Behavior Associations in Lone Actor Terrorists

Ayca Altay*[a], Melike Baykal-Gürsoy[a], Pernille Hemmer[b]

[a]Industrial & Systems Engineering, Rutgers University, Piscataway, NJ, USA

[b]Department of Psychology, Rutgers University, Piscataway, NJ, USA

*CoRE Building, 96 Frelinghuysen Rd, Piscataway, NJ 08854

ayca.altay@rutgers.edu

Terrorist attacks carried out by individuals have significantly accelerated over the last 20 years. This type of lone-actor (LA) terrorism stands as one of the greatest security threats of our time. While the research on LA behavior and characteristics has produced valuable information on demographics, classifications, and warning signs, the relationship among these characters is yet to be addressed. Moreover, the means of radicalization and attacking have changed over decades. This study conducts an a-posteriori analysis of the temporal changes in LA terrorism and behavioral associations in LAs. We initially identify 25 binary behavioral characteristics of LAs and analyze 190 LAs. Next, we classify LAs according to ideology first, incident scene behavior (determined via a virtual attacker-defender game) secondly, and, finally, clusters obtained from the data. In addition, within each class, statistically significant associations and temporal relations are extracted using the A-priori algorithm. These associations would be instrumental in identifying the attacker's type and intervene at the right time. The results indicate that while pre-9/11 LAs were mostly radicalized by the people in their environment, post-9/11 LAs are more diverse. Furthermore, association chains for different LA types present unique characteristic pathways to violence and after-attack behavior.

Keywords: lone-actor terrorism, association rule mining, the A-priori algorithm, R-rules, temporal associations

Introduction

Terrorism is defined as an act of aggression against noncombatants with the objective of influencing policymakers through intimidation.[1] Terrorist threat is motivated by ideology, not mere personal vengeance.[2] Partly due to the success in counterterrorism efforts, the face of terrorism has changed dramatically in recent years. Attacks by groups with defined chains of command have declined as the prevalence of autonomous cells and individuals has grown. In particular, lone actor (LA) terrorism, such as the 2017 Las Vegas mass shooting of concertgoers[3] and the 2019 El Paso shooting in a supermarket,[4] has increased by 134% over the last 20 years.[5]

While scholars disagree about how to define LA terrorism (particularly whether it includes dyads, triads, or members of extremist organizations), they largely agree on several characteristics.[6,7] LA attacks are the consequences of a personal grudge channeled into a higher cause; thus, personal or ideological motivations may not be entirely distinguishable. [8] Moreover, LAs require a longer attack preparation process: while rarely impulsive or sudden,[9] LAs are not as well-organized as terrorist groups. [10] Finally, though LAs may align themselves with extreme movements,[11] they mostly appear to be too extremist even for terrorist organizations.[12] LA attacks differ from common crime or assassinations by involving an ulterior ideological component;[13] attackers ideologies are often a mixture of personal vendettas and ideological grievances. In the following subsections, we preview the common characteristics and prior quantitative analyses in this field.

Characteristics and Detection Challenges of LAs

The literature on behavioral characteristics of LAs focuses on (i) certain events or incidents that might cause radicalization, (ii) observable actions LAs might commit, and (iii) the environmental response to these actions. Some of these characteristics include events prior to attack intent, such as relations to extremists.[14] Some events or incidents may provoke the idea of an attack and act as a trigger. [15,16,17] Other behavioral characteristics involve details in attack planning.

Distinguishing LAs from people with extremist ideological views constitutes a challenge, as the majority of people with extremist ideological views do not pose a security threat.[18] A more extensive behavioral study conducted by Meloy et al.[19] defined eight proximal warning behaviors for an LA attack that then, were used in the Terrorist Radicalization Assessment Protocol (TRAP-18), a professional LA risk-assessment framework.[20] Besides these proximal warning behaviors , TRAP-18 also includes 10 distal characteristics [21] some of which are difficult to trace in real life.

Conventional attack prevention techniques, such as infiltration or wiretapping, are not effective for LA attacks due to the absence of a group.[22] However, LAs are commonly radicalized by Internet exchanges; and, therefore, leave their writeprints . [23,24] They spread their opinions before committing an actual attack. The biggest challenge in detecting LAs online is that search engines cannot access the deep web in which such e changes often take place. [25] These exchanges are traceable by law enforcement to a large extent.[26]

Classification of LAs

Although LAs have some commonalities, such as acting alone or being fixated on an ideology, their behaviors leading up to violence may vary among different attacker types. Consequently, the existing literature proposes different classification domains such as location, purpose, type of target, goals, and means of radicalization.[27, 28,29]

Gill et al.[30] classified LAs in terms of their ideologies: right-wing, Al-Qaeda related, and single issue. They argued that different LA subgroups have very noticeable characteristics in terms of demographics, network connectivity and operational success. This ideology-based classification was commonly applied in literature. Meloy and Gill[31] compared the three ideological groups in terms of their distal characteristics and warning behaviors.

Quantitative Approaches for LA Terrorism

Meaningful statistical analyses over LAs are difficult to conduct since LA attacks are black-swan events that are difficult to forecast.[32] Similarly, social network analysis methods fail due to the absence of a group network. [33,34] However, with the help of social media and online forums, identification, leakage and fixation are traceable online.

Brynielsson et al.[35] extracted the attack intent of an LA, a fundamental indicator of an attack, through text mining.[36,37] Phillips[38] calculated probabilistic changes on the target substitution or attack deterrence in a game-theoretical scheme. Gordon et al.[39] applied a Delphi Method, in which a facilitator gathers expert opinions on lone actor intent and target selection predictions anonymously with the sole purpose of arriving to a consensus by supplying recursive feedback.

Most quantitative studies on LA behavior consist of summary statistics and hypothesis tests. A recent study by Philips[40] demonstrated that LA attacks are deadly threats, especially in the United States. Ellis et al.[41] found that prior weapons training almost doubles the number of casualties per attack.

Although LAs have the aforementioned common characteristics, behaviors they exhibit on the pathway to violence can significantly differ. This difference requires classification of attacker types. Ideology-based classification yields common demographic characteristics,[42] but it may not necessarily provide commonalities in terms of behavioral characteristics or responses.

Another challenge for behavioral analyses is that the term behavior has different connotations in literature. Additionally, the terms terrorist behavior or attacker behavior can refer to different concepts. In some studies, the term involves attack-related behavior such as identification or fixation,[43] while in some others, behavior' refers to the response, mood, or observable actions of a terrorist.[44]

These studies indicate that while LA definition, typology, and demographics are known to a certain extent, relationships among these characteristics are yet to be discovered. We address this problem with an a-posteriori analysis by gathering data from established resources and studies rather than challenging the existing narrative. This paper makes the following contributions:

- Augments the "behavior" term with a temporal perspective.
- Identifies 25 binary attributes for LA characteristics based on the data prepared by Hamm and Spaaij.[45]
- Defines behavior-based attacker types using these binary attributes.
- Compares pre-9/11 LAs to post-9/11 LAs to reflect the temporal changes in LA terrorism.
- Analyzes the associations among LA behavioral characteristics for each type.
- Forms chain rules to summarize the evolution of each attacker type.
- Extracts temporal relations between LA behavior milestones for each type.

The structure of this paper is as follows. The next section provides detailed information on the means of LA data gathering and processing, the identification of 25 attributes for LA characteristics, and various LA classification schemes. The following introduces the A-priori algorithm, describes its statistical properties and the rule-chain-formation procedure. This is followed by a comparison of pre- and post-9/11 era. We analyze LA types based on three classification schemes: i) ideology-based, ii) incident-scene-based, and iii) behavioral-based, and form behavioral and chronological association chains of LAs for each type. Furthermore, we demonstrate the temporal relationship among observable landmarks on the attack pathway. Finally, we discuss our conclusions.

LA Characteristics, Behavior, Data, and Classifications

Data for LA Behavior and Characteristics

The National Criminal Justice Reference System (NCJRS) database prepared by Hamm and Spaaij[46] involves 98 LA attacks in the USA between 1940-2013. This dataset can be used to obtain data on LA behavior and attack characteristics. Though valuable, the database lacks the most recent data. The Global Terrorism Database (GTD)[47] holds the records of all terrorist events worldwide through 2017, which provides an additional 192 incidents. However, these include attacks claimed by terrorist groups, and unclaimed or unresolved attacks, as well. Another source, the Mother Jones database,[48] records all mass shootings in the USA, but while the overwhelming majority involves a single perpetrator, not all are categorized as LA terrorism. The following filter is used to distinguish LAs from other terrorist attacks in the GTD and other mass shootings in the Mother Jones database:

> For the GTD, the attacks should be planned and committed by a single person or two-person cells (dyads). The dyads will be evaluated separately for each attacker since they have been observed to exhibit different behaviors and have different environmental stimuli even for the same incident.
>
> In the GTD, all unclaimed and unresolved attacks are excluded, since they provide no data on the attacker.
>
> For the Mother Jones database, the motivations of attackers are checked, and attacks stemming solely from a personal grievance are excluded. However, for the sake of further research, we should note that bullying-related attacks have recently been discussed for inclusion as a part of single-issue events.[49]

In the GTD, 70 of the 196 attacks are unclaimed or unresolved, and 84 are identified as LA attacks. In the Mother Jones Database, 17 out of 44 mass shootings satisfy the criteria of LA attacks. Nine of those mass shootings overlap with GTD records. In total, data for 190 LAs have been obtained from these three databases.

Using the National Criminal Justice Reference System database as a template, we have gathered data on the following attacker characteristics:

● Demographic and socio-economic data: age, race, gender, marital status, mental health history, employment status and military history.
Distal characteristics: criminal history, relation to radical groups, means of radicalization.
Proximal warning behaviors: triggering event and leakage.
Attack decisions: target and weapon selection
Attack consequences: fatalities and after-attack behavior.

Distal characteristics differ from proximal warning behaviors [50] in that the former belong to the history of an LA before the attack idea and preparations. Proximal warning behaviors indicate that attack preparations have started. It can be observed that the distal characteristics or proximal warning behaviors we employ do not match to those in,[51] since our data do not specify warning behaviors such as last resort , energy burst or directly communicated threat . Using the available data, the distal characteristics are selected to maximize their relevance to radicalization and violence.

Our data include four female LAs, which comprise 2% of all LAs. Hence, any gender-based analysis on LAs would lack sufficient data. Three pre-9/11-era LAs have chosen terrorism as a career and committed multiple attacks over a decade. Excluding these three LAs, the average age of post-9/11 attackers is 35.11 with a standard deviation of 13.73 and a median of 31. The ages range from 15 to 88. Observations from the data indicate that sudden life changes serve as a triggering event. In fact, the three most common personal triggering events are separation from partner, losing job or student status, and emergence of mental or physical health issues. [52,53]

In this study, we choose to address algorithmic fairness concerns. Data analysis methods are prone to misjudge and manipulate outcomes if the inputs involve such sensitive characteristics. [54] One method to lead more fair results is to exclude sensitive, protected, and discriminatory characteristics, i.e. race, gender, mental history, etc. [55] Therefore, for fairness reasons, we avoid using demographic and socio-economic data directly in our behavioral characterization. However, it is also worth mentioning that the inclusion of these characters would not affect the already existing associations due to the nature of the methods we implement.

