Contents lists available at ScienceDirect

Heliyon

journal homepage: www.cell.com/heliyon

An integrated deep-learning and multi-level framework for understanding the behavior of terrorist groups

Dong Jiang[a,b,1], Jiajie Wu[a,b,1], Fangyu Ding[a,b,1], Tobias Ide[c], Jürgen Scheffran[d], David Helman[e,f], Shize Zhang[g], Yushu Qian[a], Jingying Fu[a,b], Shuai Chen[a,b], Xiaolan Xie[a,b], Tian Ma[a,b], Mengmeng Hao[a,b,*], Quansheng Ge[a,**]

[a] *Institute of Geographic Sciences and Natural Resources Research, Chinese Academy of Sciences, Beijing, 100101, China*
[b] *College of Resources and Environment, University of Chinese Academy of Sciences, Beijing, 100049, China*
[c] *Centre for Biosecurity and One Health, Harry Butler Institute, Murdoch University, Murdoch, 6150, Perth, Australia*
[d] *Institute of Geography, Center for Earth System Research and Sustainability, University of Hamburg, Hamburg, 20144, Germany*
[e] *Institute of Environmental Sciences, Department of Soil and Water Sciences, The Robert H. Smith Faculty of Agriculture, Food & Environment, The Hebrew University of Jerusalem, Rehovot, 7610001, Israel*
[f] *Advanced School for Environmental Studies, The Hebrew University of Jerusalem, Jerusalem, Israel*
[g] *Computer Network Information Center, Chinese Academy of Sciences, Beijing, 100190, China*

ARTICLE INFO

Keywords:
Terrorism
Deep learning
Terrorist group
Terrorist network

ABSTRACT

Human security is threatened by terrorism in the 21st century. A rapidly growing field of study aims to understand terrorist attack patterns for counter-terrorism policies. Existing research aimed at predicting terrorism from a single perspective, typically employing only background contextual information or past attacks of terrorist groups, has reached its limits. Here, we propose an integrated deep-learning framework that incorporates the background context of past attacked locations, social networks, and past actions of individual terrorist groups to discover the behavior patterns of terrorist groups. The results show that our framework outperforms the conventional base model at different spatio-temporal resolutions. Further, our model can project future targets of active terrorist groups to identify high-risk areas and offer other attack-related information in sequence for a specific terrorist group. Our findings highlight that the combination of a deep-learning approach and multi-scalar data can provide groundbreaking insights into terrorism and other organized violent crimes.

1. Introduction

In recent decades, terrorist attacks have continuously struck the global economy and political order. The 9/11 attacks also heightened global attention and vigilance towards terrorist activities. Among various definitions of terrorism, the most prominent one is the Global Terrorism Database (GTD) dataset, which defines terrorism as, “the threatened or actual use of illegal force and violence by a non-state actor to attain a political, economic, religious, or social goal through fear, coercion, or intimidation [1].” According to

* Corresponding author. Institute of Geographic Sciences and Natural Resources Research, Chinese Academy of Sciences, Beijing, 100101, China.
** Corresponding author.
E-mail addresses: haomm@igsnrr.ac.cn (M. Hao), geqs@igsnrr.ac.cn (Q. Ge).

[1] These authors contribute equally.

https://doi.org/10.1016/j.heliyon.2023.e18895
Received 8 December 2022; Received in revised form 27 July 2023; Accepted 2 August 2023
Available online 6 August 2023

this definition, terror attacks launched by hundreds of terrorist groups worldwide still managed to deprive 40,000 lives on average per year [2] and cause a 47.5-billion dollar economic loss since 2001 [3]. To reduce the violence and associated losses caused by terrorism, countries and peoples around the world have united to mitigate the threat of terrorism and promote peaceful and inclusive societies [4].

How do acts of terrorism evolve over time and space? Are they random episodes of violence perpetrated by terrorist groups, or do they follow predictable patterns that can be discerned? In light of the widespread occurrence and destructive impact of terrorist attacks, finding answers to these questions is of critical importance. A terrorist group can be understood as a social system with a unified group of fanatics committed to extremist aims by inflicting civilian and economic damage on particular targets [5]. In recent times, with the internationalization, alliance formation, and networking of terrorist groups, social systems have evolved into increasingly complex sociotechnical systems. The behaviors of the groups are shaped by both their interactional environment and organizational mechanisms, resulting in a continuously evolving phenomenon for an active terrorist group [6]. By gaining a deeper understanding of the spatial and temporal dynamics underlying terrorist groups, we can develop proactive measures and policies aimed at preventing or mitigating the impact of these humanitarian disasters. Academic literature frequently describes terrorism research in terms of three scales: macro, meso, and micro [7–11]. However, these scales are not rigidly defined categories in the study of terrorism, as they can overlap and be interrelated. The focus and scope of research into terrorism can vary depending on the specific research goals and questions at hand. The micro scale typically focuses on individuals and their contextual factors. These factors may include the individual's characteristics, behavior patterns, and motivations, as well as the influence of relevant organizations and social environments on their behavior [12]. The meso scale typically focuses on terrorism's organizational structure and operational methods. This research may include studies of cooperation and competition among organizations, the status of terrorist organizations within the social and political environment, and the proliferation and evolution of their activities and branches [13,14]. The macro scale typically focuses on terrorism as a global social issue, exploring factors such as political, economic, cultural, and geographic influences on a global level [15,16].

The majority of published studies use macro- and micro-perspectives [17]. Terrorism is geographically and temporally concentrated, with a higher frequency in specific hotspot areas, and it becomes increasingly stable over time [18–20]. Thus, macro-level studies normally identify contributing factors in the background context of certain geographical units such as countries, cities, or grid cells that render them more likely to experience terrorist attacks [21–24]. One of the recent works done by Python et al. [25] used data on geography, politics, and socioeconomics from grid cells at 0.5° spatial resolution to predict non-state terrorism worldwide a week ahead. On the other hand, the underlying organization and operational methods of terrorist groups involve a multitude of factors, including objectives, strategies, and ideologies [26–28]. Their activities exhibit regular patterns such as periodicity and propensity [29,30], and similar behavioral patterns exist across different organizations [31–33]. Therefore, micro-level research focuses on historical actions that were individually initiated by a terrorist group, which is a sequence comprising a series of locations it previously attacked or the means it used in the attacks, such as a suicide bombing or hijacking, reflecting its preference towards destinations or the tactics. Models and frameworks relevant to such predictions derived from past attack records include sequence learning [34], situational reasoning [35], game-theoretic frameworks [36], and neural networks [37–40], among others. Applications of such research usually provide more specific predictions of possible attacks, for example, in which particular place a specific terrorist group might attack next time. In the case of an attention-based Long Short Term Memory (LSTM) model proposed by Liu et al. [39], the goal was to predict the next province or state a terrorist group may strike at a specific time using the spatio-temporal information from the past attacks. Some studies made further efforts to pin down the potential targets with more detailed information. For instance, research conducted by Campedelli et al. [40] attempted to find out the most likely target types of attacks in the next two days in Afghanistan and Iraq by learning the similarities and dependencies among temporally close attacks. Their study involved using meta-graphs to map the links between three aspects: employed weapons, deployed tactics, and chosen targets of terrorist groups. Saidi et al. developed a hybrid deep learning model based on Convolutional Neural Networks and Long Short-Term Memory models to predict the types and success rates of terrorist attacks, which demonstrated a correlation between the occurrence of attacks and the type of weapons used [41]. The third and least frequent perspective focuses on the meso-scale, which requires incorporating social relationships among terrorist groups. Although many have endorsed the theory of the terrorist networks being effective in prediction, given that terrorist groups grow more transnational, allied, and networked over time [42,43], limited predictions have been made from this perspective. These deficits are due to the finite resources of established mature networks that undisputedly capture the very subtle and implicit connections among these groups. A few studies have constructed the networks themselves with their own interpretation of the relationships among the groups, and those founded on the idea of one group relating to the others who share similar goals or take actions in a similar pattern are normally considered better predictors [44–48]. Such network-building processes provide meso-scale forecasting with more theoretically supported terrorist networks.

In general, the literature review has provided valuable insights into the effective use of different models for predicting the behavior of terrorist organizations. By extracting useful features, machine learning and pattern recognition methods can be employed to accurately forecast future activities [49,50]. As specific as they intended to predict the high-risk targets or the next moves of terrorist groups, their assistance in designing countermeasures against future attacks is so far limited [51–54]. Their predictions of targets made within a large range of areas with little information on tactics and weapons a terrorist group might employ are not informative enough for the authorities to take the required precautions, organize defensive measures, and deploy forces against such potential attacks. The reason lies in the complex mechanism of terrorism, which encompasses multiple political, cultural, economic, and social dimensions, as well as individual psychological and ideological aspects [55]. Moreover, terrorist groups constantly evolve their strategies and targets efficiently, making their attack patterns more elusive to decipher, and making predictions based on longer time series difficult. Such circumstances demand more comprehensive, accurate, and effective terrorism research for the sake of devising tailor-made strategies against potential strikes [56,57]. Thus, it is a key trend to uncover the precise location and timing a particular group may strike and what would be his strategy, tactics, and weaponry used. Additionally, integrating multiple datasets from different sources and modalities has become one of the hottest topics in the field of computer research. For instance, multimodal fusion using audio, video, and text modalities and deep learning techniques have significantly improved the predictive performance of detecting attack behaviors in surveillance [58].

