access to technology, which provides groups with greater capacity to challenge strong adversaries – political-hospitability is insufficient in explaining terrorist group activity, and possibly also international counterterrorism efforts may be effective in combating terrorism activity in low technological capacity locales, although the results might be confounded in the full OLS model. It is also important to bear in mind that the *International Counterterrorism*$_{it}$ coefficient here refers to hypothetical country-years where no individuals had regular access to electricity – which is (luckily) exceedingly rare[57] – that has also been targeted by an international counterterrorism effort.

Considering these issues, it is important to interpret the interaction term substantively. Accordingly, to evaluate whether our interaction supports our hypothesis, we use our full OLS model estimates to calculate the change in *International Counterterrorism*$_{it}$'s coefficient (that is when *International Counterterrorism*$_{it}$ is changed from =0 to =1) on the expected number of terrorist activity incidents across the range of (log) *Electricity Access*$_{it}$ in a sample where all observations with missing information have been removed (5.70 ⇔ 21.04). We plot these estimated marginal effects for our full OLS model specifications, along with their 95% confidence intervals, in Figure 2 (the data used for plotting this figure includes all observations with no missing information on all variables used in the full specification in Table 1).

As shown, *International Counterterrorism*$_{it}$'s expected effects in country-years where regular access to electricity was at its minimum (i.e., log *Electricity Access*$_{it}$ = 5.70), is negative, meaning politically-hospitable conditions that invite counterterrorism intervention should (as expected) decrease the level of terrorist activity by about 55 incidents per country-year, on average,

although this effect is not different from zero. In other words, in low technological infrastructure environment, i.e., where terror group capacity to operate is low, willingness-related factors have no notable effect. However, as (log) *Electricity Access*$_{it}$ levels in a given country rise, terrorism activity within politically-hospitable countries *increases*, until reaching to (log) *Electricity Access*$_{it}$'s maximum (i.e., =21.03), where being targeted by an international counterterrorism effort (i.e., *International Counterterrorism*$_{it}$=1) is expected to increase the frequency of terrorist attacks by more than 60 incidents in a given country-year, on average, an effect that is different from zero, and which supports our broad theoretical claims (and both relationships visualized in Figure 1).

[Insert Table 1 and Figure 2 about here]

Sensitivity Analyses and Robustness Models

In this subsection we evaluate the sensitivity of our results to the disaggregation of terrorist activity by type, as well as illustrate our findings' robustness to a variety of confounders, operationalization, and modeling choices. Each of these robustness specifications corresponds to the full model estimates from Table 1, and each model is estimated twice, once in OLS and once in GMM form to ensure a causal interpretation. All models are reported in Table 2 below.

We begin by ensuring that our results are not driven by our reliance on the World Bank data for creating *Electricity Access*$_{it}$, which might be susceptible to reporting and other data collection biases, by using annual nighttime light emissions, recorded by satellites, to operationalize this variable instead, as past research has done to measure local development and capacity levels.[58] Second, we ensure that our results are not driven by the relatively wide range of our dependent variable (0 ⇔ 1,094 incidents) or the existent potential outliers in the data, by reporting a set of models where our dependent variable is logged.

Third, we report estimates from a Poisson model, which is specifically designed for the purpose of handling count data.[59] The next two sets of models then illustrate our findings' robustness to the decision to include only key controls in Table 1 by adding a large number of indicators accounting for alternative confounders. We begin by (fourth) adding controls for rents obtained from oil and whether or not there was a coup d'état in a given year to both our OLS and GMM models. In the fifth robustness test we add to our full OLS specification additional controls for percent country area that is mountainous and ethnic and religious fractionalization that – due to their time constant nature – we are unable to include in models with country fixed effects. Accordingly, instead of fixed effects, our final robustness model includes random effects by country to still account for country specific traits and heterogeneities.

Finally, in the last two columns we estimated an OLS and a GMM model where the dependent variable used includes only attacks unsanctioned by states to ensure that our hypothesized relationship does not require the active support of the state in terror attacks. Crucially, our interaction term *Electricity Access*$_{it}$ X *International Counterterrorism*$_{it}$'s positive sign and statistical significance hold across all models in both the OLS and GMM models, providing additional confirmation for our theoretical argument.

[Insert Table 2 about here]

Case Study: JeM and LeT

To provide a more effective evaluation of the three mechanisms linking technological capacity to higher terrorist activity as we theorized, *resource capacity, increased alignment capacity and optimizing identification of targets*, as well as our broader interactive hypothesis, we now turn to take a closer look at two groups that originated in Pakistan: the Lashkar-e-Taiba (LeT) and the Jaish-e-Mohammed (JeM). In selecting these two groups, we rely on the "typical" case selection

approach advocated by Seawright and Gerring, whereby an effective analysis "focuses on a case that exemplifies a stable, cross-case relationship...in which the evidence at hand (in the case) is judged according to whether it validates the stipulated causal mechanisms or not." [60] Importantly, the focus on LeT and JeM as our cases allows us to account both for the country of origin (both groups are based in Pakistan but operate largely in India) and group ideology (both groups purport an extremist agenda and support to secession of Kashmir from India).

Lashkar-e-Taiba

The LeT's principal goal is to dislodge the Indian-controlled portion Kashmir and merge it with Pakistan. Created under the patronage of Pakistani Inter-Services Intelligence (ISI) Directorate, the group has maintained a close relationship with the Pakistan Army for much of its existence, which has enabled it to access relatively advanced technological capabilities, thereby facilitating its operations and attacks in India.[61] Since its founding as a group designed to instigate a proxy war, the group's objectives have shifted toward establishing a global Islamic caliphate.[62]

Hafiz Mohammed Saeed, the founder of LeT, has played a key role in promoting and maintaining the group's Islamist identity. He has distinguished his organization from the larger jihadi movement though an emphasis on the Ahl-e-Hadith interpretation of Islam which holds that all Muslims must recognize and return to a pristine form of Islam.[63] A prominent Islamic cleric, Saeed has not only promoted the cause of regional and global jihad but has also undertaken a range of social welfare programs.[64] Stephen Tankel argues that the LeT enjoys the support of the Pakistani military because of its dual functions: its missionary/welfare role and simultaneous commitment to global jihad.[65] Importantly for our purposes, this relationship highlights the

mechanisms through which LeT's has gained access to military technology while enjoying a politically-viable sanctuary.