We construct the behavior and attack characteristics list using the following columns of NCJRS database prepared by Hamm and Spaaij:[56] fatalities/ injuries, weapons used, prior criminal history, military history, affinity with extremist groups, broadcasting intent, locus of radicalization, triggering event, and capture/arrest. For a more accurate binary characterization, we have analyzed and categorized the narratives in [57,58,59,60,61,62,63,64,65,66] and broken down the data into 25 binary characteristics under 10 headings as follows:

I) criminal history before the attack: 1) no criminal history; 2) one offense; 3) multiple offenses;

II) knowledge of weapons: 4) had formal weaponry training;

III) relation to radical groups: 5) no prior relations with any extremist groups; 6) has contacts with an extremist or a terrorist group/people;

IV) means of radicalization: 7) self-radicalized; 8) was not self-radicalized;

V) triggering event: 9) a triggering event caused the attack idea; 10) no particular triggering event, radicalized incrementally by the socio-political atmosphere;

VI) leakage: 11) no leakage was made; 12) leakage was made offline; 13) leakage was made online;

VII) targets: 14) civilians; 15) person symbolizing the enemy ideology (politician, religious leader, abortion doctor, etc.); 16) law enforcement (military, police, etc.) or government officials; 17) no targets aimed / fake or symbolic attack;

VIII) means of attack: 18) firearms; 19) other weapons;

IX) fatalities: 20) no fatalities or injuries; 21) only injuries but no fatalities; 22) at least one fatality;

X) after-attack behavior: 23) was able to escape the crime scene; 24) surrendered or was arrested at the crime scene; 25) committed suicide or was killed at the crime scene.

In this list, if a statement is true, then its value is entered as 1, otherwise, it is 0. For e ample, if an LA has no criminal histor prior to the attack, then no criminal histor characteristic has the value of 1, and one offense or multiple offenses will take value 0, since they cannot all be true at the same time. An example of binary coding for a hypothetical LA is given in Figure 1.

PLEASE INSERT FIGURE 1 HERE

The term behavior , hence, is mostly going to refer to the observable actions of the LA.[67] To provide semantic clarity, we first introduce the following temporal terminology on attacker behavior:

Early behavior and characteristics: These behaviors and characteristics do not affect the attack directly; they are behaviors or responses before the attack idea. As such, they include the radicalization process. Examples are prior criminal history, childhood abuse, employment status, etc. Smith[68] considered criminal history as a criterion and assessed if an individual on a radicalization pathway has a prior criminal history or not. However, our aggregate data indicates that some attackers had already integrated criminal activity as a natural part of their lives. Led by our data, we have chosen to distinguish between a lifetime of criminal activity and a one-time offense. Having prior connections to extremist/radical groups is determined as a factor by Gill et al. [69]

In some cases, a triggering event is included in this phase, which causes mostly a personal grievance that results in the attack idea. In other cases, incremental radicalization rouses the attack idea without requiring any triggering incidents. Distal characteristics in the TRAP 18 framework[70] are among the early behavior and characteristics.

Preparatory and precursor behavior and characteristics: These types of behaviors and characteristics are the activities or responses that come with the attack idea, such as acquiring or transporting weaponry and leaking intent. Most studies analyzed the existence of a leakage;[71,72] but we further break down the leakage as online and offline to capture the effect of technology on the attack outcome. Proximal behaviors in the TRAP 18 framework[73] are among the preparatory and precursor behavior and characteristics.

Incident-scene behavior and characteristics: These types of behaviors and characteristics are the activities at the incident scene prior to the attack. Examples include the following: an abnormal trajectory, counter-surveillance related or cycling behavior, wearing suspicious clothing. Incident-scene behavior is analyzed under abnormal or unusual trajectory. Inevitably, information at this detail is not publicly available, since attacks are mostly caught on grainy security footage if at all.

After-attack behavior and characteristics: These types of behaviors and characteristics involve the behavior of the terrorist right after the attack. Some examples are escaping the scene or committing suicide.

The available literature mostly focuses on early, preparatory and after-attack behavior.[74,75]

The first 8 characteristics in the list above involve the attacker's early behavior and characteristics. Having prior criminal records and formal weaponry training are factors that are found to increase the number of casualties.[76] Some LAs even enroll in the formal weapons training units to enhance their attack capabilities.[77] The locus of radicalization also differs among attackers. One LA, who was responsible for 16 bank robberies and two bombings, was radicalized by his parents since childhood, while another was a member of Al-Qaeda. Therefore, while some LAs have prior contacts to terrorist organizations; others have no connections to radical organizations but to radical people. Furthermore, some LAs do not have such connections but are radicalized by their own gaslighting .

The attack decision may stem from a triggering event that can be personal, such as being fired from a job, or social, such as 9/11-attacks.[78] Pre-9/11 LAs are excluded in the analyses because the trigger times are seldom available online. In our database, 99 out of 152 post-9/11 LAs have certain triggering events initiating the attack idea. The

NCJRS database already holds the trigger event data. For the 94 LAs whose data were from the Mother Jones and GTD databases, we gathered information through local and national newspaper archives searching through s nonms for the word trigger in the related context. Any triggering events were not relevant or not found for 24 of the 94 LAs. 4 of the trigger events happened months or years ahead of the attack, besides the exact time of the trigger event was not available. For the remaining LAs, we were able to find the triggering events and their times. We identify trigger events as personal or social, depending on the person affected by it. Out of the 99 LAs who experienced trigger events, 67 of them were triggered by a personal event. Two of these LAs were triggered by multiple personal events. 30 LAs were triggered by a social event. Two LAs were triggered both by a social and a personal event. Personal trigger events are broken down in Table 1.

PLEASE INSERT TABLE 1 HERE

Leakage is also a common trait of attackers; many LAs leak their intent before the actual attack. In one extreme case, an LA posted a 1500-page manifesto on social media the night before the attack.[79] These leaks can be offline through chats, letters, etc.; or online through social media, e-mails, etc. Our definition of online leakage involves cases in which the LA benefits from the Internet to broadcast attack intent; hence, phone calls are considered as offline.

Target selection is another attack characteristic. The targets are civilians in most attacks; however, if the LA fixates on one person who symbolizes the enemy ideology, the attacker may choose to spare others. The target can also be security forces, military, or a formal government official on duty.[80] Most LA attacks are perpetrated with firearms, which are shown to be more deadly.[81] Other weapons include explosives, blades, bodily weapons (hand, feet, etc.), or vehicles (trucks, cars, etc.).

Methodology

LA Classification

Using 9/11 as a cutoff point for understanding recent exacerbation in terrorism, we first compare pre-9/11 and post-9/11 LAs to detect the changes in LA terrorism over time. Then, focusing on post-9/11, we classify LAs in multiple domains. The first domain, offered by Gill et al.,[82] is the ideological classification: Al-Qaeda related LAs, right-wing LAs, and single-issue LAs.

The second classification domain is clustering according to incident-scene behavior. However, incident-scene visuals or data are not publicly available. Serious game design simulating real-world conditions is a suitable surrogate and a widely used approach for the resolution of such predicaments.[83] In the absence of available data, at the Game Research for Information SecuriTy (GRIST) Lab[1] at Rutgers, we have developed a 2D-game where players can imitate the trajectory and target selection of an attacker or the strategy of a defender aiming to catch the attacker. The game considers the effect of human dynamics and crowd flow on target selection. In this game, the attacker moves over a network and knows the density of each adjacent node before he makes his selection to move to another node or stay at the same, or attack (see Figure 2). On the other hand, the defender patrols the network without knowing the exact

[1] http://gursoy.rutgers.edu/GRIST/index.html

location of the attacker. If both players are at the same node, the defender detects the attacker with some probability. Data from playthroughs are collected for each session.

PLEASE INSERT FIGURE 2 HERE

101 game sessions (15 two-people runs, 69 against greedy-AI and 17 against improved AI) are analyzed using simple clustering tools (hierarchical clustering) and results are compared in order to select the best features for clustering. In terms of the attacker, the important classifiers are determined as: i) time of planting the bomb, ii) distance between the attacker and the defender, iii) node's occupancy rank, and iv) node's centrality. In the clustering results, the occupancy rank of nodes has emerged as more important than the actual population itself. According to these features, 5 types of attackers are extracted (Table 2): i) maximum damagers, ii) symbolic attackers, iii) daredevils, iv) attention seekers, and v) stallers.

PLEASE INSERT TABLE 2 HERE

The maximum damagers try to reach a node with the highest population, whereas stallers tend to keep a spiral route and wait for an opportunity to attack a fixed target. Daredevils stay close to the defenders in a risk-seeking manner.

The real-world counterparts of these LA types are derived from the correlations between the game and real-world data. Real-world maximum damagers aim to harm as many people as possible or conduct a series of attacks. Real-world symbolic attackers target a person or a leader that symbolizes the enemy ideology or send a message by attacking with fake weapons. Daredevils directly attack security forces where being successful is highly unlikely or go on a killing spree without a plan; whereas, attention seekers attack central locations at odd hours without intending heavy casualties. Finally, stallers fixate on a location or a person, and plan the attack.

Finally, the third classification domain is in terms of behaviors. In order to obtain behavioral classes, 152 post-9/11 LAs are clustered by a K-Means algorithm. The best results are obtained with 7 clusters with distinct characteristics. Three of these clusters contain a small and insufficient number of LAs, and hence, we will operate on the four clusters involving sufficient number of LAs.

The A-priori Algorithm

The A-priori algorithm was proposed by Agrawal and Srikant,[84] and has been successfully applied to many social problems. Nijkemp et al.[85] implemented it to identify the association rules for the valuation of different biodiversity indicators, while Parack et al.[86] analyzed the relationship between the grading system and attendance in an educational setting. A security-based application of the A-priori algorithm by Nazeri et al.[87] analyzed the relationship between different classes of passengers and safety factors.

In this study, the A-priori algorithm is applied to extract the associations among behavioral and attack characteristics. We present a brief introduction to the methodology and refer the readers to resource[88] for further mathematical details.

For LAs, an association rule of the form $A \rightarrow B$ can be interpreted as If behavior A exists, then behavior B also exists . A rule chain is of the form $A \rightarrow B \rightarrow C$, meaning that If behavior A exists, then behavior B also exists. If behavior B exists, then behavior C also exists .

Let $\mathcal{S}$ be a set of d items, i.e. $\mathcal{S}$ $s , s , \ldots , s$, and $\mathcal{T}$be a set of n transactions in a database, i.e. $\mathcal{T}$ $t , t , \ldots , t$. A transaction involves at least one item. In the LA terrorism setting, the transactions are LAs, and the items are one of the 25 binary characteristics. In our list, a given LA satisfies at least one condition on the list. In our case, d = 25, representing each one of the 25 binary characteristics, and n is 190 for overall LA evaluations, 38 for pre-9/11 LAs, 152 for post-9/11 LAs since it is the number of LAs that are available in each category.

In order to establish an association rule of the form $\boldsymbol{A \rightarrow B}$, item-sets must employ three thresholds to pass: support, confidence, and lift. The support of A is defined as the fraction of transactions involving A, and the support of B is similarly defined. In the LA setting, the support threshold checks if these characteristics are frequent enough to generalize them. If the support exceeds a predetermined threshold, then the characteristics are assumed to be frequent enough.

If A and B are frequent enough, then to be able to claim $\boldsymbol{A \rightarrow B},$ a confidence test is applied. Confidence is the fraction of the transactions that A and B both exist to the transactions that involve only B. In the LA setting, the confidence is the fraction of number of LAs who also have the characteristic A among LAs who have the characteristic B. If the confidence exceeds a predetermined threshold, then coincidentally or not, we say A implies B.

Another measure, lift, which is also called the interestingness factor, controls whether this association is coincidental. It compares the number of transactions that A and B are together to the multiplication of the number of transactions that A and B exist marginally. If the number of transactions that A and B are together is higher, then the association is not coincidental, and $\boldsymbol{A \rightarrow B}$.