Here we propose an integrated framework model that incorporates all three perspectives, including factors at macro-, meso-, and micro-scales, to discover the patterns of terrorist group behaviors. As shown in Fig. 1, in our framework, the actions of a terrorist group in the next session are impacted by the confluence of all three types of elements: the covariates of grid cells, the historical behaviors of individual terrorist groups, and the social network of these groups in the previous session. Among them, we constructed four social networks, namely GTD-Net, BAAD-Net, EDTG-Net, and Pattern-Net, with reference to previous research [46–48,59–61]. Our approach utilizes a recurrent neural network (RNN) [62] to model the historical behaviors of a terrorist organization within a session, and extract their dynamic individual preferences. Secondly, our model distinguishes between short-term preference models and long-term preference models of friends based on the social network, and then determines the influence of each friend using a dynamic graph attention network (DGAN) [63]. Finally, our model employs a multi-layer perceptron (MLP) to handle the covariates of candidate prediction targets, and extract their dynamic contextual risks. Based on the above construction, our framework offers predictions of the locations where terrorist groups are likely to attack in a specific period and the attack action sequence of certain groups, including attack locations and other pertinent information such as victim nationality, weaponry type, type of attack, and target. We tested our framework at multiple spatio-temporal resolutions and with different terrorist networks. The results show that our framework excels at predicting terrorist group actions compared with the baseline model that refers to the Embedding and MLP paradigms shared in most popular model structures [64]. Moreover, we also display the model's accuracy when the predictor is a two-by-two combination of location and each of the four terror attributes mentioned above. Among them, the performance of the model combining location and victim nationality shows a little drop in accuracy compared to the location-only model, and the models' accuracy for the other three attributes drops dramatically. Furthermore, we showcase the predictive results on a global scale and focus on a specific group to detailedly demonstrate the predictive power of our model. Overall, our research unites different perspectives and deep-learning techniques to understand terrorist group behaviors, which will assist in developing concrete proposals and practical tools for authorities to design counter-terrorism policies.

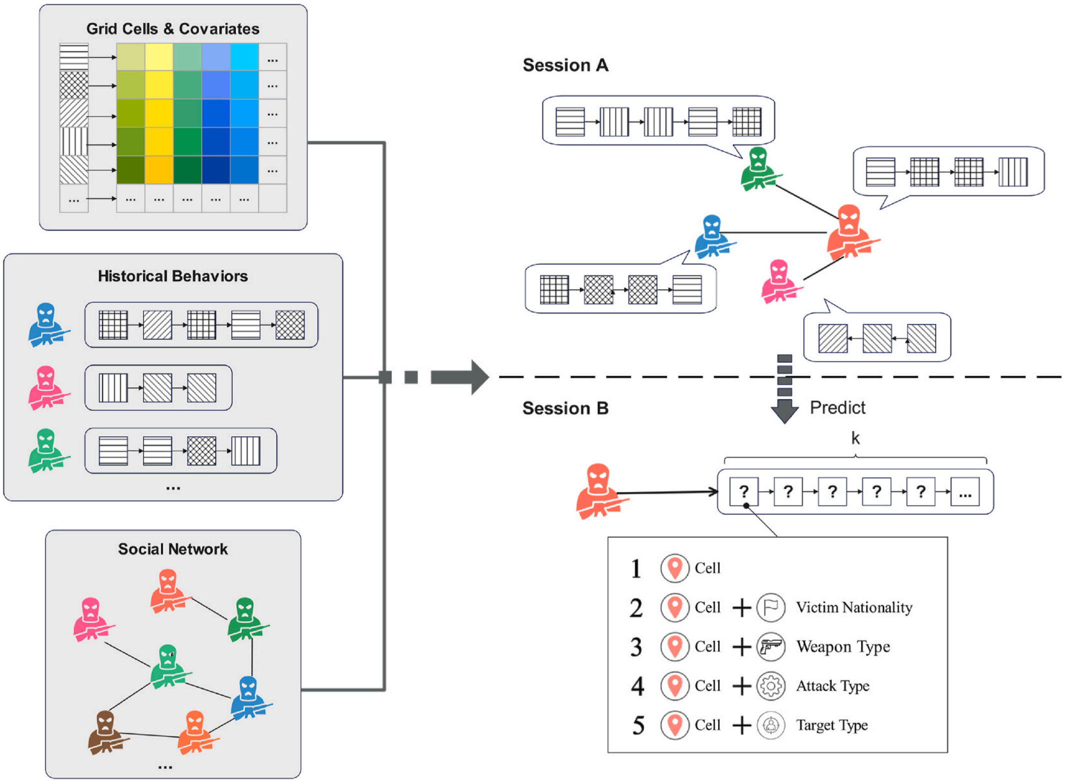


Fig. 1. Schematic diagram of terrorist organization behavior prediction.

2. Materials and methods

2.1. Materials

Actions of Individual Group. Gathering information on past attacks is what we reckon to be the prerequisite for capturing the dynamically changing individual behavior of each terrorist group. Considering the requirement for data coverage, we use GTD in this study as the resource of historical terrorist attacks [65]. We restrict our analysis to global terrorist attacks from 2002 to 2019, given that the 9/11 2001 attack was considered a major breakpoint in global terrorism [66]. Each terrorist group with attack records in this dataset was assigned a GroupID as an identifier that brands their past attacks by combining the TimeID (time window of the attack) and CellID (place of an attack). In recommendation systems, a session refers to a series of user interactions that occur within a certain period of time [67]. In our study, this can be exemplified by a terrorist organization launching a series of attacks within a specific time window. We combined GroupID and TimeID into session identifiers (SessionID) and made predictions on a session basis. Thus, the records of attacks executed by a terrorist group in a TimeID are generated as one terrorist attack sequence by SessionID. An example of such a sequence of terrorist attacks by a terrorist group “g” is presented in Fig. 2.

To form a new set of CellIDs with elements, including the victim nationality, weapon type, attack type, and target type attached to each grid cell, we encoded such categorical information acquired from GTD. Eventually, an action sequence of a terrorist organization over a time period is formed according to the following rules.

a) In a time period, the behavioral sequence of a terrorist group consists of a series of CellIDs, arranged in ascending order according to the time of occurrence;
b) With the same time of occurrence, CellIDs are arranged in descending order according to the number of casualties.

In a time period, if multiple attacks happened in the same grid cell on the same day, they will be merged into one, and the casualties are the total of the casualties of these multiple records.

A social network of terrorist groups. As mentioned earlier, we believe that an organization might refer to the choices of its terrorism community in the social network when picking targets. It could aim at either the recent targets appealing to its fellow groups or the time-insensitive targets that have drawn considerable attention in the community. Once we discover the networks formed among these groups, we can procure the short-term interests of organizations related to given groups by studying their recent attacks while obtaining the long-term interests of their community in social networks through average historical target choices.

Typically, a terrorist group is connected to other groups by formally claiming alliances or engaging in rivalry. Informal yet observable links can be discovered among these organizations. Terrorist networks established previously, such as BAAD global network, tend to focus on large and intimidating organizations without paying much attention to the seemingly less threatening ones. Due to the lack of a more inclusive terrorist network, we constructed our own networks of terrorist groups and named them based on different data sources and approaches, as explained below. We then run our model with these networks to make comparisons between model performance by different networks [47,48]. We constructed GTD-Net with the attacks recorded in GTD where more than one party is an active participant in the attack [46]. Those who have taken part in the same action were therefore considered correlated with each other. BAAD-Net provides a global network of terrorist groups built with the latest records from BAAD, derived from

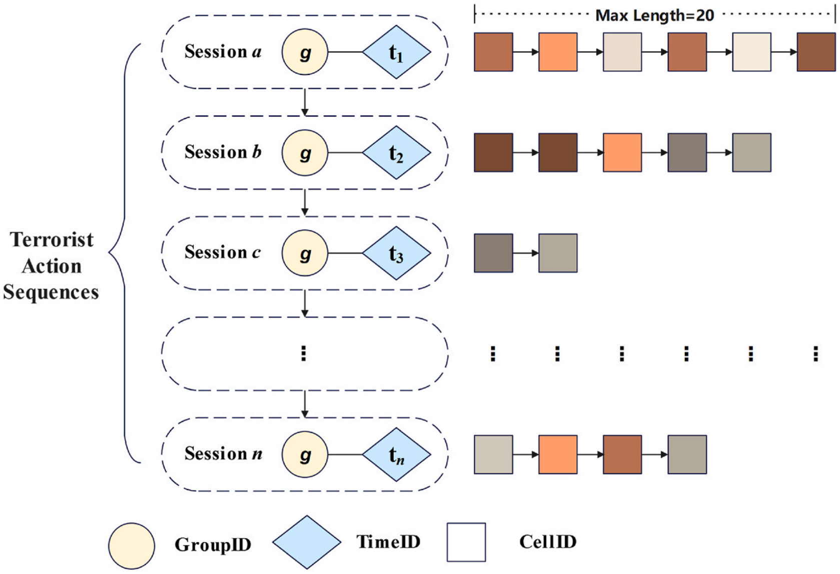


Fig. 2. The example of sequences of terrorist attacks by a terrorist group.

terrorism-related expertise. Here, we created two additional networks: (1) The EDTG-Net by using cosine similarity to measure the similarity between all pairs of terrorist groups with information on the base origin, ideology, and main target of the groups recorded in Extended Data on Terrorist Groups (EDTG) [61]; and (2) The Pattern-Net through overlap coefficient that measures the similarity between two groups regarding the strategy and target of their attack, derived from GTD dataset using three-way decisions theory that can determine boundary regions, which represent the actions of one group that can be associated with another group [47]. In addition, when constructing EDTG-net and Pattern-Net, we use agglomerative clustering and silhouette coefficient to determine the optimal number of group clusters. Descriptive statistics of relationships in all four networks (GTD-Net, BAAD-Net, and the two networks we built – EDTG-Net and Pattern-Net) are shown in Table 1. Table 1 contains the number of terrorist organizations in each network, the number of records in GTD related to these organizations, the average number of records per terrorist organization, the number of network links, and the average number of links per terrorist organization.

Background context of strike locations. Local environment and socioeconomic attributes often explain the context of selecting a given site for attack by terrorist groups. To capture the background context of terrorist attacks, we divided the world up into uniformly-sized grids of a given size, referring to PRIO-GRID [68], for example, 1 × 1 decimal degree spatial resolution. Each grid cell is distinguished from the rest by a given CellID. Features within each of the included grids associated with the possibility of attack occurrence were extracted from 23 geographic and socioeconomic elements that are considered high relative to terrorist attacks after we draw on prior research [25] (Table 2).

We aimed in this study to examine the variation in performance of our model over different spatial and temporal scales. Therefore, the model was run at multiple spatial (1 × 1, 0.5 × 0.5, and 0.1 × 0.1 decimal degrees) and temporal (1 week, two weeks, one month, and two months) resolutions. Like the spatially divided grids, each session was assigned a TimeID at the abovementioned given temporal scale.

2.2. Methods

The emergence of AlphaGo further demonstrated the ability of deep neural networks to handle complex problems [69], so we recognize the potential of deep learning techniques to be applied for terrorism prediction [70]. Our model employs deep learning techniques as technical support to represent each factor's dynamic influence on the attacks. As shown in Fig. 3, the flow chart of our proposed model, the first step is inputting all necessary data required for prediction, including the sequenced attack records of terrorist groups, the organizations associated with given groups in the terrorist network, and their recent attacks in sequence, and the geographic and socioeconomic elements of past target locations (grid cells).

