Multi-Modal Networks Reveal Patterns of Operational Similarity of Terrorist Organizations

Gian Maria Campedelli[a,1,2], **Iain Cruickshank**[b,1], **and Kathleen M. Carley**[b]

[a]Department of Sociology and Social Research - University of Trento, 38122 Trento, Italy; [b]School of Computer Science - Carnegie Mellon University, 15213 Pittsburgh, PA, United States of America

This manuscript was compiled on April 14, 2025

Capturing dynamics of operational similarity among terrorist groups is critical to provide actionable insights for intelligence monitoring and counter-terrorism risk assessment tools. Nonetheless, in spite of its theoretical and practical relevance, research addressing this problem is currently lacking. We here propose a scalable computational framework for detecting clusters of terrorist groups sharing similar behaviors, focusing on each group's yearly repertoire of deployed tactics, attacked targets, and utilized weapons. In the current work, we specifically consider those organizations that have plotted at least 50 attacks from 1997 to 2018 accounting for a total of 105 groups responsible for more than 42,000 attacks worldwide. Our clustering approach offers three sets of results. First, we show that the yearly ratio between the number of detected clusters and the number of active organizations displays a downward trend over the years, signaling increasing operational cohesiveness and diminished overall heterogeneity in global terrorism. Second, we highlight that year-to-year stability in co-clustering among groups has been particularly high from 2009 to 2018, suggesting high temporal consistency in behaviors in the last decade. Third, we demonstrate that operational similarity between two organizations is driven by three factors: (a) their overall levels of activity; (b) the difference in the diversity of their operational repertoires; (c) the difference in the ratios between their operational diversity and their overall activity. Groups' operational preferences, geographical homophily and ideological affinity have no consistent role in determining co-clustering. Implications for practice are also discussed.

political violence | network science | computational social science | conflict research | counter-terrorism

Research on terrorism has examined the decision-making processes of terrorist organizations in terms of tactical behaviors and operations from various perspectives (1, 2). The empirical relevance of the topic is both theoretical and practical, transcending the boundaries of pure scientific inquiry. In fact, unraveling behaviors of terrorist organizations in terms of the epitome of their decision-making processes - i.e., their attacks - can significantly aid the design of counter-terrorism strategies.

Particularly, the choice of targets, tactics, and timing of terrorist organizations is defined by McCormick as a group's operating profile (1). A group's operating profile lies in between the concepts of influence and security: on the one hand, influence determines the group's ability to grow in terms of support and resources. On the other hand, security is fundamental to avoid external interventions and disruption. Beyond the competitive influence-security dichotomy, a group's operating profile is constrained by a set of exogenous and endogenous factors. Among these, the literature has identified ideology, resources, group size, and goals.

Terrorist groups may decide to attack specific targets because of their symbolic or strategic values in conveying ideological messages during terrorism campaigns (3–5). Furthermore, a group's operating profile can be determined by the availability of financial or material resources, as more resources tend to guarantee easier technology adoption and, consequently, higher effectiveness in terrorist operations (6, 7). Concerning goals, previous works for instance outlined how different aims are associated with different choices in target selection (8). Research on terrorists' life cycles further reveals that organizations are subject to variations in their goals, strategies, support, and resources, thus in turn also reflecting a temporal layer of variability in their decision-making processes (9–11). A group's operating profile is hence a dynamic concept, and is inherently connected to the study of terrorists' tactical innovations.

In fact, innovation not only pertains to the invention of novel weapons or the development of unprecedented strategies (12). Instead, it refers to a broad set of changes in activity that may be related to tactical shifts, such as campaigns against alternative types of targets, or modifications of a group's usual modus operandi, in line with the definition provided by Crenshaw, who argued that terrorist innovation broadly regards the adoption of new patterns of behaviors (13).

Much has been written on terrorists' decision-making, innovation and evolution of operations. Both in quantitative and qualitative terms, scholars mostly concentrated on individual groups to map changes in these aspects. However, research overlooked comprehensive comparative accounts of terrorist

Significance Statement

We present a computational framework exploiting the representational flexibility of multi-modal networks to analyze patterns of operational similarity of terrorist groups active worldwide from 1997 to 2018. Generating yearly graphs focusing on each group's deployed tactics, attacked targets, and utilized weapons, our clustering results first show that operational variability is overall in decline in the last years. Second, stability in year-to-year co-clustering has significantly heightened after 2009, outlining higher temporal consistency. Third, operational similarity between two organizations is mostly driven by groups' amount of activity, operational repertoire, and a combination of the two. Our scalable framework may result useful for improved intelligence monitoring and counter-terrorism assessment tools.

Please provide details of author contributions here.

Please declare any competing interests here.

[1]G.M.C (Author One) contributed equally to this work with I.C. (Author Two).