Another interestingness measure is cohesion, which is a substitute for lift. It uses the entropy concept that measures the disorder or uncertainty in data. While lift controls if A and B together is frequent enough for the rule $\boldsymbol{A \rightarrow B}$, entropy controls whether A is not frequent enough in the absence of B. Then, cohesion is calculated as an inverse measure of entropy. If the cohesion exceeds a predetermined threshold, it can be concluded that A implies B.

Parameter Selection

The literature defines strong associations as rules that hold with a high degree of support and confidence threshold. [89,90] These threshold values are determined as 50% for minimum support and 70% for minimum confidence. If both rules $X \rightarrow Y$and $Y \rightarrow X$ hold, then we say this is a two-way association rule and denote it by $X \leftrightarrow Y$. A strong two-way association rule holds when both X$\rightarrow Y$and $Y \rightarrow X$ exceed a minimum support threshold of 50% and a minimum confidence threshold of 70%. It should be noted that the literature on A-priori association rules mostly implements a minimum support threshold level of 10-15%.[91,92] Because LA events are rare, such rates of the data refers to a number that is insufficient for generalization. Hence, the minimum support threshold is increased to 50%. The minimum support and minimum confidence threshold values are determined by tuning in a way that provides sufficient data while leading to important association rules.

The A-priori algorithm parameters (support and confidence) aim to balance generating non-significant association rules (type 1 error) and missing significant ones (type 2 error).[93] In our case, the minimum confidence threshold is 0.7, which is relatively low. Such a confidence level avoids missing significant rules, at the expense of producing non-significant ones A further statistical test is required to determine its significance once a rule is constructed in the form of $\boldsymbol{A \rightarrow B}$. This test has the null hypothesis that A and B are independent. In order to check independence, the number of occurrences of A and B are compared to the expected number of occurrences when they are independent. If the null hypothesis is rejected, then a proof for the associations has been found.

Chain Rules (R-Rules)

An R-rule, also known as a rule of rules, is a hyper-rule in the form $A \rightarrow B \rightarrow C \rightarrow D$. An association chain is a special type of R-rule in the form ($A \rightarrow B \rightarrow B \rightarrow \cdots$ ... $\rightarrow$ ... $\rightarrow$ or $\rightarrow \quad \rightarrow \cdots \rightarrow$. In other words, an association chain is a statistically significant aggregation of association rules in the form of $\rightarrow \quad \rightarrow \cdots \rightarrow$.

The statistical significance of an R-rule is measured by cohesion.[94] While the item-wise cohesion measure checks whether A does not occur frequently enough without B, the rule-wise cohesion measure uses the cohesion for if $A \rightarrow B$, $B \rightarrow C$, and $A \rightarrow C$ hold.

It should be noted that an association rule does not signify a cause-effect relationship, or an indisputable certainty, but rather an uncoincidental indicative relationship in LA behaviors. Moreover, the algorithm may produce intuitive results such as If the attacker uses firearms, then there are fatalities . Such intuitive results are used to check the consistency of the rules and provide guidance for parameter selection. It is also likely that the algorithm provides associations inverse in time. A behavior later in the timeline may be associated with a former behavior. Such rules cannot be used in predicting the LA behavior in time but can provide a traceback view on the LA s history. Due to the excess number of rules, only strong rules are emphasized in the text, but figures also present weaker association rules.

Association Rules for LA Behavior

The following subsections present the outputs of the A-priori algorithm results. In the next subsection, we provide the A-priori algorithm results for all 190 LAs in the database, and the following section compares pre- and post-9/11 LAs to display the temporal change in LA characteristics. Bakker and de Graaf[95] conclude that LAs yield more common characteristics when analyzed by their ideologies. Referring to this study, next, we analyze LAs according to their ideological motivations. We also compare these results to incident-scene-based classification and behavior-based classification.

Overall Evaluations

Analyzing 190 LAs over 60 years, we have found the following most common characteristics:

62.1% required a triggering event,

62.1% targeted civilians,

59.5% committed their attacks using firearms,

52.1% had no prior connections to extremist/terrorist people,

51.0% of LA attacks were fatal.

The overall analysis of 190 LAs produce few common characteristics and none belonging to the early behavior stage. Hence, these common characteristics are not viable in capturing the early signs of an LA. Figure 3 displays the associations among common characteristics found by the A-priori algorithm. These results are:

One strong two-way association emerges: the usage of firearms implies fatalities, and vice versa.

Only two strong one-way associations are available for all LAs.

- Usage of firearms implies a triggering event.
- Fatalities imply civilian targets.

PLEASE INSERT FIGURE 3 HERE

Even though some commonalities can be identified, the face of LAs has changed significantly over time. To capture these changes, we will first compare pre-9/11 LAs to post-9/11 LAs.

Comparison of Pre-9/11 and Post-9/11 LAs

Analyzing all LAs has yielded sparse relationships, as shown in the previous section. One reason for this sparsity is that the triggers, technologies, opportunities, and other conditions that lead an LA to an attack have changed significantly over the years. Hence, in this subsection, we compare the associations for pre-9/11 and post-9/11 LAs. The database holds 38 LAs before 9/11, and 152 LAs after 9/11 and the A-priori algorithm was separately applied to these two data sets. We present the associations for both eras in Figure 4. The density of gray-shaded cells indicates that pre-9/11 LAs had more common characteristics than post-9/11 LAs. In the following subsections, we delve deeper into both time periods and present the results of the A-priori algorithm results.

PLEASE INSERT FIGURE 4 HERE

Associations in the pre-9/11 era

We have found the following most common characteristics:

81.6% of the pre-9/11 LAs used firearms in their attacks.

76.3% of the pre-9/11 LA attacks were fatal.

68.3% of the pre-9/11 LAs had a triggering event that led to attack idea.

65.8% of the LAs leaked intent offline.

65.8% of the LAs were not self-radicalized.

63.2% of the LAs had prior contacts with extremist or terrorist groups.

The algorithm produces eight strong two-way associations (Figure 4a):

The existence of a triggering event implies the usage of firearms, and vice versa.

Having prior contacts to extremist/terrorist groups implies not being self-radicalized, and vice versa.

The existence of a triggering event implies offline leakage, and vice versa.

Not being self-radicalized implies a trigger event, and vice versa.

Not being self-radicalized implies the usage of firearms, and vice versa.

Civilian targets imply fatalities, and vice versa.

The usage of firearms implies fatalities, and vice versa.

Strong one-way associations are:

Having prior contacts to extremist/terrorist groups is implied by being able to escape from the crime scene.

The existence of a triggering event and the usage of firearms are implied by any of the following: having prior contacts to extremist/terrorist groups, offline leakage, targeting a person who symbolizes an enemy ideology, being able to escape from the crime scene.

Offline leakage is implied by targeting a person who symbolizes an enemy ideology.

Fatalities are implied by having prior contacts to extremist/terrorist groups, offline leakage, targeting civilians or a person who symbolizes an enemy ideology, being able to escape from the crime scene.

Associations in the post-9/11 era

In this era, the LA attack types and modi operandi have diverged, and as a result, there is only one common characteristic: 60.5% of the LAs experienced a triggering event that led to the attack idea.

Interestingly, no strong two-way associations are obtained for this time period and as can be seen from Figure 4b; only one strong one-way association exists for post-9/11 LAs: The usage of firearms implies a triggering event.

Comparison of Pre-9/11 and Post-9/11 LAs

The common characteristics and the associations show that pre-9/11 LAs had more connections to extremist/terrorist people than post-9/11 LAs. This indicates that while violence once was a means chosen by people living around extremists, it has now trickled down to people without any radical connections. This result also holds for formal weapons training (military or otherwise); 47% of pre-9/11 LAs had formal weapons training, 22% of post-9/11 LAs did, indicating that terrorism has spread into the realm of ordinary civilians more and more. Furthermore, LA terrorism has become more diverse in preparatory behavioral characteristics. While both pre- and post-9/11 LAs target civilians more, the rate of targeting other groups has significantly risen. The rate of targeting law enforcement and government officials has increased from 13% to 29%. Similarly, the usage of firearms has dropped from 89% to 53%. Post-9/11 LAs weapon choices vary from explosives to hatchets, machetes, or personal vehicles.[96] The variety in target and weapon selection has led to varieties in the aftermath of the attack. While pre-9/11 attacks had a higher fatal attack rate (76%), post-9/11 LAs commit less fatal attacks (47%). However, the number of fatalities per attack does not exhibit statistically significant differences. On the contrary, the standard deviation in the number of fatalities has more than doubled for post-9/11 LAs (from 3.60 to 8.43); meaning that, while the number of unsuccessful attacks has increased due to sting operations or improved technology, post-9/11 LAs have caused more mass casualty than pre-9/11 LAs. The rate of escapes after the attack has significantly decreased while the rate of suicides/killings has increased due to technological advances. For example, in 2016, the police killed an attacker with a remote-controlled bomb disposal robot, which was the first time a robot was used to subdue a terrorist.[97]

Evaluations regarding attacker motivation

As stated by Bakker and de Graaf[98], classifying LAs into three ideological segments (Al-Qaeda related LAs, right-wing LAs, single-issue LAs) produces numerous distinct characteristics. In our data, these three groups hold 88% of the post-9/11 LAs. Grouping LAs according to their ideology reveals more similarities and stronger associations (see Figure 5). Among the 152 post-9/11 LAs, 40 are Al-Qaeda related LAs, 58 are right-wing LAs, and 36 are single-issue LAs. Table 3 presents all common characteristics, strong two-way and one-way associations for each ideological class.

PLEASE INSERT FIGURE 5 HERE
PLEASE INSERT TABLE 3 HERE

According to this classification, right-wing LAs are more diverse in behavior, and Al-Qaeda related LAs are the least diverse. While Al-Qaeda related LAs are not necessarily triggered or self-radicalized, right-wing LAs require a triggering event and are mostly self-radicalized.

As can be seen from Table 3, when the group of interest is heterogeneous, the analysis merely produces intuitive rules without valuable knowledge. Observing only such rules indicate that further classification schemes are necessary. This observation validates our attempt on behavioral clustering to obtain stronger association rules.

Evaluations regarding incident-scene behavior

Given that ideological classification has not provided distinct behavioral characteristics, another perspective becomes necessary. Such a classification also allows us to evaluate the reflection of incident-scene behavior in early, preparation, and after-attack behaviors and characteristics. Out of 152 post-9/11 LAs, 54 of them are maximum damagers, 37 are symbolic attackers, 27 are daredevils, 27 are attention seekers, and 7 are stallers. The characteristics of each type are presented in Table 4. Since the data for stallers are statistically insufficient for analysis, we will focus on the other four groups to investigate associations. The results of the A-priori algorithm are presented in Figure 6 and Table 5.

PLEASE INSERT TABLE 4 HERE
PLEASE INSERT FIGURE 6 HERE
PLEASE INSERT TABLE 5 HERE

Symbolic attackers and daredevils reveal many similarities and associations; however, maximum damagers are diverse and do not yield many associations. The main reason is that some maximum damagers choose to spare people who support their ideologies rather than harming everyone.

Evaluations regarding behavioral clusters

This classification method attempts to maximize the common characters in behaviors. For this reason, the K-Means clustering algorithm is applied to 152 post-9/11 LA data points. K-Means algorithm requires a predetermined number of clusters. To verify the clustering results, we have used the C-Index.[99] In our trials, seven clusters produce the smallest C-Index value. However, three of these clusters only contain outliers and do not provide sufficient data. Hence, we will proceed with four behavioral characteristic clusters.