In particular, LeT's 2008 attack in Mumbai illustrates how the group's access to technology, facilitated with the assistance of the Pakistani military, as well as its general ability to exist uninterrupted within the Pakistani state was crucial in its ability to facilitate recruitment, select key targets, and provide the group with the necessary equipment, ranging from marine landing gear to specialized weaponry. Being able to access technology and resources principally led to the evolution of the group's terrorist activities, ranging from staging small two-person attacks against Indian troops in the Kashmir Valley during its early years to the daring November 2008 attack in Mumbai that lasted over 3 days and left 166 dead.[66] During the latter, 10 LeT operatives entered India via the Arabian sea from the Pakistani port city of Karachi and targeted a major train terminus, a Jewish community center, a popular café and two hotels, the Taj at the Gateway of India and the Oberoi Trident. The terrorists were armed with explosives, hand grenades and high-powered assault rifles. They also carried substantial amounts of provisions designed to sustain themselves for at least two days.

The arrest of David Headley, a Pakistani American LeT member, by the U.S. was crucial in understanding the plan of the terrorist attack. Headley served as the link between LeT and ISI and his court testimony revealed that the ISI had provided access to financial and technological resources that were used for conducting an extensive reconnaissance and surveillance operation in Mumbai prior to the launch of the attack.[67] As such, his testimony helps in illustrating how the three mechanisms we hypothesize have operated before, during, and after the 2008 attack.

First, with respect to resource capacity, it is worth noting that the terrorists who had landed on a beach adjacent to Mumbai had access to and were trained in using GPS technology. They also

had access to both a Pakistan-flagged cargo ship and specialized marine landing crafts. The ISI had made all these resources available to LeT terrorists.[68]

Other features of the attack illustrate the operation of the target selection mechanism we hypothesize in showing how technology improved the group's ability to optimize its targeting activities. For instance, during the siege, LeT commanders operating from a control room in Karachi gave instructions to the terrorists using Voice over Internet Protocol (VoIP) technology, which – among other effects – allowed the terrorists to coordinate bomb explosions and relay information back to their commanders in Pakistan. Additionally, LeT commanders were able to use Indian television feeds to give real-time instructions to the terrorists, especially during the siege at the Taj Hotel, thereby optimizing their ability to avoid state forces and inflict damage. Indeed, relying on VoIP had enabled the operatives not only to hide their physical location from the Indian authorities but also the identities of the users.[69] Finally, effectively trained in and having access to GPS technology, LeT operators were able not only to deploy with precision, but also to identify specific sets of targets in address in advance.

After Indian authorities arrested Abu Hamza, an Indian Mujahideen militant, he revealed how LeT commanders recruited terrorists specifically for this operation, and his testimony illustrates the viability of our final hypothesized mechanism, namely increased alignment capacity.[70] In particular, the group has drawn on successful 2008 attack to expand its recruitment activities and reach new potential recruits using technology. [71] In particular, LeT recruitment after the 2008 attack has become increasingly reliant on social media, where the group could promote its agenda, attract recruits, and incite an anti-India sentiment, especially within India.[72] Through the cyber unit of Jammat-ud-Dawah (JuD), LeT's political arm, the group has maintained a strong online presence on social media websites such as Facebook, Twitter, YouTube, and Whatsapp.

These online activities included, among others, creating multiple user profiles that engaged with distributing and moderating aggressive and extremist context, attracting and enrolling new users in relevant groups, and even running an original computer game, "Age of Jihad," as a tool to increase engagement and facilitate recruitment.[73]

Additionally, the LeT (through JuD) has used technology as a channel for direct communication with supporters. For example, when Hafiz Saeed delivered a speech on 'jihad, terrorism, ISIS & impact of social media,' he did it during a two-day cyber conference organized by the JuD to mark the launch of its 24x7 cyber cell in 2015.[74] The group simultaneously developed a customized VoIP application, Ibotel, that ensures the group's IT security through encrypting relevant content and restricting access only to preapproved individuals.[75] The LeT's innovative use of technology is exemplified in its "evolution from technology users to developers,"[76] in particular its ability to create an original technological framework based on its needs and operation strategies. Indeed, the ability to expand its online presence and fighting capabilities by mastering the technological capacities available in its host country has been responsible, at least partly, to the fact that LeT has become a threat to Pakistani national security.[77]

Yet, and especially before they fell out of grace with ISI, the LeT's operations also illustrate the importance of the political hospitability aspect of our theory. Although Indian authorities had repeatedly blamed Saeed for the Mumbai attack and demanded a response from the Pakistan government,[78] a charge that the latter had denied,[79] it was only under sustained American pressure that Pakistani authorities finally arrested Saeed in 2019 on the charge of terrorism financing.[80] Saeed's arrest, however, did little to curb the group's activities in both Pakistan and India, where one of its factions recently reemerged in Kashmir as the Resistance Front (TRF) in a response to the Indian government's decision to revoke Jammu and Kashmir's special status.[81] Nevertheless,

as the above discussion illustrates, it was not only the relative political freedom – and indeed, active government support – to operate that allowed LeT to become a formidable group; it was its ability to access and effectively deploy technological capacities, whether these were obtained via ISI sponsoring or independently, that allowed LeT to increase and optimize its operations, in line with our broad theory.