[2]To whom correspondence should be addressed. E-mail: gianmaria.campedelliunitn.it

behaviors and hence currently lacks knowledge on operational similarity patterns among different organizations. Such an approach may shed light on global characteristics of terrorist violence and can help both research and practice in unfolding the complexity of terrorist behaviors by highlighting behavioral tendencies that cannot be captured when considering organizations independently.

In this work we hence address this research problem, focusing on operational patterns of similarity among terrorist groups from 1998 to 2018, analyzing their dynamic mechanisms and studying the factors explaining operational affinity, building on the representational power of multi-modal networks.

In the last two decades, network science has gained a prominent role in the analysis of terrorism (14, 15). Most applications focus on the study of connections among affiliates within terrorist organizations (16, 17) or alliance relations among groups (18–20). Additionally, the literature has lately explored the flexibility of networks to map terrorist behaviors going beyond mere physical or communication networks, experimenting with computational techniques that focus on operational or strategical features of terrorist groups' behaviors (21–23). Our work fits into this latter evolving strand of transdisciplinary research.

By exploiting data retrieved from the Global Terrorist Database (24), we consider all the groups that have plotted at least 50 attacks from 1997 to 2018, accounting for a total of 105 organizations and more than 42,000 events. We specifically investigate patterns of operational similarity deriving clusters of organizations sharing similar behaviors at the yearly level using event-level information on three distinct attack dimensions — i.e., tactics, targets, and weapons. Clusters are detected using Multi-view Modularity Clustering (MVMC), an ensemble multi-view clustering technique develop to specifically deal with networks measuring or describing phenomena that can be expressed through a multi-modal representation. We use the number of detected clusters as a measure of overall heterogeneity in terrorist operations and co-clustering, i.e., being assigned to the same cluster, as evidence of operational similarity between groups. How clustering, and co-clustering, change in time help us better capture the dynamic range of macro-behavioral profiles that characterize terrorism complexity and what factors explain are able to explain pairwise patterns of similarity.

We first detected an overall reduction in operational heterogeneity over time, considering the ratio between the yearly number of the detected clusters and the yearly number of active terrorist organizations. Second, we observe increased stability of co-clustering over time. Prior to 2002 we note high year-to-year co-clustering variability, indicating that groups that were clustered together at t were then separated in the following years. This signals overall frequent changes in modi operandi in the first years of our analyses. Over time more stable co-clustering emerges, especially during the 2009-2018 period, indicating consistency in operational similarity patterns. Third, and finally, we demonstrate that the fact that two organizations are clustered together is explained by three operational characteristics and that preferences in tactics, targets, and weapons, as well as geographical and ideological homophily, do not have a role in determining operational similarity.

Materials and Methods

Data. The primary data source of this work is the Global Terrorism Database (GTD), which is the most comprehensive open-access database on terrorist events available worldwide. We here consider the world most prominent and active terrorist organizations that we operationalize as the groups that have plotted at least 50 attacks from January 1, 1997, to December 31, 2018. The sample accounts for a total of 105 organizations that have plotted more than 42,000 events worldwide. The GTD gathers more than one hundred variables associated with each event, including the perpetrator, the location (at various resolutions), the time, and operational information on the attack such as the deployed tactics, selected targets, and employed weapons.

In the present work, we specifically focus on these three latter sources of information to study the operational behaviors of terrorist groups at the yearly level. All events can be featured by up to three different tactics (labeled as "attack type"), three different targets, and four different weapons. To exemplify, an attack may be plotted using a mix of tactics, using multiple weapons against several targets simultaneously. This allows gaining a comprehensive picture of the operational yearly repertoire of each group.

Furthermore, to analyze the composition of the detected clusters, we exploit other variables included in the GTD, and particularly the regions in which organizations operate, and information on group ideologies retrieved from three main sources: the Big Allied and Dangerous (BAAD) Database (25), the Extended Data on Terrorist Groups (EDTG) dataset (26) and the TRAC platform maintained by the Terrorism Research & Analysis Consortium (27).

Multi-View Modularity Clustering. Our data are naturally structured in a multi-modal form, with tactics, targets, and weapons being the three modes defining terrorists' attacks and, in turn, terrorists' operations. Given this characteristic, and given the independent nature of the three (deploying tactic x does not imply attacking target y or using weapon z), we approach this problem as a multi-view clustering problem. From the GTD data, for each organization in each year t, and for each view of the data, we form yearly multimodal bipartite graphs, $\mathcal{G}_t^M = \left\{G_t^{\text{group}\times\text{tactic}}, G_t^{\text{group}\times\text{target}}, G_t^{\text{group}\times\text{weapon}}\right\}$, in which weights are integer entries denoting whether and how many times each terrorist organization used a certain kind of tactic, employed a certain weapon, or hit a given target.