Problem Definition. Table 3 presents the primary notations used in our study, followed by the essential definitions of factors for predicting the next actions of a given terrorist group and introducing the details of the base model and our framework.

The object of the prediction. The object of a terrorist attack by terrorist group g is the grid cell where the attack was executed or the grid cell combined with other attack-related attributes (target type or attack type), which is defined as: $c^{g}_{t,p}$, meaning the p-th object attacked by terrorist group g in the t-th session.

Terrorist action sequences. During the t-th session, $\overrightarrow{S}^{g}_{t}$ is formed of a set of objects, $\{c^{g}_{t,1}, c^{g}_{t,2}, \ldots, c^{g}_{t,N_{g,t}}\}$, where $\mathrm{N}_{\mathrm{g,t}}$ is the number of objects attacked by terrorist group g in this session. The past actions of terrorist group g at time step T consist of attacks during a series of sessions, $C^{g}_{T} = \{\overrightarrow{S}^{g}_{1}, \overrightarrow{S}^{g}_{2}, \ldots, \overrightarrow{S}^{g}_{T}\}$.

Social network among terrorist groups. First, we encode the terrorist network in a graph, with nodes representing groups (i.e. target users and their friends) and edges representing the relationship among the groups, defined as: $TN = (G,E)$, where E is the set of social links among terrorist groups. $|N(g)|$ is the number of groups associated with a particular group, and they together sum to $|N(g)| + 1$ nodes. Our framework allows us to study the impact on each group from their higher-order "friends". The 0-order node is the group itself, and the nodes directly linked with it belong to the 1-order neighbors in the graph. By that analogy, the 2-order neighbors are groups linked to the 1-order groups that are directly associated with the 0-order node group.

Background context of grid cells. The objects used in the model are the spots that have been subjected to terrorist attacks, and the attack-related context elements we use here are extracted only from the grid cells containing these objects. The data sources of all the elements used as the indicator of the background context of attacked locations in the modeling process are listed in Table S3.

2.2.1. Base model

Through the embedding layer, large-scale sparse features are transformed into low-dimensional dense vectors. We define M as the size of sparse features and d_{model} as the embedding size. The sparse features are therefore expressed mathematically by $E \in \mathbb{R}^{M\times d_{model}}$. With the embedding layer, GroupIDs can be represented by $X^{G} \in \mathbb{R}^{d_{model}}$, generating a lookup table that stores embeddings of IDs of all

Table 1
Descriptive statistics of four indices of the networks among terrorist groups.

Network	Terrorist groups	Records	Avg. Records/terrorist group	Links	Avg. Links/terrorist group
GTD-Net	709	58060	81.89	1882	2.65
BAAD-Net	112	42290	377.59	440	3.92
EDTG-Net	659	47833	72.58	17088	25.93
Pattern-Net	961	61422	63.91	8812	9.17

Table 2
Elements of background context of attacked locations used in the overall framework.

Feature name	Time lag	Type
longitude	static	geographical
latitude		
altitude		
altitude standard deviation		
mountain coverage		
road density		socioeconomic
accessibility to cities		
distance to nearest capital city		geopolitical
distance to nearest national border		
whether drug cultivation exists		socioeconomic
whether onshore petroleum deposits exist		
whether gold deposits exist		
whether gems&diamonds deposits exist		
satellite night lights	year lag 1	
satellite night light changes		

population density	2000 for 2002–2005;
	2005 for 2006–2010;
	2010 for 2011–2015;
	2015 for 2016–2019	

per capita GDP		
human development index		
number of conflict events	TimeID lag 1	geopolitical
number of terrorist attacks		
number of terrorist attacks	TimeID lag 2	
number of terrorist attacks	TimeID lag 3	
number of terrorist attacks	TimeID lag 4	

terrorist groups. Similarly, CellIDs can be represented by $X^C \in \mathbb{R}^{d_{model}}$, in order to perform a direct lookup on CellIDs to obtain their corresponding object embeddings.

In our study, the dense layer is a fully-connected layer or a combination of multiple fully-connected layers (called multiple layer perceptron, MLP). The Embedding&MLP paradigm is used as the base model by most popular model structures [64]. In our base model, the embeddings of terrorist group action sequences and context elements of objects are fed into MLP with an activation function like rectified linear units (ReLU) [71] and then concatenated together. The attack preference of individual terrorist group g in the baseline is defined as: $h_n = ReLU(W_1[c^g_{T+1,n}, h_{n-1}])$.

The representation of background context is the same as in our framework, which is described below.

2.2.2. Our framework

Dynamic Individual Interests. In this research, our challenges require algorithms to process time-series data or, more broadly, sequences. Recurrent Neural Network (RNN) is one type of algorithm that meets our standards. One of the advantages of RNN is its possibility of connecting earlier knowledge to the current activity. Long Short Term Memory networks (LSTM) [72] are a special kind of RNN that has been proposed to address the well-known problem of vanishing (or exploding) gradients in traditional RNN. In this research, we employ an RNN with LSTM units. We utilize RNN to model the actions of a terrorist group in a session in order to capture their rapidly shifting attack preferences. For each terrorist group g, the representation of a session is: $\overrightarrow{S}^g_{T+1} = \{c^g_{T+1,1}, c^g_{T+1,2}, \ldots, c^g_{T+1,n}\}$.

We next merge the representations of all previous tokens with the most recent token in a recursive manner, i.e., $h_n = f(c^g_{T+1,n}, h_{n-1})$, where h_n is the attack behavior of terrorist group g and $f(.,.)$ is a nonlinear function that combines both sets of information. As a combination function, the LSTM unit mentioned above includes:

$$x_n = \sigma\left(W_x\left[h_{n-1}, c^g_{T+1,n}\right] + b_x\right) \tag{1}$$

$$f_n = \sigma\left(W_f\left[h_{n-1}, c^g_{T+1,n}\right] + b_f\right) \tag{2}$$

$$o_n = \sigma\left(W_o\left[h_{n-1}, c^g_{T+1,n}\right] + b_o\right) \tag{3}$$

$$\widetilde{d}_n = tanh\left(W_d\left[h_{n-1}, c^g_{T+1,n}\right] + b_d\right) \tag{4}$$

$$d_n = f_n \odot d_{n-1} + x_n \odot \widetilde{d}_n \tag{5}$$

$$h_n = o_n \odot tanh(d_n) \tag{6}$$

where σ is the sigmoid function: $\sigma(x) = (1 + \exp(-x))^{-1}$.

Social Influences. For the session to make a prediction, the short-term preference of group k is represented by the final output of the RNN: $s^s_k = f(c^k_{T,N_{k,T}}, r_{N_{k,T-1}})$. Long-term preference, though insensitive to present activities, is influenced by the community of the

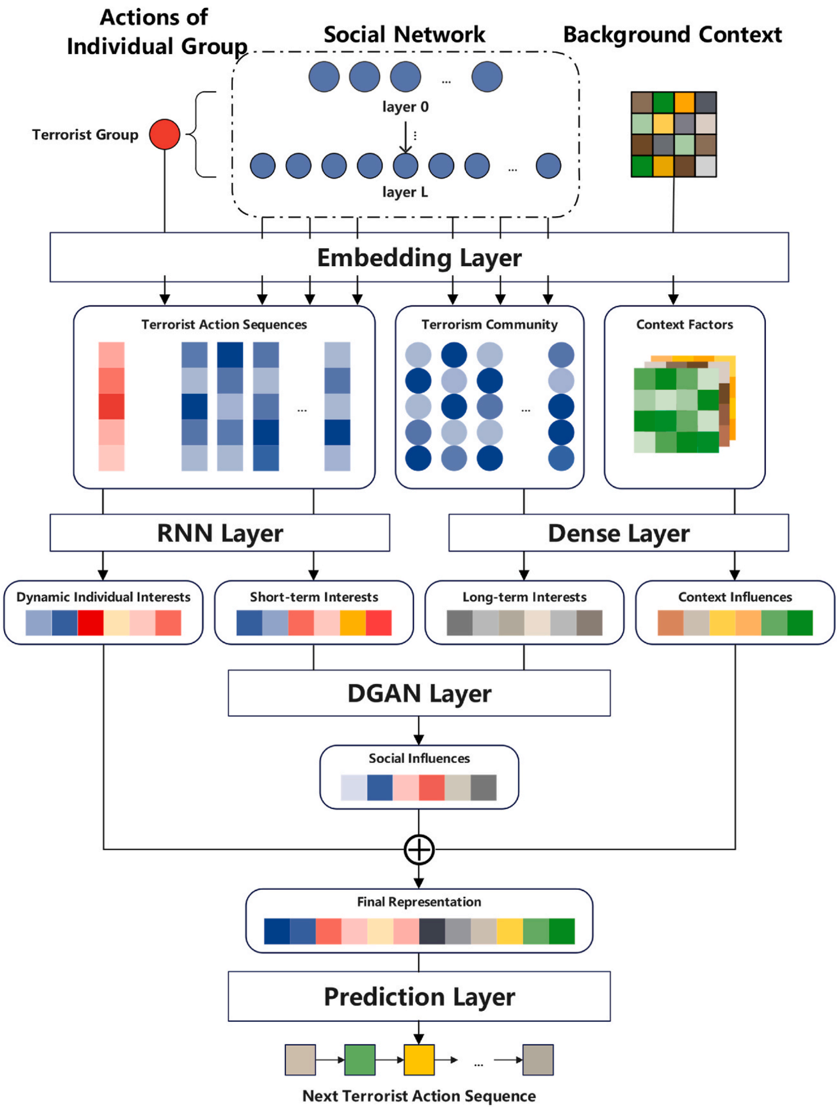


Fig. 3. The overview architecture of the proposed framework model.

Table 3
Primary notations used in the study.

Symbol	Description
g, G	A terrorist group and the set of all terrorist groups
c, C	The object of the prediction and the set of all objects
T	Time step
X_t	Context elements of grid cells in the t-th session
W_*	Transformation matrix (*:1, 2, 3, ...)
b_*	Constant term (*:1, 2, 3, ...)

target group (which consists of all linked groups in multiple orders). Therefore it is represented as: $s_k^l = W_g[k,:]$, where the long-term preference s_k^l of group k is the k-th row of the group embedding matrix W_g. In the next step, we concatenate both short-term and long-term interests using a nonlinear transformation: $s_k = ReLU(W_2[s_k^s; s_k^l])$, where $ReLU(x) = max(0, x)$ is a nonlinear activation function.