PLEASE INSERT TABLE 6 HERE

Table 6 shows the distinctive characteristics of each cluster. A triggering event appears as a characteristic for three clusters, and leakage is a common characteristic for one of the clusters. Noticeable similarities are found between the incident-scene-based and behavior-based classification (see Table 7). More than half of the first and the fourth clusters are composed of maximum damagers. 55% of the LAs in the first cluster are maximum damagers. The LAs in this cluster target civilians, use firearms and have high fatality rates. 61% of the fourth cluster is also composed of maximum damagers. The stories and backgrounds of these maximum damagers show that the first cluster contains LAs with a me vs. them mentality and the fourth cluster contains LAs with an us vs. them mentality. An LA with a me vs. them mentality sees every civilian as a target; whereas, an LA with an us vs. them mentality wants to spare people with their own ideologies and only target civilians from other ideologies. Furthermore, having a me vs. them mentality increases the fatality rate. An interesting result is that most "us vs. them" maximum damagers have prior contacts to extremist groups and are not self-radicalized. 67% of the second cluster is composed of self-radicalized symbolic attackers and attention seekers. It also shows some similarity to symbolic attackers who are the majority compared to other incident-scene types (48%). They mostly have no prior extremist connections and use other weapons than firearms. This cluster mostly exhibits no triggering event and no leakage. Fortunately, their attacks are mostly not fatal. Slightly less than half of the third cluster (43%) is composed of daredevils. Since their actions are not well-planned, their attacks are likely to fail, and their arrest rate is high. They target law enforcement and government officials using firearms. They do not leak intent since the duration between the trigger event and the attack is, in general, too short.

Table 8 shows the ideological tendencies of each cluster. While the first two clusters have a majority of right-wing terrorists, the third cluster (mostly daredevils) is diverse in terms of ideology. Finally, the last cluster (us vs. them ' maximum damagers) is almost equally dominated by Al-Qaeda related and right-wing terrorists. The algorithm results of these clusters are presented in Table 9 for clusters 1 and 2, and in Table 10 for clusters 3 and 4. Figure 7 also presents the associations between each characteristic.

PLEASE INSERT TABLE 7 HERE
PLEASE INSERT TABLE 8 HERE
PLEASE INSERT FIGURE 7 HERE
PLEASE INSERT TABLE 9 HERE
PLEASE INSERT TABLE 10 HERE

Association Chains

In this section, we extract chain rules. A chain rule is a chain of associations that satisfy a cohesion threshold level of 70% and an overall minimum confidence threshold level of 70% given an initial node. Each node represents a behavior or an attack characteristic and is filled with a color code indicating chronological occurrence. The color codes for the timeline are presented in Figure 8. Finally, two-way arrows indicate that if the nodes on each edge of a two-way arrow are interchanged, the chain still satisfies the aforementioned conditions.

PLEASE INSERT FIGURE 8 HERE

Overall evaluation of LAs and post-9/11 LAs do not exhibit any association chains due to data being too heterogeneous. Similarly, ideological classification has not revealed any association chains either. Figure 9 presents the chains for pre-9/11 LAs. The central theme for pre-9/11 LAs is not being self-radicalized, fatalities, and the usage of firearms.

PLEASE INSERT FIGURE 9 HERE

Among the incident-scene behavior-based classification, maximum damagers and attention seekers do not yield any chains. However, the chains for symbolic attackers and daredevils are given in Figure 10 and Figure 11.

PLEASE INSERT FIGURE 10 HERE
PLEASE INSERT FIGURE 11 HERE

While symbolic attackers are mostly self-radicalized, their attacks do not necessarily aim to kill. Hence, low casualty appears as the central theme. Daredevils, however, are mostly not self-radicalized and do not generally leak intent because their attacks are the most impulsive ones. They either target the law enforcement face-to-face or exhibit violence immediately when triggered, and their attacks are mostly fatal.

The behavior-based classification has revealed longer, statistically more robust chains compared to other classification schemes. The association chain for Cluster 1 is presented in Figure 12. This group includes more ordinary people who may not be considered threatening. They have no prior criminal history or prior contacts to other extremist, radical, or terrorist groups. However, after a trigger, their grievance induces an armed attack intent. Consequently, the fatality rate of their attacks is high. Cluster 1 is the only group that mostly leaks intent online. Hence, they leave their writeprints .

PLEASE INSERT FIGURE 12 HERE

Figure 13 exhibits the association chain for Cluster 2. The attackers in this cluster do not usually use firearms. They are self-radicalized and have no prior contacts to other extremist or terrorist groups. They experience a triggering event similar to the ones in Cluster 1; however, unlike Cluster 1, they do not leak intent. They mostly target civilians.

PLEASE INSERT FIGURE 13 HERE

Figure 14 demonstrates the association chain for Cluster 3. This cluster exhibits similar behavior to daredevils; their targets are the law enforcement or government officials, and they use firearms. They are mostly arrested after the attack. While no leakage' is an important characteristic of this cluster, a trigger event is not prominent.

PLEASE INSERT FIGURE 14 HERE

Figure 15 displays the association chain for Cluster 4. The LAs in this cluster are not subjected to a trigger event and have no prior criminal history. In contrast to Cluster 2, they have prior contacts to other extremist or terrorist groups and are not self-radicalized. However, similar to Cluster 2, they choose weapons other than firearms; hence, the rate of fatal attacks is low.

PLEASE INSERT FIGURE 15 HERE

Temporal Associations

Among behavioral characteristics, online leakage and trigger events are important and traceable milestones on the pathway to an attack. In this section, we will provide the statistical properties between these milestones for each LA type. The most prominent landmark is the trigger event and its timing.

72 of the 99 triggering events have the exact dates. 24 attacks have the exact week, two of them have the month and four of them have the year. In the statistical analyses, we have used the day and the week data because month and year information assumptions largely affect the results. The statistical properties of the duration between the trigger event and the attack are given in Table 11. Even though the association rules and chains hold, the temporal deviations between the trigger event and the attack are very large.

PLEASE INSERT TABLE 11 HERE

Another important landmark is the leakage, but only one attacker type has leakage as a prominent characteristic. Cluster 1 has scored high on online leakage. In this group, 20 exact leakage dates are found and the mean between leakage and attack is 60 days with a large standard deviation of 87 days. Despite the large standard deviation, the median time span between the leakage and the attack is 7 days, meaning that 50% of LAs attack within a week after the leakage.

Intervals between the landmarks show a vast variation; all groups have high coefficient of variation and the duration cannot be generalized within groups. Another question is whether these durations are related to the rate of fatal attacks. Non-fatal attacks have an average of 115 days with a standard deviation of 234.7 days between the trigger and the attack, whereas fatal attacks have an average of 141 days with a standard deviation of 234.8 days between the trigger and the attack. A t-test comparing these groups yields a p-value of 0.63, which indicates that fatal and non-fatal attacks do not have a significant difference between their trigger-attack durations. Another comparison between fatal and non-fatal attacks has been made in terms of the duration between leakage and attack times. Non-fatal attacks have an average of 44 days with a standard deviation of 53.4 days between the leakage and the attack, whereas fatal attacks have an average of 36 days with a standard deviation of 64.2 days between the trigger and the attack. A t-test comparing these groups yields a p-value of 0.711, which indicates no significant difference between leakage and fatality.

Despite the large standard deviations of temporal difference between mileposts, medians provide valuable insights. Almost 50% of the LAs attack in a month after the trigger. Even though daredevils are more impulsive than other types, attention seekers have a much smaller median, that is, 50% of attention seekers attack in less than 5 days after the trigger. Likely, 50% of Group 2 (mostly consisting of symbolic attackers and attention seekers) attacks less than a week after the trigger. One important remark is maximum damagers have longer duration than any other group; hence, it can be argued that a high fatality rate requires longer attack preparation time.

Conclusions and Future Work

The number of attacks by individuals has been more frequent than ever over the last two decades, making LA terrorism one of the most accelerating man-made threats, especially in the US. As a result, there is a need for academic work to understand LA behavior and characteristics. While LA behavior has been studied qualitatively and quantitatively, the associations and connections between those behavioral characteristics have not been analyzed in a temporal manner for an attempt to intervene at the right time.

In this a-posteriori analysis, distal and proximal characteristics of LAs are analyzed together with attack characteristics and after-attack behaviors. To provide clarity on the term behavior , we have defined four temporal behavior phases: early behavior, preparatory behavior, incident-scene behavior, and after attack behavior. The results indicate that while pre-9/11 LAs had prior contacts to extremist/radical groups and mostly radicalized by the people in their environment, post-9/11 LAs are more diverse. The most noticeable change we have found is that LA terrorism has trickled down to people who do not have prior connections, and the weapon of choice has diverged greatly.

Besides ideological classification, we introduce two new classifications of LAs: incident-scene-based and behavior-based classification. The incident-scene-based data provides five types of attackers: maximum damagers, symbolic attackers, daredevils, attention seekers, and stallers. Behavior-based classification further divides maximum damagers to me vs. them and us vs. them types. Through behavior-based classification, we are able to understand the evolution process of an LA attacker by generating association chains.

Triggering event and leakage are traceable characteristics if they have online writeprints . However, the durations between triggering event and attack, or the durations between leakage and attack, have high standard deviations for each LA type. Moreover, these durations do not have a statistically significant effect on fatal attack rates. While the median provides a month between the trigger and the attack, and a week between the leakage and the attack, further analysis that minimizes the variance is required for connecting behaviors and characteristics to the attack timeline.

The capabilities and intentions of an attacker depend on their type. One aspect of these a-posteriori analyses is to support assessment tools such as TRAP 18 via the following results: (1) if an online leakage to a wide audience is made, the indicated attack is more likely to be a maximum-damage type with firearms to civilian targets that might result in a high number of fatalities. Most attackers leak intent at a time when preparations come to a close; (2) if there is no trigger event, then incrementally developing an attack idea might be a possible gaslighting by the extremist/terrorist connections of the attacker. It is more probable that the attack does not involve firearms in this case; (3) an attack employing firearms without any leakage is most probably aimed at law enforcement. In light of these findings, our further focus will be on high fatality attacks with leakage. We plan to focus our future studies on developing algorithms for tracing signals of attack preparation, and weak signals of online trigger and leakage statements.

Notes

[1] Gary LaFree, and Joshua D. Freilich, " Bringing Criminology into the Study

of Terrorism," in The Handbook of Criminology of Terrorism, ed. Gary LaFree, and Joshua D. Freilich, (West Sussex, Wiley-Blackwell, 2017), 3-14.

[2] Ramon Spaaij, The enigma of lone wolf terrorism: An assessment, Studies in Conflict & Terrorism 33, no. 9 (2010): 854 870.

[3] John Hinkson, Learning from Las Vegas, Arena Magazine 150, (2017): 5 6.

[4] Natasha Quek, Growing Threat of White Supremacists, (RSIS Commentaries. Singapore: Nanyang Technological University, 2019), 4.

[5] Rafaello Pantucci, Claire Ellis, and Lorien Chaplais, Lone-Actor Terrorism Literature Review , Countering Lone-Actor Terrorism Series No. 1, (Royal United Service Institute for Defense and Security Studies, 2015).

[6] Spaaij, Enigma , 856. (see Note 2 above).

[7] Paul Gill, John Horgan, and Paige Deckert, Bombing alone: Tracing the motivations and antecedent behaviors of lone-actor terrorists, Journal of Forensic Sciences 59, no. 2 (2014): 425 435.

[8] Spaaij, Enigma , 856. (see Note 2 above).