Having established these bipartite graphs for each view and year of the data, we use the multi-view clustering technique of Multi-view Modularity Clustering (MVMC). * MVMC is a technique designed to work with multiple views, of any data type, of the same underlying social-based phenomena to produce one set of clusters (29). The technique works in two main steps. First, we take as input each graph in $\mathcal{G}_t^M$ and learn as many unipartite weighted graphs using a Radius Ball, with each new graph connecting together groups that are behaviorally similar in each respective mode. Second, an iterative process clusters all of the modal unipartite graphs by optimizing a view-weighted, resolution-adjusted modularity function (technical details are available in the SI Appendix).

Since the terrorist organizations frequently contain a small

* Source code is available at https://github.com/ijcruic/Multi-view-Clustering-of-Social-Based-Data and also as a tool within the ORA-Pro software (28)

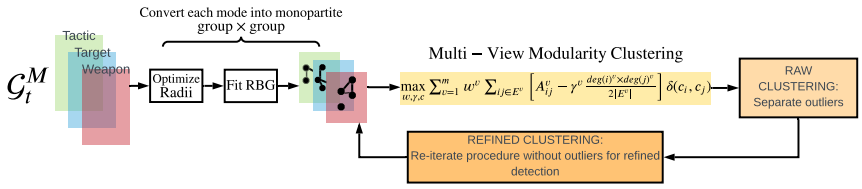

Fig. 1. Diagram of the MVMC method as used in this study. We first find Radius Ball Graphs (RBG) for each of the views of the terrorist attacks and then cluster the organizations to obtain the course clusters. We then go through the MVMC process one more time with just the organizations that end up in the single large clusters to produce the refined clusters.

number of outlier groups with significantly more attacks than most of the other terrorist organizations (see Supplementary), we iteratively perform the MVMC procedure twice to get a better clustering of the organizations. The first, or 'raw' clustering separates the outlier organizations. The second, or 'refined' clustering focuses on the remaining organizations. In this way, we can get more nuanced clusters by working on more than one resolution of the data, instead of just separating the anomalous organizations. Figure 1, provides a graphical overview of the multi-view clustering technique we use.

Finally, we perform this procedure multiple times for the same data using cluster ensembling (30). Since the MVMC algorithm is stochastic, we performed an ensembling process to guarantee robustness and make sure the discovered clusters were consistent and not a result of chance, also exploiting the computational efficiency of the algorithm.

Temporal stability in clustering assignments. To quantify the degree of co-clustering stability among terrorist organizations over the years we employ two alternative metrics: the Adjusted Rand Index (ARI) and the Fowkles Mallows score (FMS). For each pair of years taken into consideration, both metrics are calculated on the intersection sub-sample of active groups, given the level of variability in organizations active over time. This means that given two years t_i and t_j, in which two sets of groups $O_{t=i} = \{o_{1_{t=i}}, \cdots, o_{n_{t=i}}\}$ and $O_{t=j} = \left\{o_{1_{t=j}}, \cdots, o_{n_{t=j}}\right\}$ have plotted terrorist attacks, the metrics are computed on $S = O_{t=i} \cap O_{t=j}$.

The ARI is a version of the Rand Index which is adjusted for randomness. In an unsupervised learning setting with ground-truth labeling, it is generally calculated as a similarity score between two clusterings counting pairs of organizations assigned to the same clusters comparing predicted and ground-truth clusterings. In our work, we do not have ground-truth clusters labels, therefore the calculation is made taking into consideration pairs of clusterings of groups active in a given year $C(O_t = i)$ against clustering groups active in another year $C(O_t = j)$, for all possible pairs. The equation is:

$$\text{ARI} = \frac{RI - \text{expected}(RI)}{\max(RI) - \text{expected}(RI)} \qquad [1]$$

where RI stands for Rand Index and is the ratio between the number of agreeing pairs of groups clustered together and the total number of pairs possible. The score is symmetric as $\text{ARI}(C(O_t = i); C(O_t = j)) = \text{ARI}(C(O_t = j); C(O_t = i))$ and takes values in the range [-1;1], with higher values certifying higher stability.

The FMS score is instead defined as the geometric mean of precision and recall through the equation:

$$\text{FMS} = \frac{TP}{\sqrt{(TP + FP) \times (TP + FN)}} \qquad [2]$$

where TP is the number of true positives cases, i.e the pairs of organizations co-clustered together at $t = i$ and $t = j$, FP is the count of pairs of organizations belonging to the same cluster at $t = i$ but not in $t = j$ and FN is the number of pairs of organizations clustered together in $t = j$ but not in $t = i$. The FMS is bounded in the range [0;1], with higher values indicating higher similarity between clusterings in different years $C(O_t = i)$ and $C(O_t = j)$.