The attention mechanism [73] was often used to improve the performance of the encoder-decoder model for machine translation. It allows the decoder to utilize the most relevant parts of the input sequence flexibly through a weighted combination of all encoded input vectors, with the most relevant vectors receiving the highest weights. Different from the graph convolutional network [74] (the weights of different neighbors are fixed from the normalized Laplace matrix), the graph attention network (GAN) [75] achieves the adaptive assignment of different neighbor weights by performing the aggregation operation on the neighbor nodes through the attention mechanism, which greatly improves the expressiveness of the graph neural network model. On this basis, DGAN [63] employs a dynamic graph in which node features alter over time and node attention shifts in tandem with the current context. In the social network of terrorist groups, we take both the short-term and long-term preferences of the associated groups into account. The short-term interests are extracted from the recently-attacked cells in sequence in their latest sessions. And the long-term interests are modeled by individual embedding, representing the average preference of a cluster of terrorist groups. In order to avoid treating all the associated groups equally, we use a DGAN layer to model context-dependent network influences.

The individual input representation h_n of a particular group g is expressed by $h_g^{(0)}$ and the representation of nodes directly linked to this group is $h_g^{(1)}$. For a neighbor k, s_k is the matching node feature kept unvaried during time step $T+1$. In short, the representations of node g and its neighbors, respectively, are: $h_g^{(0)} = h_n$ and $\{h_k^{(0)} = s_k, k \in N(g)\}$. We determine the similarity between the representation $h_g^{(l)}$ of one group node and all of its related groups' representations $h_k^{(l)}$ as:

$$\alpha_{gk}^{(l)} = \frac{exp\left(f\left(h_g^{(l)}, h_k^{(l)}\right)\right)}{\sum_{j \varepsilon N(g) \cup \{g\}} exp\left(f\left(h_g^{(l)}, h_j^{(l)}\right)\right)} \tag{7}$$

where $h_g^{(l)}$ represents the l-order neighbors of node/group g and $f(h_g^{(l)}, h_k^{(l)}) = {h_g^{(l)}}^T h_k^{(l)}$ defines the similarity function between two factors. Further, conditioned on the current context, $h_g^{(l)}$, $\alpha_{gk}^{(l)}$ is the weight of influence from related group k on group g. We also provide a self-connection edge to retain a group's revealed preference $\alpha_{gk}^{(l)}$. The weights are offered to combine the features: $\widetilde{h}_g^{(l)} = \sum\limits_{k \varepsilon N(g) \cup \{g\}} \alpha_{gk}^{(l)} h_k^{(l)}$, where $\widetilde{h}_g^{(l)}$ mix the interests of the l-order groups relating to group g, using a nonlinear transformation: $h_g^{(l+1)} = ReLU(W^{(l)} \widetilde{h}_g^{(l)})$. $W^{(l)}$ is the learnable weight matrix shared by l-order groups. By stacking this attention layer L times, we get the final representation of each node, and we further combine these representations, denoted by $h_g^{(L)}$.

Context Influences. The context elements include static and dynamic variables. The former has fixed values, such as latitude, longitude, and elevation, while the latter needs to be counted over time, such as the number of recent terrorist attacks and conflicts. Therefore, during the t-th session, the context elements of grid cells are defined as: $X_t = \{x_1, x_2, \ldots, x_m; x_{1,t}, x_{2,t}, \ldots, x_{n,t}\}$, where x_i is the i-th static variable, and $x_{i,t}$ is the i-th dynamic variable, m here represents the number of static variables, and n stands for the number of dynamic variables. Next, we use MLP to extract the information from the background elements of grid cells. Formally, $q_{T+1} = W_1[X_{T+1}]$, is the information of grid cells used in the prediction process of the next session.

Prediction and evaluation. In our framework, the next attack actions of a terrorist group are determined under the combined influence of its own interests, the terrorist network it belongs to, and the background context of the grids that were once attacked. Combining these influences by means of a fully-connected layer, we define the final representation as: $\widehat{h}_n = W_3[h_n; q_{T+1}; h_g^{(L)}]$. In contrast, the final representation in the base model is: $\widehat{h}_n = W_4[h_n; q_{T+1}]$. Finally, we use the *softmax* function to estimate the likelihood of the objects y being attacked by the terrorist group g in the next session $T+1$ is:

$$p\left(y \middle| c_{T+1,1}^g, \ldots, c_{T+1,n}^g; \left\{\overrightarrow{S}_T^k, k \varepsilon N(g)\right\}\right) = \frac{exp\left(\widehat{h}_n^T z_y\right)}{\sum\limits_{j=1}^{|C|} exp\left(\widehat{h}_n^T z_j\right)} \tag{8}$$

where z_y is the embedding of object y.

To evaluate the performance of all models, we use two common metrics in the recommendation system: *Recall@K* and Normalized Discounted Cumulative Gain (*NDCG*). The higher the values of *Recall@K* and *NDCG*, the more effective the model will be. *Recall@K* is the primary evaluation metric that evaluates the proportion of correct results amongst the top-K recommended items in all test cases, defined as: $Recall@K = \frac{n_{correct}}{N}$, where N denotes the number of test data in the prediction results, $n_{correct}$ denotes the number of cases with the desired items in the top-K item list. In this study, K was taken as 20. *NDCG* is a widely used ranking metric that considers the order of items and gives a higher score if the order is closer to the actual sample. It is formulated as: $NDCG = \frac{1}{\log_2(1+rank_{pos})}$, where $rank_{pos}$ is the rank of a positive item. By averaging the values of *NDCG* over all the testing examples, we get the final *NDCG*. Considering the potentially massive damage caused by terrorist attacks and the effective precautions we can help the authorities take if our predictions yield high accuracy, it is imperative that the models for predicting terrorist attacks have a high recall rate to prevent most of them from occurring. The higher the values of *Recall@K* and *NDCG*, the more effective the model is.

Model settings. For all different time resolutions, we kept the data within the last session to check the performance of the model, and the rest of the data was divided into the training set, test set, and validation set in a ratio of 8:1:1 b y chronological order. We filter out the objects and sessions that appear less than twice in the training set. In addition, to ensure that the number of sessions in which a terrorist organization participated is enough to reflect individual behavioral habits, we exclude terrorist groups that participated in fewer than two sessions.

We use TensorFlow [8] to implement our models. When applying gradient descent to optimize the loss function, we set the mini-batch size to be 200 and use Adam [9] with default parameters as the optimizer. Meanwhile, we set the learning rate to start at

0.001 and decay at the rate of 0.98 every 400 steps by applying exponential decay. In order to avoid overfitting, our models use the dropout technique [10] to randomly discard 20% of the nodes during training. We use Glorot Uniform initializer [11] for the initialization of weights and bias. We train both models for 100 epochs, and we apply a validation set strategy for early stopping [12]: when the model's Recall@20 on the validation set falls below the highest value previously obtained for 10 consecutive times, the training ends early. To improve efficiency in training graph attention networks with a large range of node degrees, we generate embeddings by sampling and aggregating features from a node's local neighborhood [13]. Furthermore, we only use the most recent sessions of the linked terrorist groups to represent their short-term attack preference.

Following the research of Song et al. [7], the dimensions of the terrorist groups and object representations for all models are fixed at

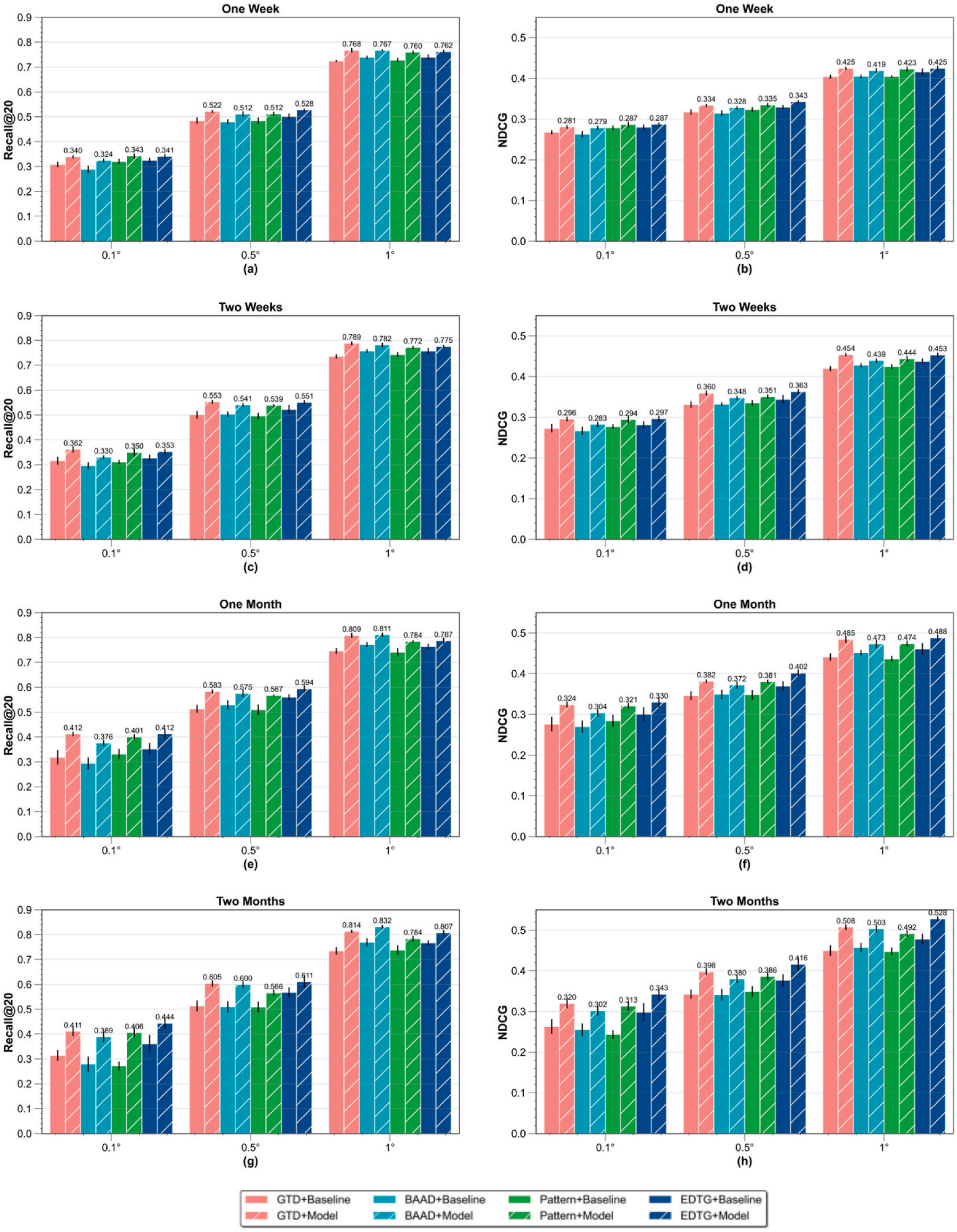


Fig. 4. The performance of our framework model and the baseline model at different spatio-temporal resolutions and with different types of terrorist group networks in terms of *Recall*@20 (a) and *NDCG* (b). For detailed numerical values, consult Table S1.