Jaish-e-Mohammed (JeM)

Formed in 1994, the JeM has had a similar objective to the LeT: the secession of Indian-controlled Kashmir and its eventual incorporation into Pakistan. Scholars have argued that the JeM similarly has enjoyed ISI sponsoring, especially its grip on the LeT was slipping due to latter's ability to deploy technological capacities independently to its own end, which – as we mentioned above – was a key reason the group has become a threat to Pakistani domestic security.[82] The JeM's founder, Maulana Masood Azhar, was originally a member of the militant group Harakat-ul-Mujahideen (HuM). Arrested by Indian security forces in 1994 when, he was released in December 1999 as part of a hostage deal involving IC-814, an Indian airliner hijacked by the HuM during a routine flight from Kathmandu, the capital of Nepal. Again, the evolution of the JeM attacks in India highlights how access to technological capacity available within a politically-hospitable state such as Pakistan has allowed the group to gradually improve and expand its terrorist activities, eventually reaching the ability to execute major attacks.

One example of such a major attack occurred in 2019, when the JeM had carried out a suicide bombing of an Indian Central Reserve Police Force (CRPF) convoy in Pulwama in Indian-controlled Kashmir that ultimately resulted in the death of 40 personnel. [83] The suicide bomber was a native Kashmiri who had joined the JeM in 2018 and the group had claimed responsibility

for the attack on social media within an hour of the attack. An investigation led by the Kashmiri police and Indian security forces revealed that JeM members smuggled explosives into Kashmir from across the border, using the support of local sympathizers. This assistance had enabled the terrorists to drive the IED laden vehicle into the convoy.[84] While the JeM has received support from Pakistan, over the past decade it has been able to cultivate a substantial network within parts of the Kashmir Valley, which enabled it to act increasingly independently.[85]

Again, the JeM's recruitment activities also illustrate the importance of the resource capacity and alignment capacity mechanisms we hypothesized. Recent investigations conducted by the India's National Intelligence Agency (NIA) show that the JeM used peer-to-peer software that allowed for digital anonymity and end-to-end encryption during the Pulwama operation. The NIA also obtained evidence of conversations between the JeM leadership in Pakistan and Mohammed Umar Farooq, a key JeM operative in India who was subsequently killed. Also in line with our hypothesized resource capacity mechanisms, Farooq was able to use different banking facilities within Pakistan, Allied Bank Limited and its Meezan Bank, to transfer and access funds in order to help funding the attack.[86] The JeM has also maintained close ties to the LeT and the Afghan Taliban, sharing training camps and recruitment efforts in Pakistan, and learning from these groups' experiences, especially with regards to using technology. These ties bolstered the JeM's presence in both Pakistan and Indian-controlled Kashmir, starting 1989.[87]

Although the two groups differ in terms of tactics, with the JeM favoring suicide bombings compared with the LeT's more organized attacks, both the 2008 Mumbai attack by the LeT and the 2019 Pulwama attack have effectively illustrated the linkages we hypothesized between political hospitability, technological capacity, and terrorism, and the mechanisms operating therein. This is especially interesting considering the fact that at least in the case of the LeT, the

ability to utilize technological capacity has been one reason that it has become a threat even to ISI and the very state that enabled its activities,[88] thereby underscoring the role of technology we theorize in this study.

Conclusion

Policymakers and scholars alike have struggled to identify and prevent the dangers of international terrorism. Since the 1970s, and especially since the beginning of the 21st century, this goal has attracted a combined effort that spans multiple states and has cost trillions of dollars. Research – and policymaking – highlighted linkages between ungoverned spaces and state failures on the one hand, and increased terrorist activity on the other.[89] In these states, terrorist organizations can take advantage of the lack of governance to establish a base of operations. Yet, building on more recent, case-based research,[90] we have shown that without the capacities to expand and develop organizational capabilities, such politically-hospitable states are still less than ideal host for terror group operations. Our results also suggest that in low-technological-capacity contexts, counterterrorism efforts by the U.S. and its allies may actually be quite effective in combating terrorism (as illustrated in Figures 1 and 2).

Yet, as was additionally illustrated in these figures, our theory findings also suggest that in a subset of these politically-hospitable countries terrorism activity indeed increases. We have specifically shown that this increase is statistically and substantively related to the extent of technological infrastructure and development levels within these hospitable/targeted states. Groups that enjoy access to greater technological capacity within these politically-enabling states, are not only more effective at expanding the range and intensity of their attacks against a host of targets, but also and specifically against coalition forces that invaded these states to eliminate them.

Our findings have important implications for policymakers. First, they suggest that efforts to identify nascent terror groups and potential attacks in advance should look to specific countries that lie at the intersection of the willingness to support – or at least enable – terrorism *and* offer relatively high technological capacity for such groups to expand their operations. Past research highlighted Pakistan as such a risk case.[91] Other possible "hotzones" include "rogue" states with relatively high technological capabilities such as Venezuela, North Korea, or (to a large extent) Lebanon, as well as contested territories within countries with relatively developed technological capacities such as the Crimean Peninsula (Ukraine), the Occupied Territories (Israel/Palestine), or Nagorno-Karabakh (Azerbaijan).

Second, in using major counterterrorism efforts as our proxy for politically-hospitable countries for terrorism, which builds on current beliefs within both the policymaking and the academic research worlds,[92] we identify another important implication. Indeed, our findings suggest that international counterterrorism efforts within high infrastructure states are not only less successful but may actually have the opposite of their intended effects, leading to a precipitous increase in terrorist activity within these states. Presumably, this happens because terrorists within these more developed targeted states can take advantage of the capacity available to them locally to wage an effective campaign against both the state and the invaders. As a result, in attempting to fight these violent actors within such hospitable and moderate-to-high technological infrastructure territories using traditional means, anti-terrorism coalitions may find their efforts to be less effective than in other contexts.