Inference on co-clustering. To understand what drives terrorist organizations' co-clustering we have applied Exponential Random Graph Modeling (ERGM) per each year, using as the network of interest the two-mode graph connecting a terrorist organization to its cluster of reference, in a given year. The ERGM is a well-known statistical approach to describe networks and investigate the factors that contribute to explain the structure of a particular network, allowing inferential reasoning about drivers of outcomes that are not independent of one another (i.e., nodes in a graph). ERGM has been first specified and presented by Wasserman and Pattison (31), building on previous statistical breakthroughs (32–34), and gained wide success in a number of fields, including political science (35, 36), criminology (37) and terrorism research (19, 21). Exponential Random Graph models can be generally written as:

$$P_{\theta,\mathcal{Y}}(\mathbf{Y} = \mathbf{y}|\mathbf{X}) = \frac{\exp\left\{\theta^{\mathrm{T}} g(y, X)\right\}}{\kappa(\theta, \mathcal{Y})} \qquad [3]$$

with Y representing a bipartite network with realization $\mathbf{y}$ where $y_{o,c} = 1$, meaning that a connection exists, if organization o belongs to cluster c, $g(y, X)$ being a vector of model statistics for network realization y, θ being the vector of coefficient of statistics $g(y)$ and $\kappa(\theta, \mathcal{Y})$ representing a normalizing constant, namely the numerator summed across all possible network realizations. Although developments in network modeling led to the extension of the traditional ERGM approach in order to take into account temporal dependence and sequentiality in network realizations, for instance through Temporal ERGM (TERGM) (38, 39) and separable temporal ERGM (40), we estimated yearly separate cross-sectional models. This enables us to observe year-to-year variations in coefficients and study how the influence of certain factors evolved over time. Also note that the use of TERGM is not justified as our yearly clusterings are not temporally dependent (that is, clusters in year t do not influence clusters in year $t + 1$), and therefore previous realizations of group-to-cluster networks cannot be used to generate successive ones.

The estimated models include eight covariates each. First, "Sum of Features Weights" measures the sum of all feature weights in the original bipartite multi-modal yearly networks $\mathcal{G}_t^M$ as a proxy of each group's yearly level of activity and resources. Second, "Difference in Number of non-zero features" assesses the role of organizations' pairwise difference in the

number of features characterizing attacks in each year, aiming at understanding how diversity in operational heterogeneity impacts the probability of co-clustering. Each organization's number of non-zero features is simply the count in the number of (binary) links in each year's $\mathcal{G}_t^M$. Third, "Difference in Non-zero Features to Weights Ratio" is a more comprehensive indicator of operational diversity. For each group, we calculate a ratio between the number of non-zero feature weights and "Sum of Features Weights". The ratio is bounded in the range $(0, 1]$, with higher values indicating that a terrorist group always differentiate its operations. In the ERGM, the covariate maps the absolute difference between this ratio for each pair of groups to understand if operational diversity in relation to resources impacts co-clustering. Fourth, fifth, and sixth, categorical variables "Shared most common target", "Shared most common tactic", and "Shared most common weapon" capture the role that homophily in operational preferences has in co-clustering, investigating whether two organizations sharing the same most common target, tactic and weapon — which are obtained by group's highest weight in the respective mode of $\mathcal{G}_t^M$ — impacts the likelihood of being in the same cluster. Seventh, the categorical variable "Shared Region" addresses geographical homophily, mapping whether two terrorist groups that are mostly active in the same geographic region are also operationally more similar. The rationale is to examine if macro-geographical affinity patterns characterizing terrorist operations exist. Eighth, and finally, the categorical covariate "Shared Ideology" analyzes whether two groups have a higher or lower likelihood of being co-clustered together when sharing the same ideological motives.

Results

Temporal Trends in Cluster Formation. The temporal trends of the yearly number of detected clusters, active groups, and the derived ratio of clusters to groups are displayed in Figure 2. Considering only the trend in the number of detected clusters, oscillations emerge and no clear pattern can be disentangled. However, when this trend is connected with the one reporting the number of active terrorist organizations in each year, and particularly when the ratio of these two quantities is taken into account, a significant downward trend can be appreciated.

This finding indicates that over the course of the period 1997-2018, terrorist groups have reduced their heterogeneity and diversity in terms of deployed tactics, selected targets, and utilized weapons. Despite a clear increase in the number of organizations, the number of clusters remains very similar, thus pointing in the direction of the presence of a considerable amount of terrorist organizations being very close to each other operationally. This intuition is further reinforced by the analysis of the network statistics of the RBG networks over time, provided in detail in the SI Appendix Fig. S8. When considering the multi-modal graphs obtained through the RBG procedure, data show an increasing graph density over time, as well as an increasing amount of clustering coefficient over all the three considered modes. In a related fashion, the number of components mostly stabilizes after oscillating dynamics after 2004. Besides the yearly oscillating number of outliers, i.e., extremely prolific groups with unique operational profiles, We argue that a critical mass of organizations, representing the majority of the active organizations, became more and more cohesive and thus similar from an operational point of view.