100. The number of hidden units of the LSTMs and most of the dense layers in our model is also set at 100. In comparison, the baseline model uses three hidden layers to extract individual attack information of terrorist groups, and the numbers of nodes in these layers are 40, 20, and 40, respectively. In all experiments, we empirically set the number of first and second-order neighbors to 10 and 5, respectively.

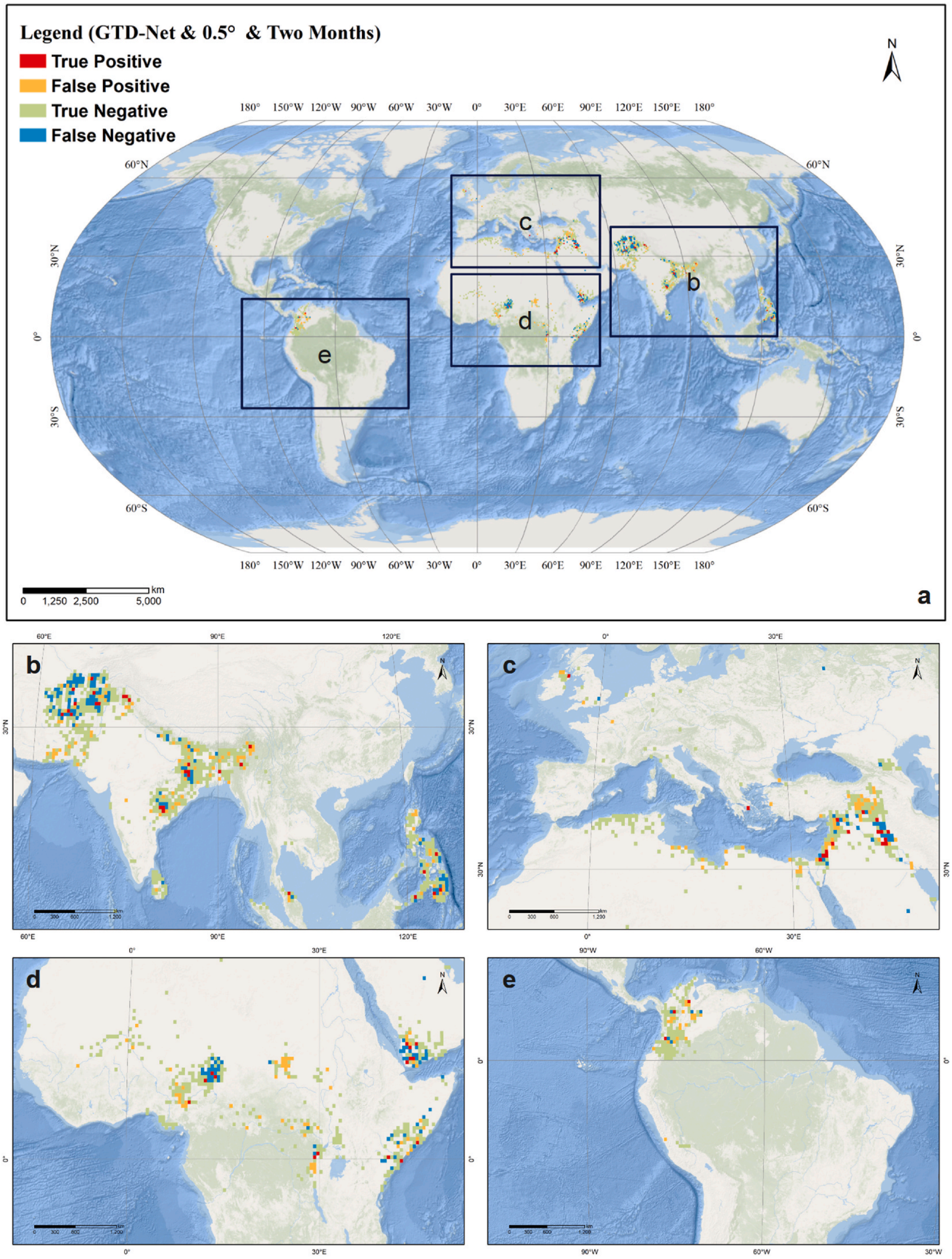


Fig. 5. The TP, TN, FP, and FN grid cells of the active terrorist groups' predictions with the GTD-Net at 0.5° and two-month lag for the last session worldwide: (a) Global; (b) South Asia and Southeast Asia; (c) North Africa and the Middle East; (d) Central Africa; (e) South America.

3. Results

3.1. The framework model compared to the baseline model

We compare our framework model with the baseline model for various combinations of spatio-temporal resolutions by the predictive performance. Spatial resolutions include 0.1 decimal degree, 0.5 decimal degree, and 1 decimal degree on latitude and longitude, while temporal resolutions include one week, two weeks, one month, and two months. To estimate the general predictive

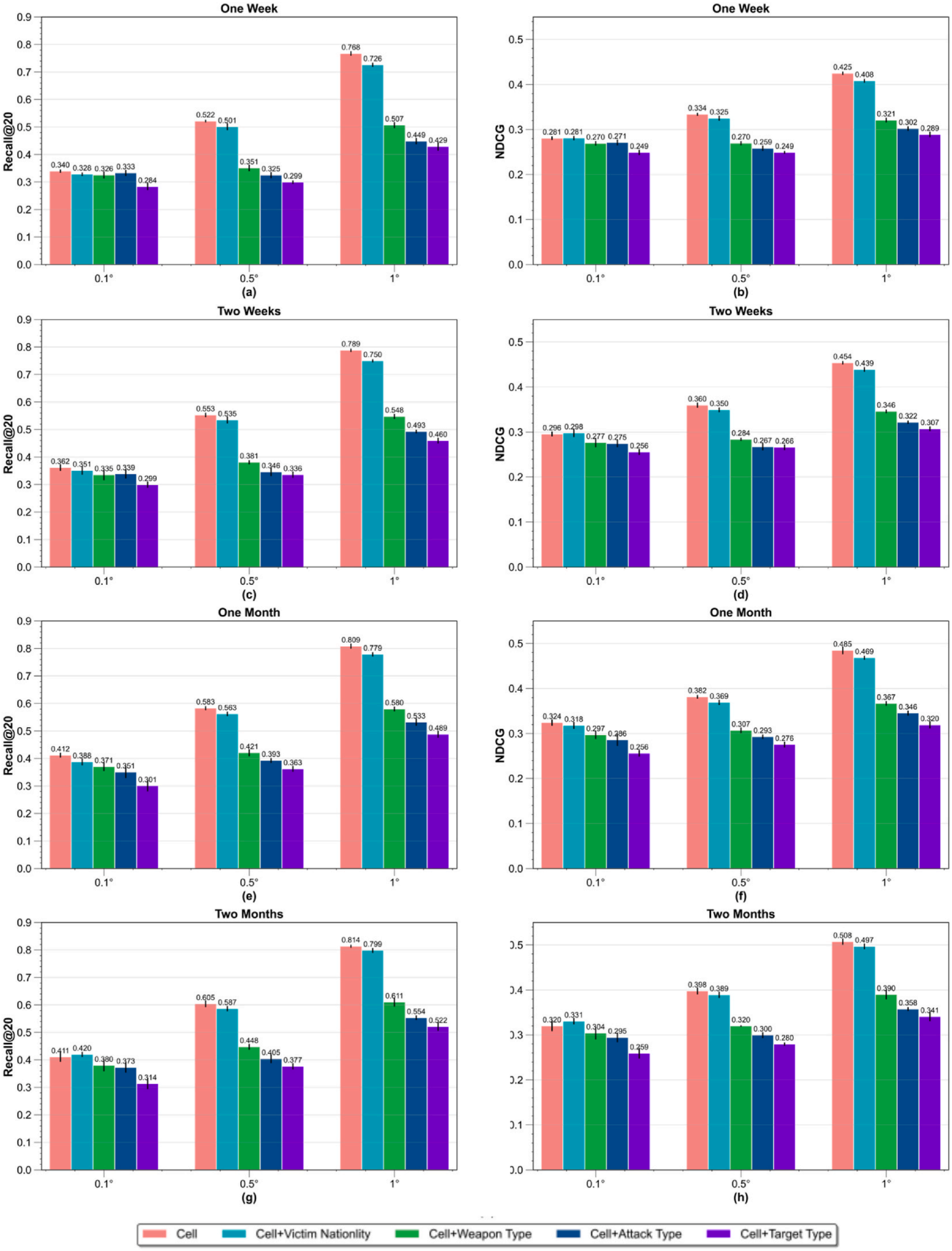
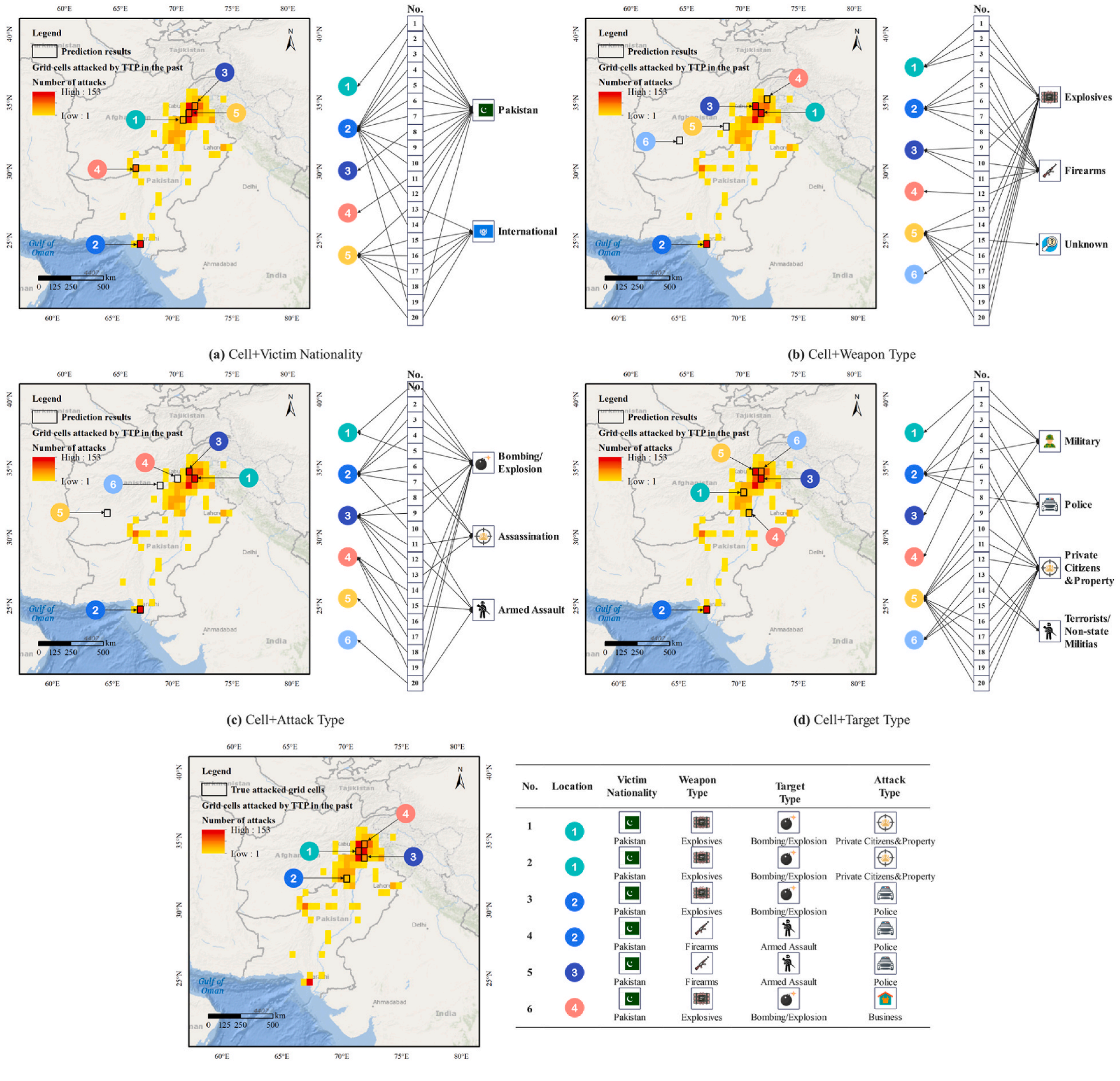