There are some possible solutions for this problem. For example, states engaged in global counterterrorism efforts could utilize local nonstate forces to assist with collecting local information and enforcing policy. One recent example has been the reliance of the U.S. on the

Kurdish *peshmerga* militia to fight the Islamic State in Syria and Iraq. It is also possible to alter the incentives of some host states (e.g., via economic sanctions or aid), encouraging them to withdraw their active or tacit support for the terror groups operating within their borders, although it is unclear how likely this method is to work, as some examples (e.g., Pakistan) illustrate.

For academics, our theory and findings highlight an important relationship between technology, politics, and terrorism, showing that that terrorist group activity will be at its highest not only in politically-hospitable countries, but specifically in a subset of these states that offer sufficient technological capacities for groups to expand their operations. Future research would benefit from examining in more detail the intersection of political willingness and technological capacity. Indeed, this approach would correspond to recent research on political violence, which looks at intersections between politics, development, and conflict at the local level.[93] In line with this research, our findings suggests that a particularly beneficial research direction would be to systematically explore where terrorist activity increases *within* both politically-hospitable and non-hospitable states; and whether the effects of technology, infrastructure, and development are uniform within these countries, or whether they vary across different areas, thus identifying specific high-risk areas within even within states that are not necessarily supportive of such activities.

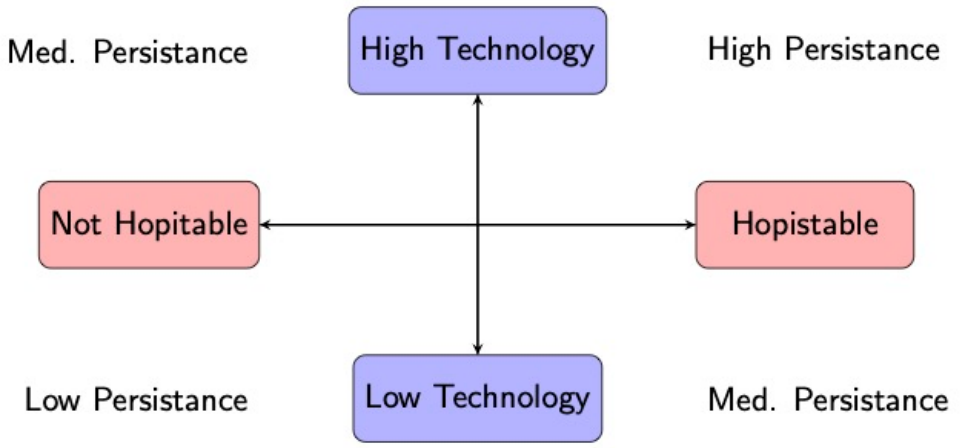
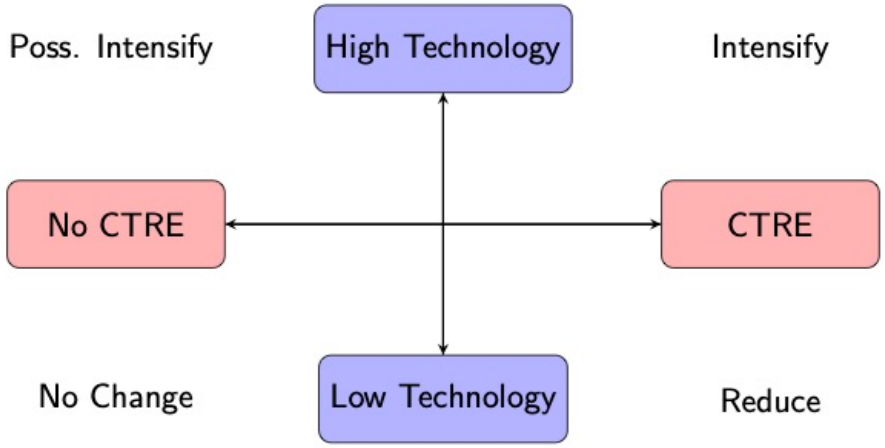


Figure 1(a): Terror group activity persistence



(Figure 1b): Counterterrorism and terrorist activity

Figure 1. The spectrums of technological capacity, political hospitability, and terror group activity persistence, and counterterrorism and terrorist activity.

	OLS		GMM	
	Baseline	**Full**	**Baseline**	**Full**
Electricity Access$_{it}$ [1]	1.043	1.218	5.146***	2.866***
	(1.515)	(1.674)	(0.417)	(0.667)
Int. Counterterrorism$_{it}$	−248.250**	−105.876	−841.829***	−81.671***
	(105.239)	(70.584)	(54.950)	(26.358)
Electricity Access$_{it}$ [1] × *Int. Counterterrorism*$_{it}$	22.623***	8.149*	60.094***	6.640***
	(6.583)	(4.530)	(3.360)	(1.678)
Population$_{it}$ [1]		−1.676		0.724
		(1.018)		(0.861)
Polity2$_{it}$		1.395***		0.476***
		(0.299)		(0.056)
GDP Per Capita$_{it}$ [1]		5.500***		−2.930***
		(1.903)		(0.517)
Military Troops$_{it}$ [1]		4.406***		0.547***
		(1.164)		(0.199)
Constant	−21.970	−132.256***		
	(31.607)	(44.081)		
Observations	2,434	1,622	2,434	1,622
R^2	0.424	0.544		
Adjusted R^2	0.381	0.493		
Sargan			152.402***	130.079***
AR(1)			-0.529	0.896

*p<0.1; **p<0.05; ***p<0.01.

Variable coefficients are reported with standard errors in parentheses. In the OLS models, SEs were clustered by country, and fixed effects by country and year were included, although not reported.

In the GMM models, two-way (country and year) effects were included and a two-step robust standard errors are reported.

[1] Natural log.