[9] Gill, Horgan, and Deckert, Bombing Alone , 434.

[10] Joel Brynielsson, Andreas Horndahl, Fredrik Johansson, Lisa Kaati, Christian Mårtenson, and Pontus Svenson, Harvesting and anal sis of weak signals for detecting lone wolf terrorists, Security Informatics 2, no. 1 (2013): 1-11.

[11] Raffaello Pantucci, A Tpolog of Lone Wolves: Preliminar Anal sis of Lone Islamist Terrorists, (The International Centre for the Stud of Radicalisation and Political Violence: 2011) 39.

[12] Edwin Bakker, and Beatrice De Graaf, Preventing lone wolf terrorism: Some CT approaches addressed, Perspectives on Terrorism 5, no. 5 6 (2011): 43-50.

[13] Br nielsson, Horndahl, Johansson, Kaati, Mrtenson, and Svenson, Harvesting and anal sis, 3.

[14] J. Reid Meloy, Jend Hoffmann, Angela Guldimann, and David James, The role of warning behaviors in threat assessment: An e ploration and suggested t polog, Behavioral Sciences & the Law30, no. 3 (2011): 256 279.

[15] Bakker, and de Graaf, Preventing, 47.

[16] Daveed Gartenstein-Ross, Radicali ation: Social media and the rise of terrorism, (Hearing before the US House of Representatives Committee on Oversight and Government Reform, Sub- committee on National Security, 2015) 28.

[17] Ramon Spaaij, Understanding Lone Wolf Terrorism: Global Patterns, Motivations and Prevention (Dohdrecht: Springer Netherlands), 41.

[18] Bakker and de Graaf, Preventing, 47.

[19] Melo, Hoffman, Guldimann, James, Role of warning, 265.

[20] J. R. Meloy, TRAP-18: Terrorist Radicalization Assessment Protocol User Manual Version 1.0. (Washington, DC: Global Institute of Forensic Research 2017).

[21] J. Reid Meloy, Alasdair M. Goodwill, M.J. Meloy, Gwyn Amat, Maria Martinez, and Melinda Morgan, Some TRAP-18 indicators discriminate between terrorist attackers and other subjects of national securit concern Journal of Threat Assessment and Management 6, no. 2 (2019): 93-110.

[22] Br nielsson, Horndahl, Johansson, Kaati, Mrtenson, and Svenson, Harvesting and anal sis, 1.

[23] Meloy, Hoffman, Guldimann, James, Role of warning, 270.

[24] Br nielsson, Horndahl, Johansson, Kaati, Mrtenson, and Svenson, Harvesting and anal sis, 11.

[25] Ibid.

[26] Nurhashikin Mohd Salleh, Siti Rahayu Selamat, Zurina Saaya, Rabiah Ahmad, and Zaki Mas d, Identifying Cyber Violent Extremism (Cyber-VE) Components by Exploring Dark Web , International Journal of Computer Science and Information Security 14, no.9 (2016): 52-61.

[27] Roger A. Bates, Dancing with wolves: Toda s lone wolf terrorists, The Journal of Public and Professional Sociology 4, no. 1 (2012): 1 14.

[28] Pantucci, Tpolog, 14-32.

[29] Bates, Toda , 5-7.

[30] Gill, Horgan, and Deckert, Bombing Alone , 426.

[31] Reid J. Melo and Paul Gill, The lone-actor terrorist and the TRAP-18, Journal of Threat Assessment and Management 3, no. 1 (2016): 37 52.

[32] Bakker, and de Graaf, Preventing, 3-4.

[33] Arie Perliger and Ami Pedahur, Social network anal sis in the stud of terrorism and political violence, PS: Political Science and Politics 44, (2011): 45 50.

[34] Ze Li, Duoong Sun, Bo Li, Zhanfeng Li, and Aobo Li, Terrorist group behavior prediction by wavelet transform- based pattern recognition, Discrete Dynamics in Nature and Society, (2018): 1 16.

[35] Br nielsson, Horndahl, Johansson, Kaati, Mrtenson, and Svenson, Harvesting and anal sis, 9.

[36] Spaaij, Enigma , 858.

[37] Peter J. Phillips, Lone wolf terrorism, Peace Economics, Peace Science and Public Policy 17, no. 1, (2011): 1-29.

[38] Ibid, 17.

[39] Theodore J. Gordon, Yair Sharan, and Eli abeth Florescu, Prospects for LoneWolf and SIMAD terrorism, Technological Forecasting and Social Change 95, (2015): 234-251

[40] Brian J. Phillips, Deadlier in the U.S.? On Lone Wolves, Terrorist Groups, and Attack Lethalit . Terrorism and Political Violence 29, no: 3 (2015): 533-549.

[41] Claire Ellis, Raffaello Pantucci, Jeanine de Roy van Zuijdewijn, Edwin Bakker, Benoît Gomis, Simon Palombi, and Melanie Smith, Lone-Actor Terrorism, (Roal United Service Institute for Defense and Security Studies, 2017).

[42] Ibid.

[43] Br nielsson, Horndahl, Johansson, Kaati, Mrtenson, and Svenson, Harvesting and anal sis, 3-10.

[44] J. M. Post, Individual and group dnamics of terrorist behavior, in Psychiatry: The State of the Art Volume 6 Drug Dependence and Alcoholism, Forensic Psychiatry, Military Psychiatry, ed. P. Pichot, P. Berner, R. Wolf, and K. Thau, (Boston, MA: Springer US, 1985): 381 386.

[45] Mark S. Hamm and Ramon Spaaij, The Age of Lone Wolf Terrorism. (New York: Columbia University Press, 2017). 23.

[46] Hamm and Spaaij, Age , 23

[47] Global Terrorism Database. https://www.start.umd.edu/gtd/. Accessed: 2019-07-03.

[48] Mother Jones. https://www.motherjones.com/politics/2012/12/ mass-shootings-mother-jones-full-data/. Accessed: 2019-06-22.

[49] Jason R. Silva, and Emily Ann Greene-Colo i, Fame-seeking mass shooters in America: Severit , characteristics, and media coverage, Aggression and Violent Behavior 48, (2019): 24 35.

[50] Meloy and Gill, TRAP-18, 38-39.

[51] Meloy, Goodwill, Meloy. Amat, Martine , and Morgan, Some TRAP-18 indicators , 100.

[52] Hamm and Spaaij, Age , 23

[53] Lasse Lindekilde, Francis OConnor, and Bart Schuurman, Radicalization patterns and modes of attack planning and preparation among lone-actor terrorists: an exploratory analysis , Behavioral Sciences of Terrorism and Political Aggression 11, no: 2, (2019): 113-133.

[54] Richard Berk, Heidari Hoda, Jabbari Michael Kearns, and Aaron Roth. Fairness in Criminal Justice Risk Assessments: The State of the Art Sociological Methods & Research, (2018).

[55] Indr liobait Measuring discrimination in algorithmic decision making Data Mining and Knowledge Discovery 31 (2017):1060-1089.

[56] Hamm and Spaaij, Age , 23

[57] Br nielsson, Horndahl, Johansson, Kaati, Mrtenson, and Svenson, Harvesting and anal sis, 1-11.

[58] Bakker and de Graaf, Preventing, 2-4.

[59] Phillips,   Lone-wolf , 17.

[60] Meloy and Gill, TRAP-18, 38-39.

[61] Gill, Horgan, and Deckert, Bombing Alone , 430-432.

[62] Michael Tierne , Spotting the lone actor: Combating lone wolf terrorism through financial investigations, Journal of Financial Crime 24, no. 4 (2017): 637 642.

[63] McCaule and Moskalenko, A profile of lone wolf terrorists , 70-75.

[64] Spaaij, Enigma , 856.

[65] Spaaij, Understanding, 3-7.

[66] Allison Smith, Risk Factors and Indicators Associated with Radicalization to Terrorism in the United States: What Research Sponsored by the National Institute of Justice Tells Us (National Institute of Justice, June 2018).

[67] Soheil Eshghi, Grace-Rose Williams, Gualtiero B. Colombo, Liam D. Turner, David G. Rand, Roger M. Whitaker, and Leandros Tassiulas, Mathematical models for social group behavior,   in 2017 IEEE SmartWorld, Ubiquitous Intelligence Computing, Advanced Trusted Computed, Scalable Computing Commu- nications, Cloud Big Data Computing, Internet of People and Smart City Innovation (Smart-World/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), (2017): 1 6.

[68] Smith, Risk Factors , 7.

[69] Gill, Horgan, and Deckert, Bombing Alone , 430-432.

[70] Meloy and Gill,   TRAP-18, 38-39.

[71] Br nielsson, Horndahl, Johansson, Kaati, Mrtenson, and Svenson, Harvesting and anal sis, 1-11.

[72] Meloy and Gill, TRAP-18, 38-39.

[73] Ibid.

[74] Br nielsson, Horndahl, Johansson, Kaati, Mrtenson, and Svenson, Harvesting and anal sis, 1-11.

[75] Bakker and de Graaf, Preventing, 2-4.

[76] Claire Ellis, Raffaello Pantucci, Jeanine de Roy van Zuijdewijn, Edwin Bakker, Melanie Smith, Benoît Gomis, and Simon Palombi., Anal   sing the processes of lone-actor terrorism: Research findings, Perspectives on Terrorism 10, no. 2, (2016): 33 41.

[77] Joel A. Capellan, Lone wolf terrorist or deranged shooter? a stud of ideological active shooter events in the United States,   Studies in Conflict & Terrorism 38, no. 6 (2015): 395 413.

[78] Hamm and Spaaij,   Age , 25.

[79] Brynielsson, Horndahl, Johansson, Kaati, Mrtenson, and Svenson, Harvesting and anal sis, 9.

[80] Michael Becker,   Eplaining lone wolf target selection in the United States, Studies in Conflict & Terrorism 37, no. 11 (2014): 959 978.

[81] Ellis, Pantucci, van Zuijdewijn, Bakker, Smith, Gomis, Palombi, Anal   ing the processes, 35.

[82] Gill, Horgan, and Deckert, Bombing Alone , 431.

[83] Bill Roungas,Alexander Verbraeck, and Sebastiaan Meijer,   The future of contextual knowledge in gaming simulations: A research agenda, in 2018 Winter Simulation Conference (WSC), (2018): 2435 2446, Dec 2018.

[84] R. Agrawal and R. Srikant,   Fast algorithms for mining association rules in large databases, in *Proceedings of the 20th International Conference on Ver Large Data Bases, VLDB 94,* (San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 1994) 487 499.

[85] Peter Nijkamp, Gabriella Vindigni, and Paulo A.L.D. Nunes   Economic valuation of biodiversit : A comparative stud, Ecological Economics 67, no. 2, (2008): 217   231.

[86] Suhem Parack, Zain Zahid, and Fatime Merchant, Application of data mining in educational databases for predicting academic trends and patterns, in 2012 IEEE International Conference on Technology Enhanced Education (ICTEE), (2012): 1-4.

[87] Zohreh Nazeri, Eric Bloedorn, and Paul Ostwald, Eperiences in mining aviation safet data, in *SIGMOD 01*, (2001).

[88] R. Agrawal and R. Srikant, Fast algorithms for mining association rules in large databases, in *Proceedings of the 20th International Conference on Ver Large Data Bases, VLDB 94,* (San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 1994) 487 499.

[89] Ke Luo, and Jie Wu, A new method to mine valid association rules, in 2003 International Conference on Machine Learning and Cybernetics 1, (2003): 88-93.