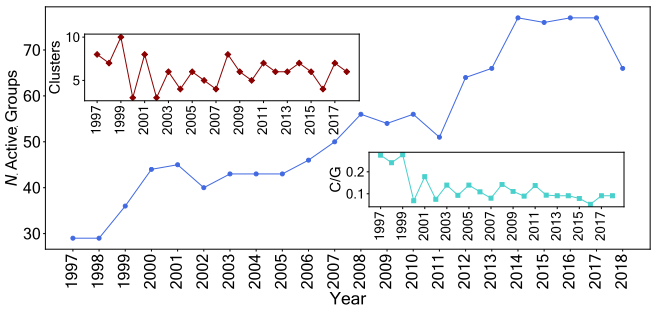

Fig. 2. Trend of detected clusters over time (top-left panel), number of active terrorist organizations in each year (main panel), and cluster to groups ratio (bottom-right panel). While the number of active groups has been significantly increasing from 1997 to 2018, the number of clusters remains almost stable, leading to a significantly decreasing trend in the cluster to groups ratio. This may indicate an overall reduction in the variety of operational behaviors, and a tendency over homogeneity.

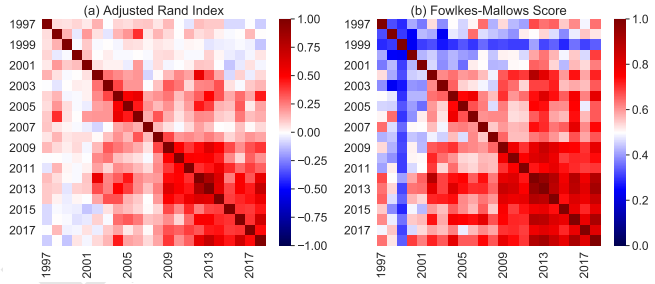

Fig. 3. ARI (left) and FMS (right) showing the degree of organizations' co-clustering stability over the years. Both metrics reveal a certain degree of stability from 2002 to 2018, with two separate sub-regions where stability is stronger, namely 2002-2006 and 2009-2018. Conversely, before 2002, terrorist organizations were more inclined to change their operations considerably from one year to another.

Stability of co-clustering. Consistent outcomes emerge in relation to co-clustering stability (Figure 3), in spite of the different ways in which the two metrics are computed. Across both measures, we can identify a temporal region of high stability from 2009 to 2018. Similarly, stability is identified in the years 2002-2006. Terrorist organizations operating in these two temporal frames tended to be clustered with the same groups year after year, suggesting a limited degree of variations in behaviors and, consequently, a certain level of consistency in operations over time. The picture is completely different when we consider terrorist organizations co-clustering prior to 2002. In the first five years of our analysis, the probability of two groups being clustered together in two different years is low, pointing in the direction of a considerable amount of operational variations in decision-making processes and behaviors characterizing terrorist organizations.

These results should be read in conjunction with the ones presented in the previous subsection, where we showcased a consistent downward trend in terrorists' operational diversity marking the years considered in our study. Results are corroborated by the robustness check with the enlarged sample (see SI Appendix Fig. S7).

Drivers of Similarity. Three factors appear to be the main drivers of operational similarity in the form of co-clustering, testified by Figure 4 (in-depth quantitative explanation of the ERGM results is provided in the SI Appendix). First, as shown by subfigure (a), "Sum of Features Weights" significantly

impacts the probability of co-clustering (avg. $\theta_{1997-2018} = -0.007$, significant at the 95% level in 68.18% of the years). The lower the summed amount of activity and resources characterizing two groups, the higher the likelihood that they will be connected to the same cluster. Conversely, the higher the sum, the lower the probability of co-clustering. High-resource groups tend to be isolated as they possess unique profiles, and groups with low resources are not clustered together with high-resource organizations as their resource mismatch is too large to allow for proper similarity detection (see SI Appendix for a proper example). Second, subfigure (b) highlights that similarity in the yearly operational repertoire correlates with co-clustering (avg. $\theta_{1997-2018} = -0.116$, significant at the 95% level in 77.27% of the years) . In fact, the lower the difference in terms of non-zero features between two organizations, the higher the likelihood of them being operationally similar. Hence, organizations with highly diverse yearly repertoires will be more likely to be in the same clusters with other terrorist groups characterized by the same behavioral heterogeneity. Third, also the difference in non-zero features to weights ratio strongly influences the odds of co-clustering for two terrorist organizations. The combination of both features weights - as a proxy of overall activity - and non-zero features - as a measure of heterogeneity - captures operational patterns of similarity among organizations (avg. $\theta_{1997-2018} = -3.332$, significant at the 95% level in 77.27% of the years).

On the other hand, the three other covariates mapping homophily in operational preferences (i.e., most common target, most common tactic, and most common weapon) do not exhibit correlations with co-clustering, with the exceptions of few years. Coefficients are mostly non-significant, and their direction is not easily identifiable, especially for shared most common tactics. The lack of consistent findings for these three variables investigating operational homophily suggests that similarity between two groups is not only a matter of raw preference over a particular target, tactic, or weapon. Instead, it involves the complex interdependencies between overall activity and the heterogeneity in each organization's operational portfolio.