Table 1. Determinants of Terrorist Activity, 2001–2016

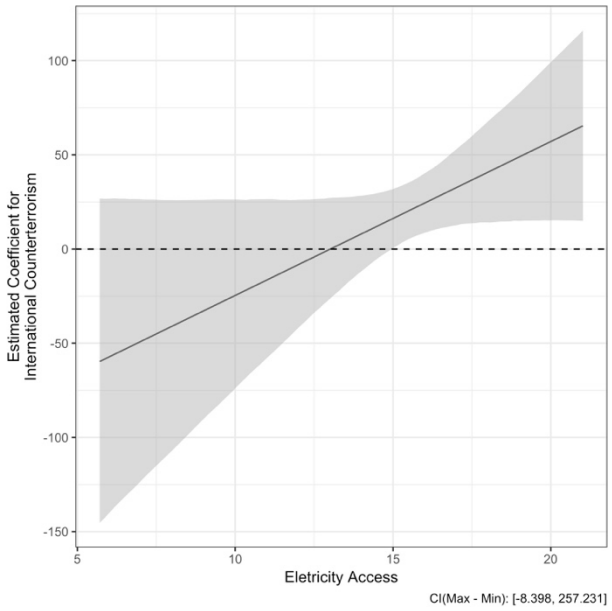


Figure 2. Change in *International Counterterrorism*$_{it}$'s coefficient as *Electricity Access*$_{it}$ changes from minimum to maximum values.

	NTL		Log DV		Count	Controls FE		Controls RE	Unsanctioned	
	OLS	GMM	OLS	GMM		OLS	GMM		OLS	GMM
Electricity Access$_{it}$[1]	−0.176	0.409	0.014	0.092	1.547***	−0.314	1.957***	1.324	1.205	2.919***
	(3.307)	(0.460)	(0.047)	(0.064)	(0.195)	(1.695)	(0.472)	(0.945)	(1.673)	(0.644)
Int. Counterterrorism$_{it}$	−5.136	−0.147	−7.889***	−7.978***	−17.576**	−158.824**	−71.108***	−119.521*	−105.557	−80.833***
	(16.026)	(2.625)	(1.961)	(1.635)	(8.766)	(79.753)	(15.297)	(71.265)	(70.535)	(25.345)
Electricity Access$_{it}$[1] × *Int. Counterterrorism*$_{it}$	6.460*	5.692***	0.613***	0.637***	1.199**	12.024**	5.953***	9.209**	8.127*	6.598***
	(3.560)	(0.184)	(0.126)	(0.118)	(0.532)	(5.272)	(0.965)	(4.589)	(4.527)	(1.603)
Population$_{it}$[1]	−1.628	3.102***	0.003	0.080	0.001	0.131	1.921***	1.317	−1.675*	0.749
	(1.067)	(0.458)	(0.028)	(0.064)	(0.021)	(1.071)	(0.359)	(0.888)	(1.017)	(0.835)
Polity2$_{it}$	1.419***	0.407***	0.033***	0.012	0.135***	1.386***	0.558***	0.926***	1.395***	0.450***
	(0.295)	(0.048)	(0.008)	(0.008)	(0.009)	(0.306)	(0.067)	(0.207)	(0.298)	(0.053)
GDP Per Capita$_{it}$[1]	5.425***	−2.011***	0.027	−0.080	0.426***	3.331*	−2.543***	−0.263	5.503***	−2.959***
	(1.904)	(0.554)	(0.053)	(0.052)	(0.060)	(1.944)	(0.244)	(1.041)	(1.902)	(0.496)
Military Troops$_{it}$[1]	4.278***	0.572***	0.175***	0.027	0.151***	0.841	0.668**	0.751	4.417***	0.558***
	(1.148)	(0.201)	(0.032)	(0.020)	(0.039)	(1.405)	(0.269)	(0.660)	(1.164)	(0.209)
Oil Rents$_{it}$						0.011	0.087***	0.059		
						(0.180)	(0.025)	(0.106)		
Coup$_{it}$						1.674	−0.376	0.966		
						(2.368)	(0.773)	(2.334)		
Mountains								0.023		
								(0.066)		
Ethnic frac.								12.888**		
								(5.580)		
Religious frac.								−9.125		
								(6.552)		
Constant	−105.184**		−1.828		−36.223***	−51.577		−48.795***	−132.218***	
	(42.565)		(1.224)		(3.675)	(46.963)		(13.785)	(44.050)	
Observations	1,640		1,622		1,622	1,589		1,589	1,622	
R^2	0.544		0.794			0.538			0.544	
Adjusted R^2	0.493		0.771			0.485			0.492	
Sargan		129.557***		69.772**			126.573***			135.388
AR(1)		1.003		-3.840***			0.928			0.915
Log Likelihood					−2,510.076			−6,887.292		
Akaike Inf. Crit.					5,352.152			13,828.580		

*p<0.1; **p<0.05; ***p<0.01.

Variable coefficients are reported with standard errors in parentheses. In the OLS models, SEs were clustered by country, and fixed effects by country and year were included, although not reported.

In the GMM models, two-way (country and year) effects were included and a two-step robust standard errors are reported.

[1] Natural log.

Table 2. Determinants of Terrorist Activity, 2001–2016, Robustness Models

Appendix:

	Min	Median	Mean	Max	Std. Dev.
Terrorist Activity$_{it}$	0	0	10.749	1094	57.950
Electricity Access$_{it}$[1]	0	15.678	15.777	21.044	1.859
Int. Counterterrorism$_{it}$	0	0	0.0170	1	0.129
Population$_{it}$[1]	6.379	9.348	9.901	19.594	2.338
Polity2$_{it}$	-10	6	3.689	10	6.313
GDP Per Capita$_{it}$[1]	5.100	8.566	8.559	11.155	1.295
Military Troops$_{it}$[1]	0	10.463	10.297	14.653	2.264
Electricity Access (NTL)$_{it}$[1]	0.240	4.463	4.553	10.045	1.974
Oil Rents$_{it}$	0	0.046	4.4201	67.528	10.635
Coup$_{it}$	0	0	0.022	2	0.191
Mountains	0	9.3	17.924	94.3	21.896
Ethnic frac.	0.001	0.395	0.414	0.925	0.275
Religious frac.	0	0.375	0.381	0.783	0.215
Unsanctioned attacks$_{it}$	0	0	10.711	1090	57.900

[1] Natural log.

