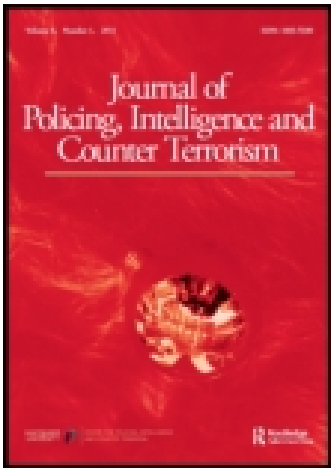

Journal of Policing, Intelligence and Counter Terrorism

Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/rpic20

Pathways to Terror: Finding Patterns Prior to an Attack

Michael Freeman [a] , David Tucker [b] & Steffen Merten [c]

[a] Assistant Professor in terrorism and terrorism financing , Naval Postgraduate School , Monterey

[b] Associate Professor in counterterrorism and homeland security , Naval Postgraduate School , Monterey

[c] Research assistant at the Naval Postgraduate School , Monterey

Published online: 03 Aug 2011.

To cite this article: Michael Freeman , David Tucker & Steffen Merten (2010) Pathways to Terror: Finding Patterns Prior to an Attack, Journal of Policing, Intelligence and Counter Terrorism, 5:1, 75-85, DOI: 10.1080/18335300.2010.9686942

To link to this article: http://dx.doi.org/10.1080/18335300.2010.9686942

Forum

Pathways to Terror: Finding Patterns Prior to an Attack

MICHAEL FREEMAN

Assistant Professor in terrorism and terrorism financing at the Naval Postgraduate School, Monterey

DAVID TUCKER

Associate Professor in counterterrorism and homeland security at the Naval Postgraduate School, Monterey

STEFFEN MERTEN

Research assistant at the Naval Postgraduate School, Monterey

ABSTRACT

To ascertain whether terrorist attacks follow an observable pattern in their pre-attack activities this study first divides the terrorists' pre-attack activities into nine phases: networking, training, general planning, attack-specific recruitment, financing, operational planning, weapons procurement, logistical preparation, and operational preparation. With these phases in mind, we then examine a range of terrorism events and identify when each of these phases occurred. We have found that the cases follow a general pattern, yet there are outliers to the pattern. In general, however, the phases we identified do seem to represent a necessary order. Some broad plan, along with networking and general training occur usually more than a year before an attack and are necessary before recruiting and financing can occur, which usually happens between six months and a year before an attack. Finally, operational planning, weapons procurement, logistical preparation, and operational preparation occur closest to the attack, typically only a few months before it occurs. This general progression is robust across types and scales of attacks and suggests that it might be used as an indication of the timing of possible future attacks.

Introduction

Do terrorist attacks follow an observable pattern in their pre-attack activities? If there is a pattern, how reliable is it? Can we use this pattern as an indicator or warning

of imminent terrorist activity? More specifically, can we use these indications and warnings to predict the *timing* of a future terrorist attack?

To answer these questions, this study will first divide the terrorists' pre-attack activities into nine phases: networking, training, general planning, attack-specific recruitment, financing, operational planning, weapons procurement, logistical preparation, and operational preparation. With these phases in mind, we will then examine a range of terrorism events and identify when each of these phases occurred. Some of the events that will be studied will include attacks on the USS Cole, September 11, the LAX airport, Bali in 2002, Madrid in 2004, the Limburg oil tanker, the USS Sullivans, the embassies in East Africa in 1998, and the USS Kearsage.

These cases provide variation across multiple dimensions; some are small, while others are large; some are maritime attacks, while others are on land or from the air; some occur in the Middle East, while others occur in Asia, Europe, and the U.S. All these variations in cases will allow us to assess the overall pattern of terrorist planning activities, but will also allow us to break the cases apart and see if there are differences according to the type of attack.

Our goal is to determine if there is a general timeframe in which each phase occurs. For example, if terrorist financing usually occurs three to six months before an attack, this will provide a valuable warning to intelligence analysts and will have different ramifications than if it occurred two to three days before an attack. If financing and other activities occur a short time before an attack, then a policy of arresting those suspected of plotting an attack as soon as their activity is noticed would make sense, since activities and attacks nearly coincide. On the other hand, if financing and other preparatory activities take place typically months before an attack then letting these activities continue, in hopes of catching more accomplices, might be a reasonable risk to take. In addition, if most attacks have a long preparatory phase, then it increases the likelihood that individuals planning terrorist attacks might come to the attention of citizens and police officers engaged in routine activities. In this case, it would make sense to increase public awareness campaigns, as well as briefings to patrol officers and others, such as fire and public health personnel, whose routine activities might bring them into contact with individuals preparing attacks.

Finally, we will be able to assess the general ordering of these phases. Does each phase usually occur in some sequential pattern or does their order change for each attack? For example, if financing activities are observed, should intelligence analysts next look for evidence of weapons procurement or attack-specific recruitment or something else?