[90] Binay Singh, and Abhijit Mustafi, A novel approach to rank association rules using genetic algorithm, International Journal of Current Engineering and Technology 4, no:2 (2003): 850-859..

[91] K.N.V.D. Sarath and Vadlamani Ravi, Association rule mining using binar particle swarm optimi ation, Engineering Applications of Artificial Intelligence 26, no. 8, (2013): 1832 1840.

[92] Zhang Danping and Deng Jin, The data mining of the human resources data warehouse in universit based on association rule, Journal of Computers 6, no. 1 (2011): pp. 1832 1840.

[93] Wilhelmiina Hämäläinen, and Matti Nykänen, Efficient discover of statisticall significant association rules, in 2008 Eighth IEEE International Conference on Data Mining, (2008): 203 212.

[94] R. Gras and P. Kunt , Discovering r-rules with a directed hierarch, Soft Computing 10, (2006): 453 460.

[95] Bakker, and de Graaf, Preventing, 47.

[96] Hamm and Spaaij, Age , 23

[97] Jeffrey William Lewis, The human use of human beings: Suicide bombing, technological innovation, and the asmmetr of modern warfare, Global Politics Review 2, no. 2, (2015): 9 27.

[98] Bakker, and de Graaf, Preventing, 47.

[99] Lawrence J. Hubert and Joel R. Levin, A general statistical framework for assessing categorical clustering in free recall, Psychological Bulletin 83, no. 6 (1976): 1072 1080.

Personal Event	Frequency
Separating from partner/wife/family	13
Losing job or dropping out of school	10
Mental/physical health problems	8
Arrest-related issues	6
News / poster / graffiti / newspaper irritation	5
Sting operations	5
Rejection by friends / colleagues / other people	4
Financial or social security problems	3
Eviction / homelessness	3
Fight with neighbors	3
Denied applications	2
Deployment as an army member	2
Travel	2
Online discussions	1
Unreturned calls	1
Gaslighted by partner	1

Table 1. Personal Trigger Events and Their Frequencies

	Centrality		High Population		Avoids being caught		Fixated on a location	
	Aims for central locations	Avoids central locations	Aims for highly populated areas	Avoids highly populated areas	Risk-seeking	Risk-averse	Will wait for an opportunity	May substitute location
Maximum Damagers	✓		✓			✓		✓
Symbolic attackers		✓		✓		✓		✓
Daredevils	Both				✓			✓
Attention seekers	✓			✓		✓		✓
Stallers	✓		✓			✓	✓	

Table 2. LA-types using incident-scene behavior obtained from the playable game.

	Common Characteristics	Strong two-way associations	Strong one-way associations
Al-Qaeda related LAs (Figure 4a)	67.5% do not leak the attack intent. 62.5% choose weapons other than firearms as the means of attack (mostly explosives). 70% target civilians. Together with the law enforcement targets, they make up 97% of jihadist LAs' targets. Half of the jihadist LAs are not self-radicalized and half of them do not need a triggering event for to exhibit attack intent.	Having prior contacts to extremist/terrorist groups implies not being self-radicalized, and vice versa.	Civilian targets are implied by no fatalities after the attack or no intent leakage. No injuries/fatalities after the attack are implied by being arrested at the crime scene. Being arrested at the crime scene is implied by not being self-radicalized.
Right-wing LAs (Figure 4b)	84.4% of the right-wing LAs target civilians. 70.7% of the right-wing LAs require a triggering event for the attack intent.		Civilian targets are implied by not having prior contacts to extremist/terrorist groups. A triggering event is implied by either not having prior contacts to extremist/terrorist groups or usage of firearms.
Single-issue LAs (Figure 4c)	72.2% of these single-issue LAs have no prior contacts to extremist/terrorist groups or people. 61.1% of these LAs require a traumatic triggering event to intend the attack.	Usage of firearms implies law enforcement/government official targets, and vice versa.	Not having prior contacts to extremist/terrorist groups is implied by either law enforcement/government official targets or usage of firearms. Law enforcement/government official targets also imply the existence of a trigger event or no intent leakage.

Table 3. A-priori algorithm results for ideological classification. Common characteristics are the properties that are valid for at least 50% of the class. Strong two-way and one-way associations are rules that have a confidence of at least 70% and a lift of at least 1.

Clusters	Prior Contacts to Extremists	Trigger Event	Leakage	Weapon choice	Target Selection	Fatalities
Maximum damagers	-	-	-	-	Civilians	High
Symbolic Attackers	None	Yes	-	Other than firearms	-	None/Low
Daredevils	-	Yes	None	Firearms	Law enforcement/ government officials	High
Attention seekers	-	-	None	-	Civilians	None/Low

Table 4. Class comparisons for incident-scene behavior

	Common Characteristics	Strong two-way associations	Strong one-way associations
Maximum Damagers (Figure 5a)	92.5% target civilians. 61.1% of the attacks are fatal.	The usage of firearms implies fatalities, and vice versa.	Not having prior contacts to extremist/terrorist groups implies civilian targets and fatalities. A triggering event involves fatalities. The usage of other weapons implies civilians.
Symbolic Attackers (Figure 5b)	72.9% use other weapons than firearms. 70.3% of the attacks end up with no injuries or fatalities. 67.5% do not have prior contacts to extremist/terrorist groups. 64.5% require a triggering event for the attack intent.	Self-radicalization implies no prior contacts to extremist/terrorist groups, and vice versa. The usage of other weapons than firearms implies no casualties, and vice versa.	No casualties are implied by the existence of a triggering event or being self-radicalized. A triggering event implies not having prior contacts to extremist/terrorist groups. Self-radicalization implies a trigger event.
Daredevils (Figure 5c)	88.9% use firearms. 74.1% require a triggering event for the attack intent. 70.4% target the law enforcement or government officials. 70.4% do not leak the attack intent. 62.9% of the attacks are fatal.	Having no prior contacts to extremist/terrorist groups implies no leakage, and vice versa. A triggering event implies targeting the law enforcement or government officials, and vice versa. A triggering event implies targeting the usage of firearms officials, and vice versa. The usage of firearms implies targeting the law enforcement or government officials, and vice versa.	Fatalities imply the usage of firearms. A trigger event is implied by not-being self-radicalized. Targeting the law enforcement or government officials is implied by either not-being self-radicalized or fatalities after attack. The usage of firearms implies not being self-radicalized.
Attention Seekers (Figure 5d)	67.0% of the attention seekers target civilians. 62.9% of their attacks end up with no injuries or fatalities. 62.9% of the attention seekers do not leak the attack intent.		Civilian targets are implied by either of the following: no prior contacts to extremist/terrorist groups, the existence of a triggering event, or usage of other weapons than firearms. The existence of a triggering event is implied by either no prior contacts to extremist/terrorist groups or usage of firearms. Not having prior contacts to extremist/terrorist groups implies no leakage. Usage of other weapons than firearms implies no casualties.

Table 5. A-priori algorithm results for incident-scene based classification.

Clusters	Prior Criminal History	Prior Contacts to Extremists	Radicalization enabler	Trigger event	Leakage	Weapon choice	Target selection	Fatalities	After-attack behavior
Cluster 1	None	None	-	Yes	Online	Firearms	Civilians	High	-
Cluster 2	-	None	Self-radicalized	Yes	None	Other than firearms	Civilians	-	-
Cluster 3	-	-	Not self-radicalized	Yes	None	Firearms	Law enforcement/ Government officials	-	Arrested/ surrendered
Cluster 4	None	Yes	Not self-radicalized	None	-	Other than firearms	Civilians	None/Low	-

Table 6. Cluster comparisons.

	Maximum damagers	Symbolic attackers	Daredevils	Attention seekers	Stallers
Cluster 1	55%	16%	13%	13%	3%
Cluster 2	23%	48%	6%	19%	3%
Cluster 3	9%	17%	43%	30%	0%
Cluster 4	61%	22%	0%	17%	0%

Table 7. Comparison of two clustering domains.

	Cluster 1	Cluster 2	Cluster 3	Cluster 4
Al-Qaeda related	16.1%	19.4%	37.5%	47.8%
Right-wing	51.6%	48.4%	29.2%	43.5%
Single-issue	16.1%	19.4%	29.2%	4.3%

Table 8. Relationship between ideology-based and behavioral-based classification

.

	Common Characteristics	Strong two-way associations	Strong one-way associations
Cluster 1 (Figure 6a)	100.0% target civilians. 96.7% use firearms. 90.3% require a triggering event for the attack intent. 87.1% of the attacks are fatal. 77.4% have no prior contacts to extremist/terrorist groups. 65.4% commit suicide or are killed at the crime scene.	Not having prior contacts to extremist/terrorist groups implies civilian targets, and vice versa. Online leakage implies committing suicide or being killed at the crime scene, and vice versa. Not having prior contacts to extremist/terrorist groups implies fatalities, and vice versa. Civilian targets imply a triggering event, and vice versa. The usage of firearms implies civilian targets, and vice versa. The usage of firearms implies fatalities, and vice versa.	Civilian targets are implied by either of the following: no prior criminal history, the existence of a triggering event, online leakage, or committing suicide or being killed at the crime scene. Not having prior criminal history implies no prior contacts to extremist/terrorist groups and fatalities. Committing suicide or being killed at the crime scene implies fatalities.
Cluster 2 (Figure 6b)	93.6% have no prior contacts to extremist/terrorist groups. 93.6% use other weapons than firearms. 87.1% are self-radicalized. 77.2% do not leak the attack intent. 67.8% require a triggering event for the attack intent. 64.5% target civilians. 64.5% of the attacks have no casualties.	The existence of a triggering event implies civilian targets, and vice versa. No leakage implies not having any prior contacts to extremist/terrorist groups, and vice versa. Self-radicalization implies not having any prior contacts to extremist/terrorist groups, and vice versa.	No casualties imply the existence of a triggering event, not having any prior contacts to extremist/terrorist groups, and self-radicalization. Not having prior criminal history implies no leakage and self-radicalization. Civilian targets imply no leakage and usage of other weapons than firearms.

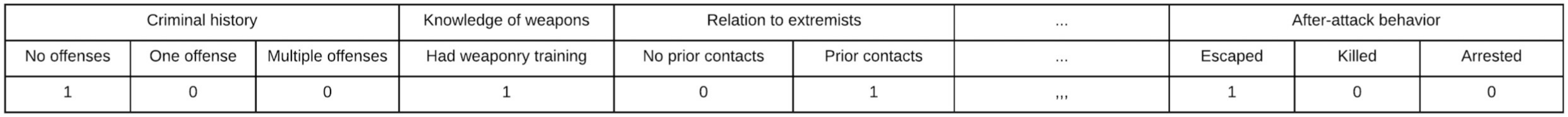
Table 9. A-priori algorithm results for behavior-based classification (Cluster 1 and Cluster 2).