Table A1. Summary Statistics of All Empirical Variables

[1] Rem Korteweg, and David Ehrhardt, "Terrorist black holes: A study into terrorist sanctuaries and governmental weakness" (Clingendael Centre for Strategic Studies, The Hague, 2005), 26; Cristiana C. Brafman. Kittner, "The role of safe havens in Islamist terrorism," *Terrorism and Political Violence* 19, no. 3 (2007): 307-329; James A. Piazza "Incubators of terror: Do failed and failing states promote transnational terrorism?" *International Studies Quarterly* 52, no. 3 (2008): 469-488.

[2] Stewart Patrick, "Weak states and global threats: Fact or fiction?" *Washington Quarterly* 29, no. 2 (2006): 27-53; Ken Menkhaus, "Quasi-states, nation-building, and terrorist safe havens" *Journal of Conflict Studies* 23, no. 2 (2003); Elizabeth Grimm Arsenault, and Tricia Bacon. "Disaggregating and defeating terrorist safe havens*," Studies in Conflict & Terrorism* 38, no. 2 (2015): 85-112.

[3] Robert A. Pape, "The strategic logic of suicide terrorism," *American Political Science Review* 97, no. 3 (2003): 343-361; Martha Crenshaw, "Terrorism research: The record," *International Interactions* 40, no. 4 (2014): 556-567; Arsenault and Bacon, "Disaggregating and defeating terrorist safe havens"; Piazza, "Incubators of terror".

[4] Gary LaFree and Laura Dugan, "Introducing the global terrorism database," *Terrorism and Political Violence* 19, no. 2 (2007): 181-204.

[5] Korteweg and Ehrhardt, "Terrorist black holes".

[6] Ibid., 23.

[7] Kittner, "The role of safe havens in Islamist terrorism".

[8] Piazza, "Incubators of terror", 470.

[9] Patrick, "Weak states and global threats".

[10] Ken Menkhaus, "Quasi-states, nation-building, and terrorist safe havens," *Journal of Conflict Studies* 23, no. 2 (2003).

[11] Ariel I. Ahram, "The role of state-sponsored militias in genocide," *Terrorism and Political Violence* 26, no. 3 (2014): 488-503.

[12] e.g., Aidan Hehir, "The myth of the failed state and the war on terror: A challenge to the conventional wisdom," *Journal of Intervention and Statebuilding* 1, no. 3 (2007): 307-332.

[13] Arsenault and Bacon, "Disaggregating and defeating terrorist safe havens".

[14] Ibid.

[15] Menkhaus, "Quasi-states, nation-building, and terrorist safe havens", Korteweg and Ehrhardt, "Terrorist black holes" and Piazza, "Incubators of terror".

[16] Ore Koren, "Food, state power, and rebellion: The case of maize," *International Interactions* 45, no. 1 (2019): 170-197; Ore Koren and Anoop K. Sarbahi. "State capacity, insurgency, and civil war: A disaggregated analysis," *International Studies Quarterly* 62, no. 2 (2018): 274-288.

[17] Adam Roberts, "The 'war on terror' in historical perspective," *Survival* 47, no. 2 (2005): 101-130.

[18] Brian A. Jackson, "Technology acquisition by terrorist groups: threat assessment informed by lessons from private sector technology adoption," *Studies in Conflict & Terrorism* 24, no. 3 (2001): 183-213; Craig Espeseth, Jessica Gibson, Andy Jones, and Seymour Goodman, "Terrorist use of communication technology and social networks," in *Technological Dimensions of Defense Against Terrorism*, ed. U. Feyyaz Aydogdu, (Amsterdam: IOS Press, 2013), 91-105.

[19] e.g., Pape, "The strategic logic of suicide terrorism"; Gordon H. McCormick, "Terrorist decision making," *Annual Review of Political Science* 6, no. 1 (2003): 473-507 ; Crenshaw,