Fig. 6. The performance of our framework model with GTD-Net in different prediction modes where the outputs are locations of targets combined with different attack attributes in terms of *Recall*@20 (a) and *NDCG* (b). For detailed numerical values, consult Table S2.

performance of the models, we compute *Recall*@20 and *NDCG*, which evaluate their correctness and ranking performance, respectively.

The results in Fig. 4 show that our framework outperforms the baseline model at all spatio-temporal resolutions using both *Recall*@ 20 and *NDCG* and with all terrorist organization networks. The accuracy of the models decreases with the spatial resolution and the shortening of the time lag, which implies that group-oriented attacks are increasingly challenging to predict on finer scales. The accuracy difference among the spatial scales is much more significant than that among the temporal scales, suggesting a greater impact of the spatial resolution on predicting terrorist attacks. Models with EDTG-Net and GTD-Net generally performed better than BAAD-Net and Pattern-Net, especially at high spatial resolutions. There was no significant difference between the results of EDTG-Net and GTD-Net, which suggests that the network constructed with clustering algorithms is just as applicable as those based on expertise in substituting the real terrorist networks.

Despite the high accuracy of the model at 1° spatial resolution (about 111 × 111 km^2), the coarse resolution of such a prediction



(a) Cell+Victim Nationality

(b) Cell+Weapon Type

(c) Cell+Attack Type

(d) Cell+Target Type

No.	Location	Victim Nationality	Weapon Type	Target Type	Attack Type
1	1	Pakistan	Explosives	Bombing/Explosion	Private Citizens&Property
2	1	Pakistan	Explosives	Bombing/Explosion	Private Citizens&Property
3	2	Pakistan	Explosives	Bombing/Explosion	Police
4	2	Pakistan	Firearms	Armed Assault	Police
5	3	Pakistan	Firearms	Armed Assault	Police
6	4	Pakistan	Explosives	Bombing/Explosion	Business

(e) True Results

Fig. 7. Predicted results (two months ahead) and true ones of TTP in the GTD-Net at 0.5° resolution in November and December of 2019, showing the combination of location with terrorist attack-related information: (a) Cell + Victim Nationality; (b) Cell + Weapon Type; (c) Cell + Attack Type; (d) Cell + Target Type; (e) True Results. We marked grid cells with potential strikes in black, labeling each with a number representing the order of occurrence, limiting our prediction to a maximum of 20 attacks. The color legend shows the number of past terrorist attacks.

makes it hardly possible for the authorities to locate specific targets. Regarding the time resolution, the maximum improvement of our model over the baseline model at a specific spatial scale is achieved at a two-month time interval (with both *Recall*@20 and *NDCG*). When taking both the efficiency of anti-terrorism deployment and the prediction accuracy of our model into consideration, the best spatial and temporal resolutions for such predictions is 0.5° and two-month lag, respectively.

3.2. *Predicting high-risk locations of potential terrorism attacks*

A prediction example of our framework model is presented on the map in Fig. 5. We chose active terrorist groups in the terrorist network to predict potential locations of attacks two months in advance. A terrorist group was defined as active if it had striked at least once in the last five years [76]. For every group, we predicted its attack sequences in the sessions that were not involved in model training. All predictions were then aggregated into the grid cells. Every alternative cell would be labeled as positive if it included at least one prediction and negative otherwise. When the forecasts are compared to the actual situation, they could be classified as true positive (TP), false positive (FP), true negative (TN), or false negative (FN). Further, the overall accuracy, recall, and precision within a single session could be calculated (Fig. S1). Because of the dangers of terrorism, the recall of the model is much more critical. The GTD-Net was chosen to have the highest recall when applied to the last session at the best spatio-temporal resolution, the results of which were shown in Fig. 5 (showing TP, TN, FP, and FN grid cells). The TN cells (green) are the most common of the four types in Fig. 5, which is due to the fact that there are many more negative examples than positive ones in a whole grid. Fig. 5 depicts the results of our framework model forecasting places at high risk of global terrorism. And the FN cells (blue) are the most noticeable, and their number has a direct impact on the recall. The slope of the regression line of the assessment metrics versus time in Fig. S1 shows a decreasing trend in the model's performance over time. The framework model should be continually trained and updated in real-time to maintain a high recall. The results derived from models based on other terrorist networks are shown in Figs. S2–S4.

3.3. *Major attributes predicting terrorist strikes*

We selected GTD-Net as the terrorist network input to run our framework model for different objectives of prediction. The site of a terrorist attack (specific grid cell in our framework) serves as the foundation for predicting terrorism, while other attributes of the incident (such as victim nationality, weapon type, attack type, and target type) provide extra knowledge that can assist in counter-terrorism operations.

Fig. 6 indicates better accuracy yielded from *Cell* on *Recall*@20 and *NDCG* in the mode of *Cell* only and *Cell* + *Victim Nationality* than the remaining three prediction modes while no significant difference between *Cell* and *Cell* + *Victim Nationality* can be observed. Therefore, location and victim nationality were by far the main reliably predicted attributes of terrorism attacks, while the remaining attributes– choice of weaponry, method of attack, and type of target, were less accurately predicted. One explanation is that terrorist groups tend to act locally, rendering high consistency between the nationalities of the targeted people (location), while their attacking strategies and tactics, which involve target type, method of attack, and weaponry use, might be more random and difficult to predict.

3.4. *Predicting the details of a potential strike by an active terrorist group*

Selecting a single terrorist group – the Tehrik-i-Taliban Pakistan (TTP), we show the numerous predicting attributes on the risk of its terrorism attacks (Fig. 7). The TTP was chosen because of its large terrorist activity in major areas such as Afghanistan and Pakistan. It is also listed in the top 10 most weighted and joint degrees (the number of partners) of terrorist organizations in GTD-Net [46]. We demonstrate predicted TTP strikes and the recorded real attacks of TPP from the last session (two months ahead) at 0.5°. In addition to showing the location of their potential attacks, we present the victim's nationality, weapon type, method of attack, and target type. Further, we link these results with the corresponding order of their occurrence.

To present how a terrorist group may strike the same target more than once with varying methods of attack, type of target, and choice of weaponry used, we linked each targeted location to these three attributes in a chronological sequence of attacks. We observed an apparent discrepancy in results between the different prediction modes (*Cell* + *Victim Nationality*, *Cell* + *Weapon Type*, *Cell* + *Attack Type*, and *Cell* + *Target Type*), which may be owing to our ways of constructing each mode. In each mode, we presented targeted cells with different types of related attributes, and we distinguished one attack from another by highlighting a specific type of predicted feature, which itself often varies from attack to attack. All of these may lead to differences in the constructed attack sequences and, therefore, different results by prediction mode. Compared to the actual attack records of TTP during the last session, the predicted results of our four modes hit half of the four records regarding location. In terms of other additional attributes, our model correctly predicts the great majority of the outcomes.