Similarly, being active in the same world region does not provide enduring evidence of increased (or decreased) likelihood of co-clustering for two given terrorist groups. Notably, this statistical outcome posits the absence of geographical homophily mechanisms: there is no statistically significant difference in the probability of co-clustering for two pairs of groups, one being characterized by organizations plotting attacks in two distinct regions and another being characterized by spatially closer organizations.

Finally, even clearer evidence demonstrates that operational similarity is not driven by or correlated with organizations' ideologies. While the literature has posited that ideology influences terrorists' decision-making processes, our results argue that two groups acting with the same ideology have a probability of being clustered together which is not significantly different from the probability of two groups characterized by distinct ideologies being in the same cluster. Besides the insufficient amount of statistical significance associated with ideology as a covariate, it is worth noting that the direction of the coefficients seems at least to follow clear stable patterns: while in the first part of the period under consideration the (non-significant) coefficients were negative, from 2003 on, ideology estimates became positive, although in the last years they got closer again to zero.

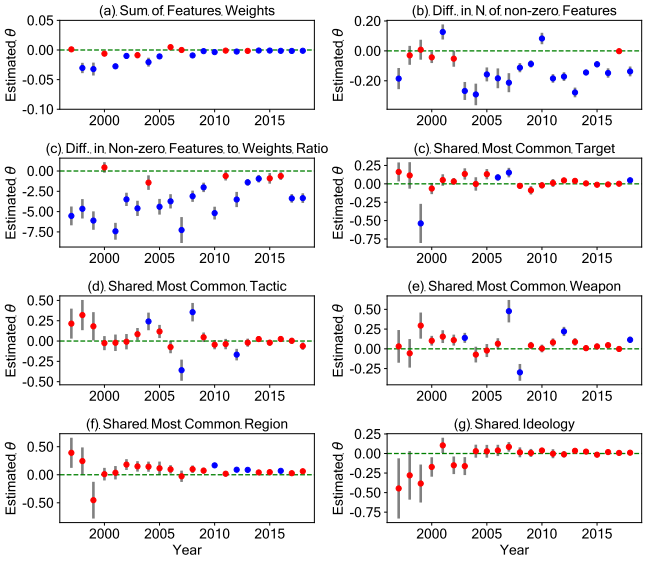

Fig. 4. Estimated coefficients for each covariate included in the analysis of drivers of co-clustering, with standard error bars. Blue dots are statistically significant at the 95% level (red are not). (a) "Sum of Features Weights" , capturing a group's overall activity, is a consistently significant predictor in determining the probability of being clustered together: the negative estimated θ suggest the higher the sum of features weights between two groups, the lower the probability they will be clustered together.(b) The difference in non-zero features, considered as a proxy for repertoire diversity, and particularly the absolute difference between two organizations is the other consistent driver of operational similarity. Results indicate that the more two groups are different in terms of repertoire diversity, the lower the chances of being clustered together. The difference in non-zero features to weights ratio (c) also explains co-clustering: the lower the difference in this joint measure of activity and diversity, the higher the likelihood of co-clustering.

Like the previous two subsections, all the results regarding the drivers of similarity are empirically corroborated by robustness models presented in the SI Appendix "Robustness: Drivers of Similarity" subsection.

Discussion and Conclusions

Little is known about patterns of similarity among organizations engaging in political violence. To address this research problem, we have here presented the results of a computational framework for detecting clusters of terrorist organizations that are similar in their operations. We considered groups that have plotted at least 50 attacks worldwide in the period 1997-2018 and gathered yearly clusters obtained from multi-modal networks that map terrorist behaviors in terms of their selection of tactics, targets, and weapons.

We highlighted that when coupling the relatively little variability in the number of clusters over the period 1997-2018 with the yearly growing number of active groups, a clear downward trend in the cluster to groups ratio is found, possibly indicating decreasing overall heterogeneity in terrorist operations globally and increasing cohesiveness.

Furthermore, we demonstrated that prior to 2002, year-to-year stability of co-clustering was very low, suggesting a relevant level of behavioral and operational variability for terrorist organizations involved. Conversely, stability increases after 2002, reaching considerably high levels after 2009, thus

corroborating the intuition that terrorist groups became more operationally consistent in recent years.

Finally, we have disentangled drivers of co-clustering, which maps operational similarity, finding that similarity is mainly driven by groups' yearly amount of activity, homophily in repertoire diversity and a measure of the two combined. The other tested measures, namely homophily in operational preferences, geographical homophily and ideological homophily revealed their non-significant role in driving co-clustering. With regards to geospatial dynamics, future research should explore whether finer-grained spatial resolutions provide different insights on geographical micro-patterns of terrorist behaviors. Concerning ideology, while extant work showed that sharing the same ideology drives inter-group alliances (19, 20), our analyses demonstrated that when organizations are primarily represented by their mere operations, ideology fails to hold its driving assortative force, as it does not explain operational similarity. All our results are robust, as analyses re-estimated on an enlarged sample of terrorist organizations demonstrate.