"Terrorism research" ; James A. Piazza, "Regime age and terrorism: Are new democracies prone to terrorism?" *International Interactions* 39, no. 2 (2013): 246-263.
[20] Ahram, "The role of state-sponsored militias in genocide"; Korteweg and Ehrhardt, "Terrorist black holes"; Piazza, "Incubators of terror".
[21] Arsenault and Bacon, "Disaggregating and defeating terrorist safe havens".
[22] Piazza, "Incubators of terror", 483.
[23] Roberts, "The 'war on terror' in historical perspective"; Crenshaw, "Terrorism research".
[24] Jackson, "Technology acquisition by terrorist groups", Espeseth et al., "Terrorist use of communication technology and social networks".
[25] Arsenault and Bacon, "Disaggregating and defeating terrorist safe havens".
[26] e.g., Xi Chen and William D. Nordhaus, "Using luminosity data as a proxy for economic statistics," *Proceedings of the National Academy of Sciences* 108, no. 21 (2011): 8589-8594; Koren, "Food, state power, and rebellion".
[27] e.g., Piazza, "Incubators of terror"; McCormick, "Terrorist decision making".
[28] Koren and Sarbahi, "State capacity, insurgency, and civil war"; Chen and Nordhaus, "Using luminosity data as a proxy for economic statistics".
[29] Koren and Sarbahi, "State capacity, insurgency, and civil war".
[30]Espeseth et al., "Terrorist use of communication technology and social networks".
[31] Geoff Dean and Peter Bell, "The dark side of social media: review of online terrorism," *Pakistan Journal of Criminology* 3, no. 4 (2012): 191-210.
[32] Md Sazzad Hossain, "Social media and terrorism: threats and challenges to the modern era," *South Asian Survey* 22, no. 2 (2015): 141.
[33] Ibid., 144.
[34] Chen and Nordhaus, "Using Luminosity Data as a Proxy for Economic Statistics"; Koren and Sarbahi, "State Capacity, Insurgency, and Civil War".
[35] Ore Koren and Bumba Mukherjee, "Economic Crises, Civilian Mobilization, and Repression in Developing States," *Conflict Management and Peace Science* (forthcoming).
[36] Roberts, "The 'war on terror' in historical perspective".
[37]Arsenault and Bacon, "Disaggregating and defeating terrorist safe havens".
[38] Roberts, "The 'war on terror' in historical perspective".
[39] Jackson, "Technology acquisition by terrorist groups"; Roberts, "The 'war on terror' in historical perspective"; Crenshaw, "Terrorism research".
[40] Although we have data on terrorist attacks going up to 2018, we were forced to omit the last two years due to missing information on our *Electricity Access*$_{it}$ indicator.
[41] Note: the *i* and *t* subscripts refer to a given country and a given year, respectively.
[42] Gary LaFree and Laura Dugan, "Introducing the global terrorism database*", Terrorism and Political Violence* 19, no. 2 (2007): 181-204.
[43] Note that the same group could operate in different countries. Considering our emphasis on within-country variations, we account for these issues in the empirical models below.
[44] A complete list of all incidents coded over the 2001-2018 period, a total of 34,855 unique incidents, is provided in a separate online-only supplemental file.
[45] e.g., Chen and Nordhaus, "Using Luminosity Data as a Proxy for Economic Statistics", Koren, "Food, state power, and rebellion" and Koren and Sarbahi, "State capacity, insurgency, and civil war".
[46] World Bank (WB), "World Development Indicators", The World Bank, (accessed March, 12, 2020) http://datatopics.worldbank.org/world-development-indicators/.

We estimate a robustness model that uses nighttime light emissions instead at the Supplemental Appendix.
[47] These states (i.e., where *International Counterterrorism*$_{it}$=1) include Mali (2013-2018), Mauritania (2010), Niger (2017-2018), Central African Republic (2006), Somalia (2015-2018), Libya (2016-2018), Iraq (2003-2018), Yemen (2009-2014), and Afghanistan (2001-2018).
[48] Roberts, "The 'war on terror' in historical perspective"; Arsenault and Bacon, "Disaggregating and defeating terrorist safe havens".
[49] Philip A. Schrodt, "Seven deadly sins of contemporary quantitative political analysis," *Journal of peace research* 51, no. 2 (2014): 287-300.
[50] World Bank (WB), "World Development Indicators".
[51] Kristian Skrede Gleditsch, "Expanded trade and GDP data," *Journal of Conflict Resolution* 46, no. 5 (2002): 712-724.
[52] Monty G. Marshall, Ted R. Gurr, and K. Jaggers. 2019. "Polity iv project: Political regime characteristics and transitions, 1800-2018." Technical Report.
[53] The Stockholm International Peace Research Institute (SIPRI), "Military Expenditure Database," SIPRI, (accessed January, 15 2020) https://www.sipri.org/databases/milex.
[54] Richard Blundell and Stephen Bond, "Initial conditions and moment restrictions in dynamic panel data models", *Journal of econometrics* 87, no. 1 (1998): 115-143.
[55] Joshua D. Angrist and Jörn-Steffen Pischke, *Mostly harmless econometrics: An empiricist's companion* (New York: Princeton university press, 2008).
[56] Blundell and Bond, "Initial conditions and moment restrictions in dynamic panel data models".
[57] The only country in our sample where people had no recorded regular access to electricity is Eritrea, 2012-2016. However, this country has not been targeted by an external country as part of a counterterrorism effort and, moreover, it is omitted from the full model due to missing information on some of the controls.
[58] e.g., Chen and Nordhaus, "Using Luminosity Data as a Proxy for Economic Statistics", Koren, "Food, state power, and rebellion" and Koren and Mukherjee, "Economic Crises, Civilian Mobilization, and Repression in Developing States".
[59] We use the Poisson due to our reliance on country and year fixed effects, which bias Negative Binomial model estimate (see Paul D. Allison and Richard P. Waterman, "Fixed–effects negative binomial regression models," *Sociological methodology* 32, no. 1 (2002): 247-265.
[60] Jason Seawright and John Gerring, "Case selection techniques in case study research: A menu of qualitative and quantitative options," *Political research quarterly 61*, no. 2, (2008): 299.
[61] Tricia Bacon, "The Evolution of Pakistan's Lashkar-e-Tayyiba Terrorist Group," *Orbis* 63, no. 1 (2019): 27-43.
[62] Ashley J. Tellis, "The menace that is Lashkar-e-Taiba," *Policy Outlook, Carnegie Endowment for International Peace* 13 (2012).
[63] Stephen Tankel, *Storming the world stage: The story of Lashkar-e-Taiba* (UK: Oxford University Press, 2013).
[64] Stephen Tankel, "*Lashkar-e-Taiba: Past operations and future prospects*" (New America Foundation, 2011)
[65] Tankel, *Storming the world stage.*

[66] Cathy Scott- Clark and Adrian Levy, *The Siege: 68 Hours Inside the Taj Hotel* (New York: Penguin Random House, 2013).