	Common Characteristics	Strong two-way associations	Strong one-way associations
Cluster 3 (Figure 6c)	91.7% are not self-radicalized. 87.5% require a triggering event for the attack intent. 83.3% have prior contacts to extremist/terrorist groups. 79.7% target the law enforcement or government officials. 85.0% use firearms. 70.8% do not leak the attack intent. 87.0% of the attacks have no casualties. 87.0% are arrested at the crime scene.	Not being self-radicalized implies targeting the law enforcement/government officials, and vice versa. Not being self-radicalized implies having prior contacts to extremist/terrorist groups, and vice versa. Not being self-radicalized implies the usage of firearms, and vice versa. Having prior contacts to extremist/terrorist groups implies targeting the law enforcement/government officials, and vice versa. The usage of firearms implies targeting the law enforcement/government officials, and vice versa.	Being arrested after the attack implies no leakage, the usage of firearms, and targeting the law enforcement/government officials.
Cluster 4 (Figure 6d)	100.0% use other weapons than firearms. 87.0% target civilians. 87.0% of the attacks have no casualties. 87.0% are arrested at the crime scene. 73.9% have prior contacts to extremist/terrorist groups. 60.8% are not self-radicalized.	Not being self-radicalized implies having prior contacts to extremist/terrorist groups, and vice versa. Civilian targets imply having prior contacts to extremist/terrorist groups, and vice versa. The usage of other weapons than firearms implies having prior contacts to extremist/terrorist groups, and vice versa. The usage of other weapons than firearms implies civilian targets, and vice versa. The usage of other weapons than firearms implies no casualties, and vice versa. The usage of weapons other than firearms implies being arrested at the incident scene, and vice versa. Being arrested at the incident scene implies civilian targets, and vice versa.	Having no prior criminal history implies having prior contacts to extremist/terrorist groups, civilian targets, and the usage of weapons other than firearms. Having no trigger event implies contacts to extremist/terrorist groups, the usage of weapons other than firearms, and being arrested at the incident scene. Not being self-radicalized implies the usage of weapons other than firearms.

Table 10. A-priori algorithm results for behavior-based classification (Cluster 3 and Cluster 4).

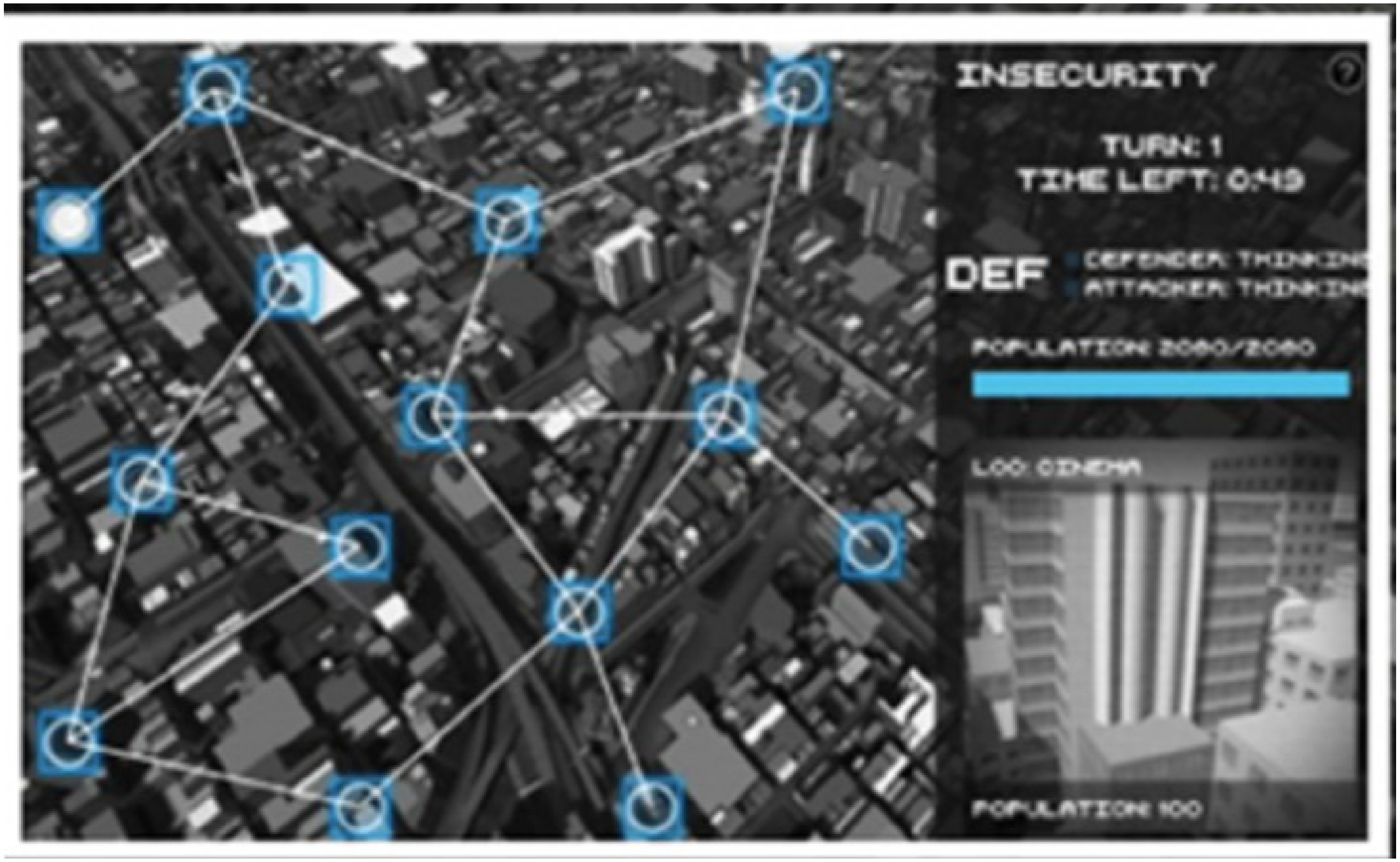
	Number of data points	Prominent characteristic	Mean	Median	Standard deviation	Coefficient of variation
Overall	93	Yes	205.7	31	419.9	2
Ideology-Based Classification						
Al-Qaeda related	24	No	150	46	320.4	2.1
Right-wing	39	Yes	205.2	18	366.8	1.8
Single-issue	20	Yes	188.5	60	370.5	2
Incident-Scene Based Classification						
Maximum damagers	30	No	364.5	151	553.8	1.5
Symbolic attackers	26	Yes	149.2	27	291	2
Daredevils	20	Yes	192.3	31	445.8	2.3
Attention seekers	15	Yes	26.9	4	59.6	2.2
Behavior-Based Classification						
Cluster 1	26	Yes	298.7	144	388.8	1.3
Cluster 2	22	Yes	41.5	7	86.9	2.1
Cluster 3	19	Yes	173.3	17	379.6	2.2
Cluster 4	8	No	209.5	31	389.2	1.9

Table 11. Temporal statistical properties between trigger and attack



Criminal history			Knowledge of weapons	Relation to extremists		...	After-attack behavior		
No offenses	One offense	Multiple offenses	Had weaponry training	No prior contacts	Prior contacts	...	Escaped	Killed	Arrested
1	0	0	1	0	1	,,,	1	0	0

Figure 1. Binary coding structure for a hypothetical LA



TURN: 1
TIME LEFT: 0:49

DEFENDER: THINKIN
ATTACKER: THINKIN

POPULATION: 2080/2080

LOC: CINEMA

POPULATION: 100

Figure 2. Security game developed in the GRIST Lab

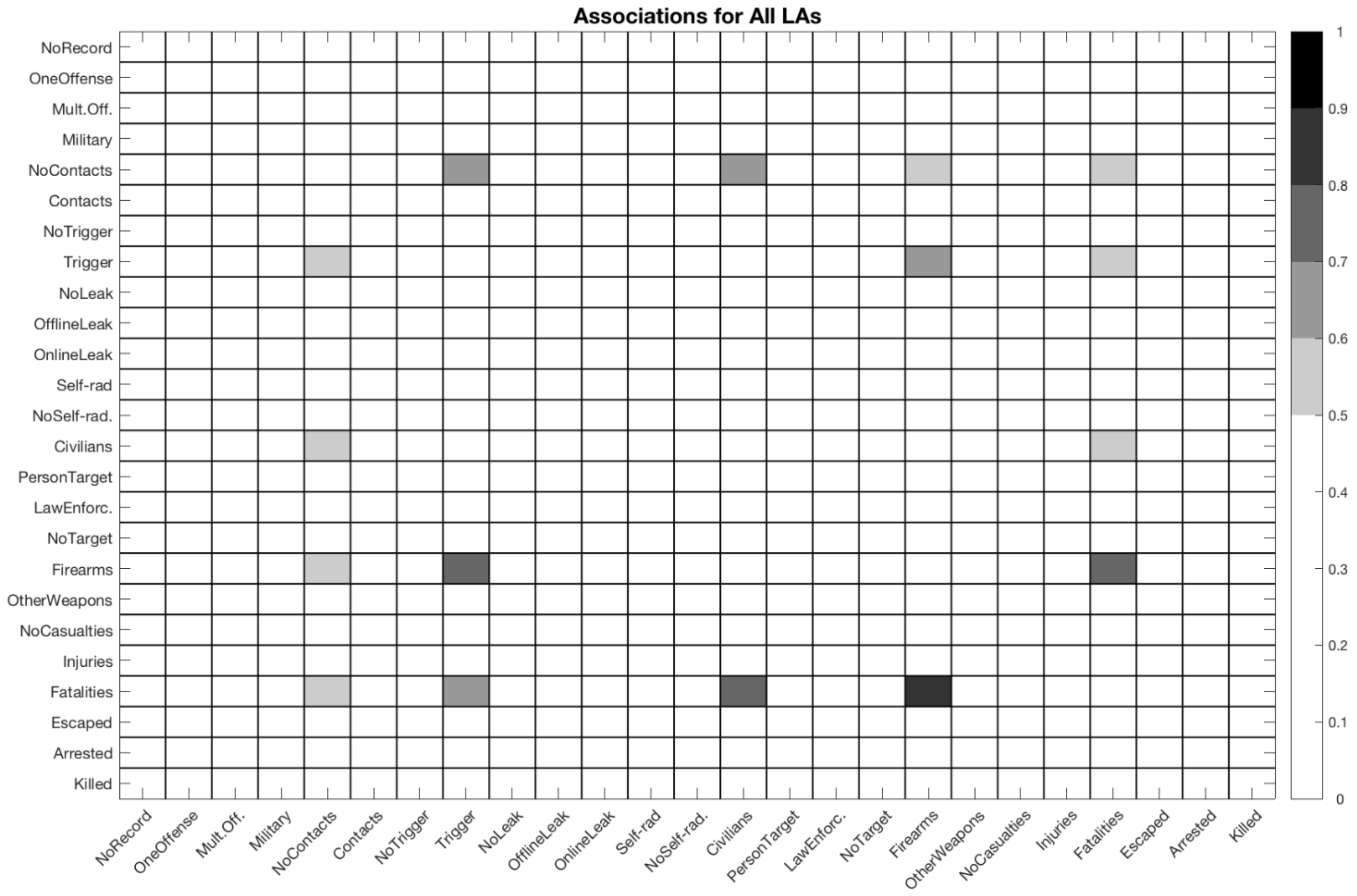
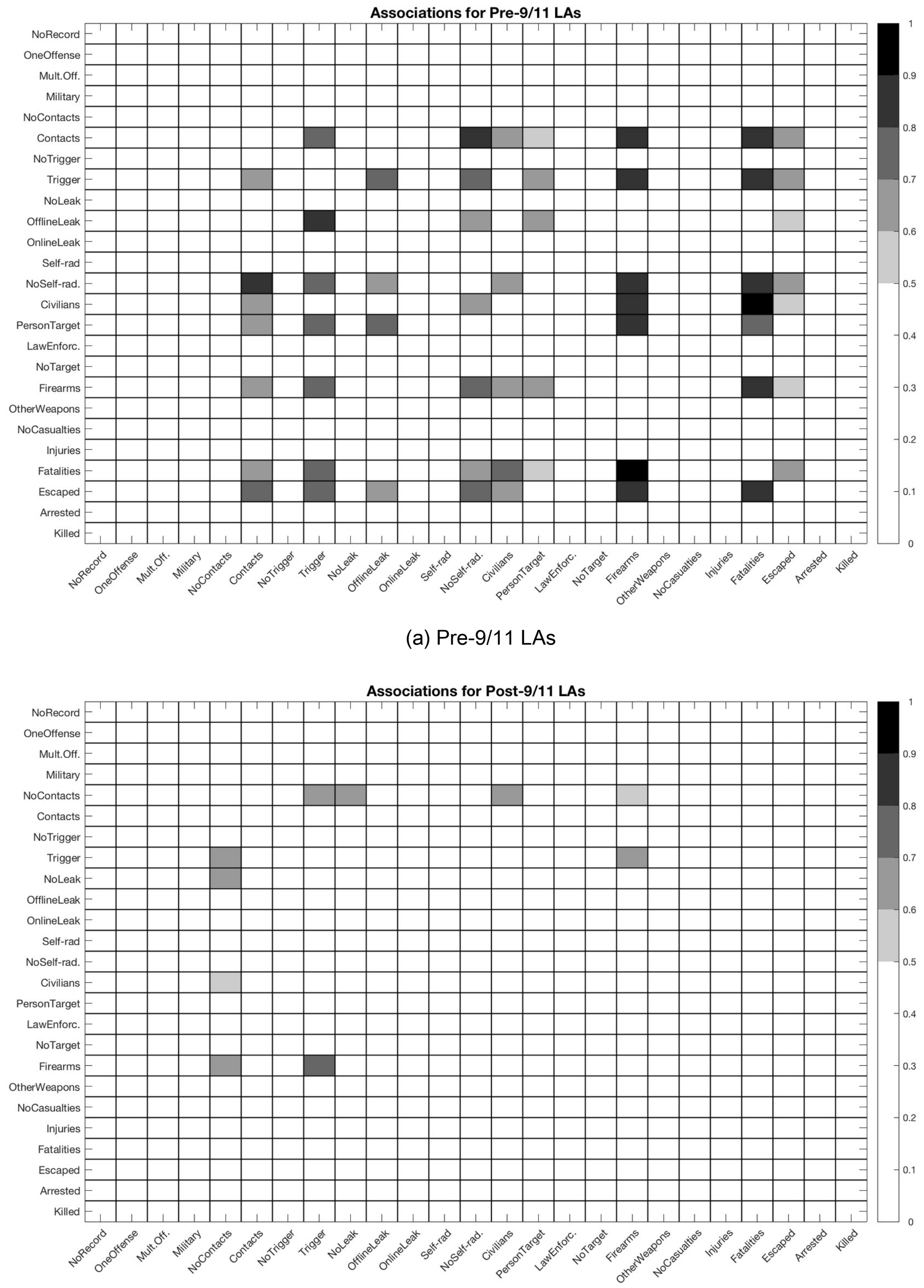