4. Discussion

Terrorism is a key global challenge of the 21st century [77–79] particularly since several groups have stepped up their activities during the COVID-19 pandemic [80–82]. Predicting the attack patterns of terrorist groups is thus on top of the agenda of both researchers and policymakers [83]. To predict terrorist attacks with high accuracy, we constructed a framework where deep learning techniques were applied to derive the dynamic impact of the predictors chosen from multiple perspectives on the future behaviors of terrorist groups. More specifically, we chose the predictors at the macro-, meso-, and micro-levels, which involve elements regarding the background context of the attacked locations, the social network among terrorist groups, and past actions of individual groups, respectively to forecast their future behaviors. We were able to identify high-risk areas subjected to potential threats on a global scale by aggregating projected locations of all the active terrorist groups worldwide in the next period. Further, for each particular group, we could also provide multi-information on its future attacks, including the attributes of the targets such as location, type, nationality, and possible means and weapons they may employ.

In terrorist risk assessment, the typical research often extracts the risks of geographical units according to the records of terrorist attacks over a certain period to build a model that predicts future high-risk locations [21–25]. While such a forecast alerts local decision-makers to the possibility of future terrorist attacks, it does not identify the source of the risk, especially the group to which potential perpetrators might belong. In other words, if we identify the terrorist groups that might send perpetrators, local decision-makers and authorities may disrupt and even stop terrorist actions with their expertise, for example, by placing temporary checkpoints along critical routes. Therefore, a more specific prediction of terrorism attacks is required for local governments to make informed decisions on providing security for the public and allocating resources appropriately. Existing studies aiming to achieve such precision normally use time-series models but do not consider the possibility of one group's action being affected by others, given their assumption that terrorist groups always act independently [37,39,40]. However, there is evidence that the actions and choices of terrorist groups refer to other groups' activities when they choose targets and strike [84]. Incorporating information from associated groups allows the terrorist groups to expand their choices beyond their past objectives and include their related groups' past targets. Taking the interaction between these groups into consideration might offer us a more comprehensive view of terrorist groups' seemingly random and clandestine target selection. Given the absence of reliable empirical data on terrorist networks, we collected domain knowledge-based networks from open-source data and constructed two networks using clustering techniques based on a previous study [47,48]. Our model better performed when employing EDTG-Net, which could be attributed to its construction based on the terrorist groups' base regions, ideologies, and motivations, aspects that highly correlate with terrorist group alliances [85,86]. As far as our results are concerned, a rational terrorist network is a key to understanding the behaviors of terrorist groups.

Our research has some limitations. Extensive studies have shown that terrorist organizations place great importance on protecting the security of their actions [87,88]. Illegal groups hope to keep their actions secret and avoid becoming the target of authorities in order to achieve their destructive collective goals, but at the same time, they need a certain degree of coordination to successfully achieve their goals, such as by spreading false information to conceal their activities [89,90]. Nearly half of the perpetrator organizations in the terrorist attack records from 2002 to 2019 used in the GTD dataset are unknown. Therefore, there may be a certain gap between the observed action trajectories of certain terrorist organizations and the actual situation. In addition, perpetrator attribution in each attack record reflects the content reported in open-source media accounts, which does not necessarily indicate legal culpability [1]. The GTD is primarily derived from media articles that may contain bias and inaccuracies in reporting on terrorist attacks [54]. Finally, after the 9/11 attacks, there has been an increase in politically motivated acts of violence committed by so-called "lone-wolf" or "lone-actor." [91] Compared to group actors, lone wolves engage in fewer precursor activities but are willing to go further in preparing for and executing attacks and can survive longer by avoiding capture [92]. There are currently limitations in the data, theory, and models we used to predict this type of terrorist attack.

Supported by currently available data and our stringent quality control of data processing, our model enables predicting future attacks at relatively fine spatial and temporal resolutions. More fine-grained datasets can further improve the predictive power of our model. Coupled with the enhancement of future deep learning technology and terrorism theory, we believe that this will enable broadening the scope of terrorism causes, improving the approach offered in this study, and further providing decision-makers with up-to-date analytical tools that could be conducive to the global counter-terrorism strategies and organized violent crime analysis.

Open research

All data used in this study is publicly available. The codes of our model are freely available online at https://github.com/wujj21b/terrorism_prediction.

Author contribution statement

Dong Jiang: Conceived and designed the experiments; Analyzed and interpreted the data; Wrote the paper.

Jiajie Wu: Performed the experiments; Analyzed and interpreted the data; Wrote the paper.

Fangyu Ding: Conceived and designed the experiments; Performed the experiments; Analyzed and interpreted the data; Wrote the paper.

Tobias Ide, Jürgen Scheffran, David Helman, Shize Zhang, Jingying Fu, Shuai Chen, Xiaolan Xie, Tian Ma: Contributed reagents, materials, analysis tools or data.

Yushu Qian: Contributed reagents, materials, analysis tools or data; Wrote the paper.

Mengmeng Hao: Conceived and designed the experiments; Performed the experiments; Analyzed and interpreted the data; Wrote the paper.

Quansheng Ge: Conceived and designed the experiments; Wrote the paper.

Data availability statement

Data will be made available on request.

Additional information

No additional information is available for this paper.

Key points

•We develop and evaluate an integrated deep-learning and multi-level framework for forecasting terrorist organizations' future targets.
•The output of the framework comprises the locations and categories of the next targets as well as the tactics of the terrorist group.
•Our methodology has the potential to provide game-changing insights into other organized violent crimes.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This research was funded by the National Natural Science Foundation of China (Grant No. 42001238) and the Strategic Priority Research Program of the Chinese Academy of Sciences (Grant No. XDA19040305).

Appendix A. Supplementary data

Supplementary data to this article can be found online at https://doi.org/10.1016/j.heliyon.2023.e18895.

References

[1] Study of terrorism and responses to terrorism (START), Global Terrorism Database Codebook: Methodology, Inclusion Criteria, and Variables (2021).
[2] Study of Terrorism and Responses to Terrorism (START), Global Terrorism Database (GTD), University of Maryland, 2021.
[3] H. Bardwell, M. Iqbal, The economic impact of terrorism from 2000 to 2018, Peace Econ. Peace Sci. Publ. Pol. 27 (2) (2021) 227–261.
[4] General Assembly, Resolution Adopted by the General Assembly on 11 September 2015. 2015, A/RES/69/315 15 September, United Nations, New York, 2015.
[5] M. Sageman, Understanding Terror Networks, University of Pennsylvania press, 2004.
[6] A. Sliva, et al., Cape: Automatically Predicting Changes in Group Behavior, Springer, 2009.
[7] T. Veldhuis, J. Staun, Islamist Radicalisation: A Root Cause Model, Netherlands Institute of International Relations Clingendael The Hague, 2009.
[8] J. Cohen, J.M. Blanco, Knowledge, the Great Challenge to Deal with Terrorism, Revista de Estudios en Seguridad Internacional, 2016.
[9] R. Tuesday, C. Colin, A. Laura, Examining the Nexus between Organised Crime and Terrorism and its Implications for EU Programming, European Union, 2017.
[10] B. Doosje, et al., Terrorism, radicalization and de-radicalization, Current Opinion in Psychology 11 (2016) 79–84.
[11] T. Bjørgo, A. Silke, Root causes of terrorism, in: Routledge Handbook of Terrorism and Counterterrorism, Routledge, 2018, pp. 57–65.
[12] C.R. McCauley, M.E. Segal, Social Psychology of Terrorist Groups, 2009.
[13] M.N. Milla, et al., Is the role of ideologists central in terrorist networks? A social network analysis of Indonesian terrorist groups, Front. Psychol. 11 (2020) 333.
[14] T. Waskiewicz, Friend of a friend influence in terrorist social networks, in: Proceedings on the International Conference on Artificial Intelligence (ICAI), The Steering Committee of The World Congress in Computer Science, Computer, 2012.
[15] G. LaFree, A. Schwarzenbach, Micro and macro-level risk factors for extremism and terrorism: toward a criminology of extremist violence, Monatsschrift für Kriminol. Strafr. 104 (3) (2021) 184–202.
[16] G. LaFree, G. Ackerman, The empirical study of terrorism: social and legal research, Annu. Rev. Law Soc. Sci. 5 (2009) 347–374.
[17] M.A. Ruiz Estrada, A. Khan, The evolution and perspectives of the terrorism academic research, Available at SSRN 3522390 (2020).
[18] S.P. Kluch, A. Vaux, The non-random nature of terrorism: an exploration of where and how global trends of terrorism have developed over 40 years, Stud. Conflict Terrorism 39 (12) (2016) 1031–1049.
[19] S. Perry, The application of the "Law of Crime Concentration" to terrorism: the Jerusalem case study, J. Quant. Criminol. 36 (2020) 583–605.
[20] B. Behlendorf, G. LaFree, R. Legault, Microcycles of violence: evidence from terrorist attacks by ETA and the FMLN, J. Quant. Criminol. 28 (2012) 49–75.
[21] W.L. Perry, et al., Predicting Suicide Attacks: Integrating Spatial, Temporal, and Social Features of Terrorist Attack Targets, Rand Corporation, 2013.
[22] S.C. Nemeth, J.A. Mauslein, C. Stapley, The primacy of the local: identifying terrorist hot spots using geographic information systems, J. Polit. 76 (2) (2014) 304–317.
[23] F. Ding, et al., Understanding the dynamics of terrorism events with multiple-discipline datasets and machine learning approach, PLoS One 12 (6) (2017), e0179057.
[24] M. Hao, et al., Simulating spatio-temporal patterns of terrorism incidents on the indochina peninsula with GIS and the random forest method, ISPRS Int. J. Geo-Inf. 8 (3) (2019) 133.
[25] A. Python, et al., Predicting non-state terrorism worldwide, Sci. Adv. 7 (31) (2021), eabg4778.
[26] M. Crenshaw, Theories of terrorism: instrumental and organizational approaches, J. Strat. Stud. 10 (4) (1987) 13–31.
[27] G.H. McCormick, Terrorist decision making, Annu. Rev. Polit. Sci. 6 (1) (2003) 473–507.
[28] R. Borum, Psychology of terrorism (2004).
[29] W. Enders, G.F. Parise, T. Sandler, A time-series analysis of transnational terrorism: trends and cycles, Defence Peace Econ. 3 (4) (1992) 305–320.
[30] Z. Li, et al., Terrorist group behavior prediction by wavelet transform-based pattern recognition, Discrete Dynamics in Nature and Society, 2018 (2018) 1–16.
[31] G.M. Campedelli, M. Bartulovic, K.M. Carley, Pairwise similarity of jihadist groups in target and weapon transitions, Journal of Computational Social Science 2 (2019) 245–270.
[32] G.M. Campedelli, I. Cruickshank, K. M Carley, A complex networks approach to find latent clusters of terrorist groups, Applied Network Science 4 (1) (2019) 1–22.