[67] Sebastian Rotella, "Militant Reaffirms Role of Pakistan in Mumbai Attacks," *Foreign Policy*, Aug. 9, 2012, https://foreignpolicy.com/2012/08/09/militant-reaffirms-role-of-pakistan-inmumbai-attacks/ (accessed April 29, 2021).
[68] Meetu Jain, "Read: David Headley's NIA interrogation report", *News 18 India*, May 24, 2011, https://www.news18.com/news/india/headley-13-370584.html (accessed April 29, 2021).
[69] Jeremy Kahn, "Mumbai Terrorists Relied on New Technology for Attacks", *New York Times*, December 8, 2008, https://www.nytimes.com/2008/12/09/world/asia/09mumbai.html (accessed April 29, 2021).
[70] S Ahmed Ali, "26/11: Abu Jundal names same Pak army officers as Headley did," *Times of India* , July 3, 2012, https://timesofindia.indiatimes.com/city/mumbai/26/11-Abu-Jundal-names-same-Pak-army-officers-as-Headley-did/articleshow/14619870.cms (accessed April 29, 2021).
[71] Bacon, "The Evolution of Pakistan's Lashkar-e-Tayyiba Terrorist Group".
[72] Wilson John, "LeT's Social Media Warfare" (Observer Research Foundation, Mumbai, 2013) http://www.orfonline.org/research/lets-social-media-warfare/ (accessed May 3, 2021).
[73] Manjeet Negi, "Exclusive: Security agencies planning to counter Lashkar-e-Taiba's social media propaganda", *India Today, April 5, 2017,* https://www.indiatoday.in/india/story/security-agencies-lashkar-e-taiba-social-media-propaganda-twitter-969715-2017-04-05 (accessed May 3, 2021).
[74] Munish Sharma, "Lashkar-e-Cyber of Hafiz Saeed" (Manohar Parrikar Institute for Defence Studies and Analyses, New Delhi) https://idsa.in/idsacomments/lashkar-e-cyber-of-hafizsaeed_msharma_310316 (accessed May 3, 2021).
[75]Ibid.
[76] Ibid.
[77] Milos Popovic, "The perils of weak organization: Explaining loyalty and defection of militant organizations toward Pakistan," *Studies in conflict & terrorism* 38, no. 11 (2015): 919-937; Paul S. Kapur and Sumit Ganguly. "The jihad paradox: Pakistan and Islamist militancy in South Asia," *International Securit*y 37, no. 1 (2012): 111-141.
[78] ET Bureau, "ISI's major Iqbal, LeT chief Saeed in India's most-wanted list", *Economic Times,* May 12, 2011, https://economictimes.indiatimes.com/news/politics-and-nation/isis-major-iqbal-let-chief-saeed-in-indias-most-wanted-list/articleshow/8257210.cms (accessed May 3, 2021).
[79] Salman Masood, "Terror Suspect Cleared Again in Pakistan", *New York Times*, October 12, 2009, https://www.nytimes.com/2009/10/13/world/asia/13lahore.html (accessed May 3, 2021).
[80] Mehmal Sarfaz, "Pakistan court indicts Hafiz Saeed on terror financing charges", *The Hindu, December 11, 2019,* https://www.thehindu.com/news/international/pak-court-indicts-hafiz-saeed-on-terror-financing-charges/article30275565.ece (accessed May 3, 2021).
[81] Shishir Gupta, "New J&K terror outfit run by LeT brass: Intel", *Hindustan Times,* May 8, 2020, https://www.hindustantimes.com/india-news/new-j-k-terror-outfit-run-by-let-brass-intel/story-wLZ5ACFQJMHVa8kt7weTPO.html (accessed May 3, 2021) ; Zeenat Zeeshan Fazil, "Little-known ISI-backed Terrorist Group Surfaces In Kashmir Valley", *Republic World,* April 28, 2020, https://www.republicworld.com/india-news/general-news/little-known-isi-backed-terrorist-group-surfaces-in-kashmir-valley.html (accessed May 3, 2021)
[82] Popovic, "The perils of weak organization"; Kapur and Ganguly, "The jihad paradox".
[83] Deeptiman Tiwary, "Pulwama attack: Probe finds car bumper, remains of can in which explosives were packed", *Indian Express,* February 19, 2019, https://indianexpress.com/article/india/pulwama-attack-probe-finds-car-bumper-remains-of-can-in-which-explosives-were-packed-5590202/ (accessed April 29, 2021).

[84] Ibid.
[85] Neeraj Chauhan, "Photos, chats and a phone: How NIA cracked the Pulwama case", *Hindustan Times,* August 26, 2020, https://www.hindustantimes.com/india-news/photos-chats-and-a-phone-how-nia-cracked-the-pulwama-case/story-ImJ7ZmnhnzXLYH9c7E2qcI.html (accessed April 29, 2021) ; Raghav Ohri, "Kashmiri youth visiting Pakistan used as terror conduits: Government agency", *Economic Times,* July 13, 2018, https://economictimes.indiatimes.com/news/defence/kashmiri-youth-visiting-pakistan-used-as-terror-conduits-government-agency/articleshow/61620328.cms (accessed May 3, 2021).
[86] Chauhan, "Photos, chats and a phone".
[87] Sumit Ganguly, *The crisis in Kashmir: Portents of war, hope of peace* (Cambridge, UK: Cambridge University Press, 1997).
[88] Bacon, "The Evolution of Pakistan's Lashkar-e-Tayyiba Terrorist Group" ; Tellis, "The menace that is Lashkar-e-Taiba".
[89] e.g., Korteweg and Ehrhardt, "Terrorist black holes", Kittner, "The role of safe havens in Islamist terrorism" and Piazza, "Incubators of terror".
[90] e.g., Arsenault and Bacon, "Disaggregating and defeating terrorist safe havens".
[91] Ibid.
[92] e.g., Roberts, "The 'war on terror' in historical perspective" ; Piazza, "Incubators of terror".
[93] e.g., Koren and Sarbahi, "State capacity, insurgency, and civil war", Koren, "Food, state power, and rebellion" and Håvard Hegre, Marie Allansson, Matthias Basedau, Michael Colaresi, Mihai Croicu, Hanne Fjelde, Frederick Hoyles et al. "ViEWS: a political violence early-warning system," *Journal of Peace Research* 56, no. 2 (2019): 155-174.