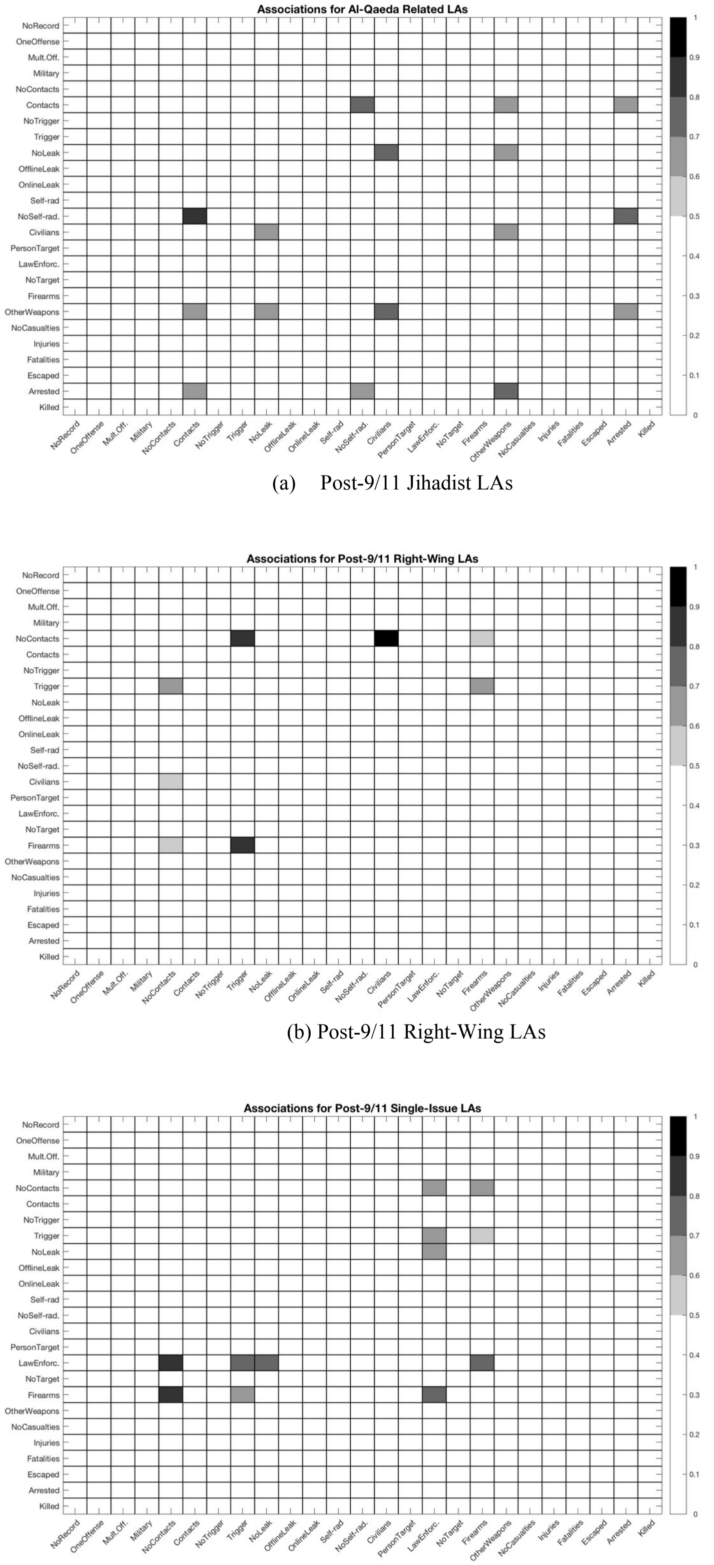
Figure 3. Associations for all LAs. For this figure and all forthcoming figures for associations, the color of each cell indicates the confidence level of the association. The color white indicates three possibilities: i) the confidence of the rule is less than 0.5, ii) the confidence of the rule is greater than 0.5 but the lift is less than 1, therefore, the associations are coincidental, and iii) at least one item is not frequent enough to construct an association. The shades of gray indicate the magnitude of the confidence, where darker shades specify a stronger association.



(a) Pre-9/11 LAs

(b) Post-9/11 LAs

Figure : Associations denoting temporal change in LA behavior. Pre-9/11 LAs having more associations than post-9/11 LAs shows that the LAs have diversified greatly in terms of behavior and characteristics.

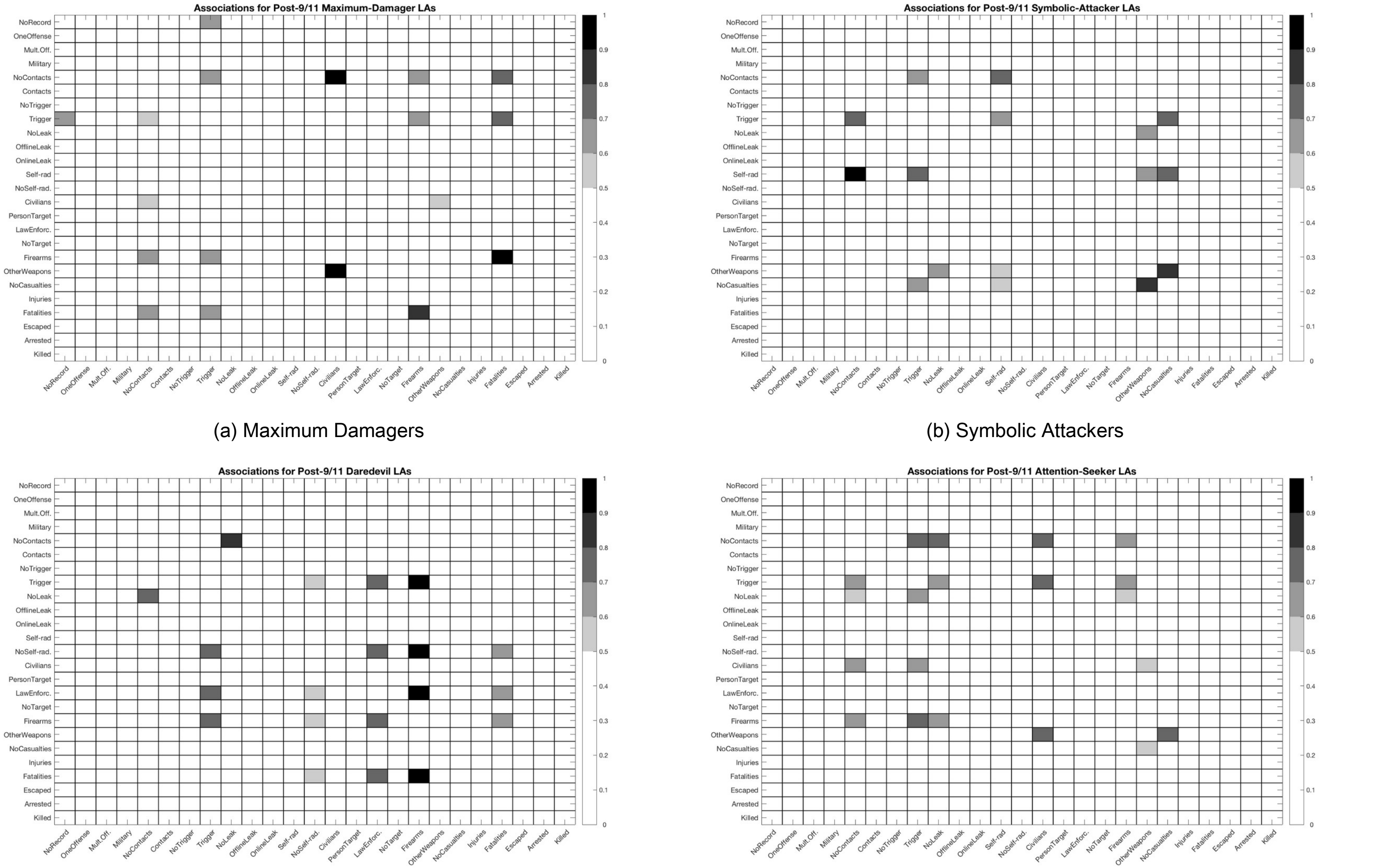


(a) Post-9/11 Jihadist LAs

(b) Post-9/11 Right-Wing LAs

(c) Post-9/11 Single-Issue LAs

Figure 5. Associations by ideological motivations. Even though each ideological class has distinctive demographic distinctive characters as given in [5, 8, 42], this classification adds very little to the post-9/11 associations and the A-priori algorithm does not find many associations.



(a) Maximum Damagers

(b) Symbolic Attackers

(c) Daredevils

(d) Attention Seekers

Figure : Incident-scene behavior produces more commonalities than ideology-based behavior as can be seen in Table 3. Even though common characteristics have increased in number, most of these commonalities belong to the after-attack behavior. Traceable warning behaviors such as intent leakage or triggering event are not prominent in this classification.