Beyond its empirical contribution to the study of terrorist behaviors, our work advances research developing computationally-oriented systems for counter-terrorism, an area of inquiry that has gained momentum in the last years (11, 41). With this regard, our approach may be useful to develop dynamic assessment tools for intelligence monitoring. Generally, risk assessment tools aim at protecting locations or targets (42) or preventing the radicalization of individuals (43). Nonetheless, adopting a complementary approach to scan behavioral changes in terrorist groups can be highly effective in enriching data-driven support for terrorism prevention. The computational efficiency and the scalability of our framework allow for the adaptation of our approach to larger samples, finer-grained geographical units and temporal windows. This flexibility offers a versatile tool that can facilitate the analysis of groups' behavioral trajectories, tailoring the context of analysis on the needs of practitioners and policy-makers. As political violence evolves and new terrorist actors emerge in the global scenario, detecting operational affinity among different organizations can offer critical insights for the design and deployment of counter-terrorism policies, anticipating possible trends and providing insights on which organizations should be prioritized in the fight against terrorist violence.

ACKNOWLEDGMENTS. We wish to thank Victor Asal, Bruce Desmarais, Maria Rita D'Orsogna, and the participants of the Trento Center for Social Research Methods seminar series for their insightful comments on this manuscript. This work was supported by the Department of Excellence initiative of the Italian Ministry of University and Research and in part by the Knight Foundation and the Office of Naval Research Grants N000141812106 and N000141812108. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Knight Foundation, Office of Naval Research or the U.S. government.