[33] G.M. Campedelli, I. Cruickshank, K.M. Carley, Multi-modal networks reveal patterns of operational similarity of terrorist organizations, Terrorism Polit. Violence (2021) 1–20.

[34] H. Ruda, S.K. Das, G.L. Zacharias, Predicting terrorist actions using sequence learning and past events, in: Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Defense and Law Enforcement II, International Society for Optics and Photonics, 2003, pp. 128–138.

[35] A. Mannes, et al., Stochastic Opponent Modeling Agents: A Case Study with Hezbollah. Social Computing, Behavioral Modeling, and Prediction, Springer, 2008, pp. 37–45.

[36] E. Serra, V. Subrahmanian, A survey of quantitative models of terror group behavior and an analysis of strategic disclosure of behavioral models, IEEE Transactions on Computational Social Systems 1 (1) (2014) 66–88.

[37] Q. Liu, et al., Predicting the next location: a recurrent model with spatial and temporal contexts, in: Thirtieth AAAI Conference on Artificial Intelligence, 2016.

[38] M.I. Uddin, et al., Prediction of Future Terrorist Activities Using Deep Neural Networks, Complexity, 2020, p. 2020.

[39] Z. Liu, et al., Predict the next attack location via an attention-based fused-SpatialTemporal LSTM, in: 2020 29th International Conference on Computer Communications and Networks (ICCCN), IEEE, 2020, pp. 1–6.

[40] G.M. Campedelli, M. Bartulovic, K.M. Carley, Learning future terrorist targets through temporal meta-graphs, Sci. Rep. 11 (1) (2021) 1–15.

[41] F. Saidi, Z. Trabelsi, A hybrid deep learning-based framework for future terrorist activities modeling and prediction, Egyptian Informatics Journal 23 (3) (2022) 437–446.

[42] A. Perliger, A. Pedahzur, Social network analysis in the study of terrorism and political violence, PS Political Sci. Polit. 44 (1) (2011) 45–50.

[43] Z. Li, et al., Terrorist group behavior prediction by wavelet transform-based pattern recognition, Discrete Dynamics in Nature and Society, 2018 (2018).

[44] A. Aleroud, A. Gangopadhyay, Multimode co-clustering for analyzing terrorist networks, Inf. Syst. Front 20 (5) (2018) 1053–1074.

[45] R. Yarlagadda, et al., Implicit terrorist networks: a two-mode social network analysis of terrorism in India, in: International Conference on Social Computing, Behavioral-Cultural Modeling and Prediction and Behavior Representation in Modeling and Simulation, Springer, 2018, pp. 340–347.

[46] G. Li, et al., Analysis of the terrorist organization alliance network based on complex network theory, IEEE Access 7 (2019) 103854–103862.

[47] V. Loia, F. Orciuoli, Understanding the composition and evolution of terrorist group networks: a rough set approach, Future Generat. Comput. Syst. 101 (2019) 983–992.

[48] D.D. Atsa'am, R. Wario, F.E. Okpo, A new terrorism categorization based on casualties and consequences using hierarchical clustering, J. Appl. Secur. Res. 15 (3) (2020) 369–384.

[49] V. Subrahmanian, et al., Computational Analysis of Terrorist Groups: Lashkar-E-Taiba: Lashkar-E-Taiba, Springer, 2013.

[50] V. Subrahmanian, et al., Indian Mujahideen: Computational Analysis and Public Policy, Springer Science & Business Media, 2013.

[51] E. Bakker, Forecasting terrorism: the need for a more systematic approach, J. Strat. Secur. 5 (4) (2012) 69–84.

[52] Q. Schiermeier, Attempts to predict terrorist attacks hit limits, Nature 517 (7535) (2015) 419–420.

[53] S. Atran, et al., Challenges in researching terrorism from the field, Science 355 (6323) (2017) 352–354.

[54] S.R. Srivastava, Y.K. Meena, G. Singh, The landscape of soft computing applications for terrorism analysis: a review, Appl. Soft Comput. 113 (2021), 107977.

[55] Editorial, Understanding and countering terrorism, Nat. Human Behav. 1 (6) (2017) 134.

[56] B. Ellis, Countering complexity: an analytical framework to guide counter-terrorism policy-making, Journal of Military and Strategic Studies 6 (1) (2003).

[57] M.D.G. Arce, T. Sandler, Counterterrorism: a game-theoretic analysis, J. Conflict Resolut. (2005) 183–200.

[58] N. Jaafar, Z. Lachiri, Multimodal fusion methods with deep neural networks and meta-information for aggression detection in surveillance, Expert Syst. Appl. 211 (2023), 118523.

[59] V.H. Asal, R.K. Rethemeyer, E.W. Schoon, in: V.H. Asal, R.K. Rethemeyer (Eds.), Replication Data for: "Crime, Conflict and the Legitimacy Tradeoff: Explaining Variation in Insurgents' Participation in Crime, Harvard Dataverse, 2018.

[60] V.H. Asal, R.K. Rethemeyer, E.W. Schoon, Crime, conflict, and the legitimacy trade-off: explaining variation in insurgents' participation in crime, J. Polit. 81 (2) (2019) 399–410.

[61] D. Hou, K. Gaibulloev, T. Sandler, Introducing extended data on terrorist groups (EDTG), 1970 to 2016, J. Conflict Resolut. 64 (1) (2020) 199–225.

[62] J.L. Elman, Finding structure in time, Cognit. Sci. 14 (2) (1990) 179–211.

[63] W. Song, et al., Session-based social recommendation via dynamic graph attention networks, in: Proceedings of the Twelfth ACM International Conference on Web Search and Data Mining, 2019, pp. 555–563.

[64] G. Zhou, et al., Deep interest network for click-through rate prediction, in: Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, 2018, pp. 1059–1068.

[65] G. LaFree, L. Dugan, Introducing the global terrorism database, Terrorism Polit. Violence 19 (2) (2007) 181–204.

[66] M. Smith, S.M. Zeigler, Terrorism before and after 9/11–a more dangerous world? Res. Politics 4 (4) (2017), 2053168017739757.

[67] B. Hidasi, et al., Session-based recommendations with recurrent neural networks, arXiv preprint arXiv:1511.06939 (2015).

[68] A.F. Tollefsen, H. Strand, H. Buhaug, PRIO-GRID: a unified spatial data structure, J. Peace Res. 49 (2) (2012) 363–374.

[69] D. Silver, et al., Mastering the game of Go with deep neural networks and tree search, Nature 529 (7587) (2016) 484–489.

[70] W. Guo, K. Gleditsch, A. Wilson, Retool AI to Forecast and Limit Wars, Nature Publishing Group, 2018.

[71] V. Nair, G.E. Hinton, Rectified linear units improve restricted Boltzmann machines, Icml (2010).

[72] S. Hochreiter, J. Schmidhuber, Long short-term memory, Neural Comput. 9 (8) (1997) 1735–1780.

[73] D. Bahdanau, K. Cho, Y. Bengio, Neural Machine Translation by Jointly Learning to Align and Translate, 2014 arXiv preprint arXiv:1409.0473.

[74] T.N. Kipf, M. Welling, Semi-supervised classification with graph convolutional networks, arXiv preprint arXiv:1609.02907 (2016).

[75] P. Velickovic, et al., Graph attention networks, Stat 1050 (2017) 20.

[76] K. Gaibulloev, D. Hou, T. Sandler, How do the factors determining terrorist groups' longevity differ from those affecting their success? Eur. J. Polit. Econ. 65 (2020), 101935.

[77] I. Duyvesteyn, How new is the new terrorism? Stud. Conflict Terrorism 27 (5) (2004) 439–454.

[78] K.M. Carley, A Dynamic Network Approach to the Assessment of Terrorist Groups and the Impact of Alternative Courses of Action, Carnegie-Mellon Univ Pittsburgh Pa Inst of Software Research Internat, 2006.

[79] J.M. Post, Terrorism and right-wing extremism: the changing face of terrorism and political violence in the 21st century: the virtual community of hatred, Int. J. Group Psychother. 65 (2) (2015) 242–271.

[80] T. Ide, COVID-19 and armed conflict, World Dev. 140 (2021), 105355.

[81] G. Ackerman, H. Peterson, Terrorism and COVID-19, Perspectives on Terrorism 14 (3) (2020) 59–73.

[82] A. Basit, COVID-19: a challenge or opportunity for terrorist groups? Journal of Policing, Intelligence and Counter Terrorism 15 (3) (2020) 263–275.

[83] J. Beall, Cities, Terrorism and Urban Wars of the 21st Century, 2007.

[84] P.J. Phillips, G. Pohl, Prospect theory and terrorist choice, J. Appl. Econ. 17 (1) (2014) 139–160.

[85] V.H. Asal, et al., With friends like these… why terrorist organizations ally, Int. Publ. Manag. J. 19 (1) (2016) 1–30.

[86] T. Bacon, Why terrorist groups form international alliances, in: Why Terrorist Groups Form International Alliances, University of Pennsylvania Press, 2018.

[87] B. McAllister, Al, Qaeda and the innovative firm: demythologizing the network, Stud. Conflict Terrorism 27 (4) (2004) 297–319.

[88] C. Stohl, M. Stohl, Networks of terror: theoretical assumptions and pragmatic consequences, Commun. Theor. 17 (2) (2007) 93–124.

[89] W.E. Baker, R.R. Faulkner, The Social Organization of Conspiracy: Illegal Networks in the Heavy Electrical Equipment Industry, American sociological review, 1993, pp. 837–860.

[90] K. Drozdova, M. Samoilov, Predictive analysis of concealed social network activities based on communication technology choices: early-warning detection of attack signals from terrorist organizations, Comput. Math. Organ. Theor. 16 (2010) 61–88.

[91] C.A. Eby, The Nation that Cried Lone Wolf: A Data-Driven Analysis of Individual Terrorists in the United States since 9/11, Naval Postgraduate School Monterey CA Dept of National Security Affairs, 2012.

[92] B.L. Smith, et al., The emergence of lone wolf terrorism: patterns of behavior and implications for intervention, in: Terrorism and Counterterrorism Today, Emerald Group Publishing Limited, 2015, pp. 89–110.