1. GH McCormick, Terrorist Decision Making. *Annu. Rev. Polit. Sci.* **6**, 473–507 (2003).
2. JN Shapiro, Terrorist Decision-Making: Insights from Economics and Political Science. *Perspectives on Terror.* **6**, 5–20 (2012) Publisher: Terrorism Research Institute.
3. CJM Drake, Ideology in *Terrorists' Target Selection*, ed. CJM Drake. (Palgrave Macmillan UK, London), pp. 16–34 (1998).
4. VH Asal, et al., The Softest of Targets: A Study on Terrorist Target Selection. *J. Appl. Secur. Res.* **4**, 258–278 (2009) Publisher: Routledge _eprint: https://doi.org/10.1080/19361610902929990.
5. R Ahmed, Terrorist Ideologies and Target Selection. *J. Appl. Secur. Res.* **13**, 376–390 (2018) Publisher: Routledge _eprint: https://doi.org/10.1080/19361610.2018.1463140.
6. BA Jackson, Technology Acquisition by Terrorist Groups: Threat Assessment Informed by Lessons from Private Sector Technology Adoption. *Stud. Confl. & Terror.* **24**, 183–213 (2001).
7. A Dolnik, *Understanding Terrorist Innovation: Technology, Tactics and Global Trends.* (Routledge), (2007).
8. SM Polo, KS Gleditsch, Twisting arms and sending messages: Terrorist tactics in civil war. *J. Peace Res.* **53**, 815–829 (2016).
9. A Clauset, KS Gleditsch, The Developmental Dynamics of Terrorist Organizations. *PLoS ONE* **7**, e48633 (2012).
10. C Santifort, T Sandler, PT Brandt, Terrorist attack and target diversity: Changepoints and their drivers. *J. Peace Res.* **50**, 75–90 (2013).
11. Y Yang, AR Pah, B Uzzi, Quantifying the future lethality of terror organizations. *Proc. Natl. Acad. Sci.* **116**, 21463–21468 (2019).
12. M Lubrano, Navigating Terrorist Innovation: A Proposal for a Conceptual Framework on How Terrorists Innovate. *Terror. Polit. Violence* **0**, 1–16 (2021) Publisher: Routledge _eprint: https://doi.org/10.1080/09546553.2021.1903440.
13. M Crenshaw, Innovation: Decision Points in the Trajectory of Terrorism. (Harvard University), (2001).
14. A Perliger, A Pedahzur, Social Network Analysis in the Study of Terrorism and Political Violence. *PS: Polit. Sci. Polit.* **44**, 45–50 (2011) Publisher: [American Political Science Association, Cambridge University Press].
15. M Bouchard, ed., *Social Networks, Terrorism and Counter-terrorism.* (Routledge, London), 1 edition edition, (2017).
16. V Krebs, Uncloaking Terrorist Networks. *First Monday* (2002).
17. RM Medina, Social Network Analysis: A case study of the Islamist terrorist network. *Secur. J.* **27**, 97–121 (2014).
18. V Asal, RK Rethemeyer, Researching Terrorist Networks. *J. Secur. Educ.* **1**, 65–74 (2006) Publisher: Routledge _eprint: https://doi.org/10.1300/J460v01n04_06.
19. VH Asal, HH Park, RK Rethemeyer, G Ackerman, With Friends Like These ... Why Terrorist Organizations Ally. *Int. Public Manag. J.* **19**, 1–30 (2016) Publisher: Routledge _eprint: https://doi.org/10.1080/10967494.2015.1027431.
20. BJ Phillips, Terrorist Group Rivalries and Alliances: Testing Competing Explanations. *Stud. Confl. & Terror.* **42**, 997–1019 (2019) Publisher: Routledge _eprint: https://doi.org/10.1080/1057610X.2018.1431365.
21. BA Desmarais, SJ Cranmer, Forecasting the locational dynamics of transnational terrorism: a network analytic approach. *Secur. Informatics* **2**, 8 (2013).
22. GM Campedelli, I Cruickshank, KM Carley, A complex networks approach to find latent clusters of terrorist groups. *Appl. Netw. Sci.* **4**, 1–22 (2019).
23. GM Campedelli, M Bartulovic, KM Carley, Learning future terrorist targets through temporal meta-graphs. *Sci. Reports* **11**, 8533 (2021).
24. G LaFree, L Dugan, Introducing the Global Terrorism Database. *Terror. Polit. Violence* **19**, 181–204 (2007).
25. V Asal, RK Rethemeyer, I Anderson, Big Allied and Dangerous (BAAD) Database 1 - Lethality Data, 1998-2005. (2011) Publisher: Harvard Dataverse type: dataset.
26. D Hou, K Gaibulloev, T Sandler, Introducing Extended Data on Terrorist Groups (EDTG), 1970 to 2016. *J. Confl. Resolut.* **64**, 199–225 (2020).
27. TB Group, TRAC - Terrorism Research & Analysis Consortium Platform (2021).
28. KM Carley, ORA: A Toolkit for Dynamic Network Analysis and Visualization in *Encyclopedia of Social Network Analysis and Mining*, eds. R Alhajj, J Rokne. (Springer New York, New York, NY), pp. 1–10 (2017).
29. IJ Cruickshank, Ph.D. Dissertation (Institute for Software Research, School of Computer Science - Carnegie Mellon University) (2020).
30. A Strehl, J Ghosh, Cluster ensembles — a knowledge reuse framework for combining multiple partitions. *The J. Mach. Learn. Res.* **3**, 583–617 (2003).
31. S Wasserman, P Pattison, Logit models and logistic regressions for social networks: I. An introduction to Markov graphs and p*. *Psychometrika* **61**, 401–425 (1996) Place: Germany Publisher: Springer.
32. PW Holland, S Leinhardt, An Exponential Family of Probability Distributions for Directed Graphs. *J. Am. Stat. Assoc.* **76**, 33–50 (1981) Publisher: [American Statistical Association, Taylor & Francis, Ltd.].
33. SE Fienberg, SS Wasserman, Categorical Data Analysis of Single Sociometric Relations. *Sociol. Methodol.* **12**, 156–192 (1981) Publisher: [American Sociological Association, Wiley, Sage Publications, Inc.].
34. D Strauss, M Ikeda, Pseudolikelihood Estimation for Social Networks. *J. Am. Stat. Assoc.* **85**, 204–212 (1990) Publisher: Taylor & Francis _eprint: https://www.tandfonline.com/doi/pdf/10.1080/01621459.1990.10475327.
35. SJ Cranmer, BA Desmarais, Inferential Network Analysis with Exponential Random Graph Models. *Polit. Analysis* **19**, 66–86 (2011) Publisher: [Oxford University Press, Society for Political Methodology].
36. SJ Cranmer, BA Desmarais, EJ Menninga, Complex Dependencies in the Alliance Network. *Confl. Manag. Peace Sci.* **29**, 279–313 (2012).
37. SW Duxbury, DL Haynie, The Network Structure of Opioid Distribution on a Darknet Cryptomarket. *J. Quant. Criminol.* **34**, 921–941 (2018).
38. S Hanneke, W Fu, EP Xing, Discrete temporal models of social networks. *Electron. J. Stat.* **4** (2010).
39. BA Desmarais, SJ Cranmer, Statistical mechanics of networks: Estimation and uncertainty. *Phys. A: Stat. Mech. its Appl.* **391**, 1865–1876 (2012) Publisher: Elsevier.
40. PN Krivitsky, MS Handcock, A Separable Model for Dynamic Networks. *J. Royal Stat. Soc. Ser. B, Stat. Methodol.* **76**, 29–46 (2014).
41. YL Chuang, N Ben-Asher, MR D'Orsogna, Local alliances and rivalries shape near-repeat terror activity of al-Qaeda, ISIS, and insurgents. *Proc. Natl. Acad. Sci.* **116**, 20898–20903 (2019).
42. W Guo, K Gleditsch, A Wilson, Retool AI to forecast and limit wars. *Nature* **562**, 331–333 (2018) Number: 7727 Publisher: Nature Publishing Group.
43. J Monahan, The individual risk assessment of terrorism. *Psychol. Public Policy, Law* **18**,

589 167–205 (2012).