This paper will first describe the operational phases and how they are coded. Next, we will analyse the data to see if any patterns emerge. Our discussion will focus on the overall pattern, as well as how different subsets of the cases have different or similar patterns. Finally, this paper will address how this research can be used to develop indications and warnings of terrorist attacks. To do so, we will show how

we can predict (with some confidence) the timing of unrealized terrorist attacks, specifically the Fort Dix and JFK airport plots.

Phases of terrorist activity

Before a terrorist attack occurs, several other things must occur. The individuals involved must join the group, get trained, plan the attack, acquire finances, weapons, and other material, and make final preparations or rehearsals for the final attack. We have created nine different phases that incorporate these activities. Each phase is meant to be as distinct as possible. We recognize, however, that some may overlap or be hard to differentiate when coding actual cases. The phases of pre-attack activity are:

(1) *Networking and Indoctrination*: The introduction of cell members and exposure to radical doctrine through events such as religious instruction, cohabitation, meetings, and social activities.

(2) *Terrorist Training*: The participation of cell members in organized terrorist training activities (often overlaps with 1).

(3) *General Planning*: The decision to conduct a terrorist attack and choice of a general target area or target set (i.e. ships, bars, Americans, soldiers, etc.). Phase also includes general "shopping" for potential targets.

(4) *Recruitment*: The selection or the activation of cell members for a specific terrorist operation by more senior terrorist elements. This assumes that there is a senior element, as there was in the 9-11 attack, which helps with recruitment and selection of personnel. In a group like the one that carried out the attacks on the London mass transit system in July 2005, this may not be the case. Yet, in groups like that a process of recruitment and selection still occurs, as pre-existing groups of friends and acquaintances go through the process of radicalisation that ultimately results in a group committed to an attack.

(5) *Financing*: The collection and allocation of funds for a specific terrorist attack. Sometimes, as with the group that carried out the attack on the USS Cole, the money comes before the decision to conduct an attack is made.

(6) *Operational Planning*: The selection of the specific target, detailed reconnaissance of the target, and specific planning for operation (delivery method, procurement methods, etc.).

(7) *Weapons Procurement*: The procurement or receipt of materials for the construction of explosives or weapons used in the attack itself (fertilizer, rockets, detonators, accelerant, etc.).

(8) *Logistical Preparation*: Logistical actions taken in preparation for the terrorist attack including safe house rental, vehicle procurement, document procurement, electronics purchase, etc.).

(9) *Operational Preparation*: Physical Preparations for the imminent terrorist attack including explosives construction, vehicle alteration, specific explosives training, multimedia preparation/creation, etc.).

Emergent patterns

We examined and coded twenty-one cases of terrorist attacks and two attacks that are not typically counted as terrorist attacks (Columbine and Virginia Tech), since they were not carried out for political reasons. We have included them only to see if any patterns in terrorist attacks also occur in non-terrorist attacks that required some planning. For each case we looked for evidence of when the terrorists (or attackers) engaged in activities across the nine phases. The cases were:

- The Achille Lauro Hijacking – 1985
- The World Trade Center Bombing – 1993
- The Oklahoma City Bombing – 1995
- The Khobar Towers Bombing – 1996
- The Dar al Islam, Nairobi AQ Bombings – 1998
- The Columbine Shooting – 1999
- The LAX Millennium Plot – 2000
- The USS Sullivans Attack – 2000
- The USS Cole Bombing – 2000
- The September 11 Attacks – 2001
- The Richard Reid Failed Attack – 2001
- The MV Limburg Bombing – 2002
- The Dubrovka Theater Siege, Moscow – 2002
- The Bali I Bombings – 2002
- The Jakarta Marriott Bombing – 2003
- The Madrid Train Bombings – 2004
- The Australia Embassy (Indonesia) Bombing – 2004
- The USS Kearsarge Attack – 2005
- The Bali II Bombings – 2005
- The London Subway Attack – 2005
- Fort Dix Plot – 2007
- JFK Airport Plot – 2007
- The Virginia Tech Shooting – 2007

These cases were not chosen randomly, and so any conclusions must be read as only tentative. In fact, the cases were chosen based on two criteria. First, we chose cases for which we expected to be able to gather data on the different phases. Second, we intentionally added cases to get as much variation as possible, but this variation may not occur in the same proportions in the overall universe of cases as it does in our dataset. For example, we chose 'big' cases like the 9/11 attacks, the Madrid train bombings, and others that we would expect to require more planning, but also smaller attacks like the LAX Millennium plot and the Richard Reid failed attack, which presumably would require less planning. We also chose al-Qaeda attacks as well

as attacks by other groups. We included maritime terrorist attacks (Cole, Sullivans, Limburg), and non-maritime attacks. We included cases of not just successful attacks, but also ones that failed (Sullivans, Richard Reid, LAX), and ones that were thwarted (Fort Dix and JFK airport). The purpose of intentionally including cases of different types was to allow us to be able to break these cases apart and see if they fit the larger, overall patterns.

For all the cases, there are issues of missing or incomplete data. For example, we know that the Limburg attackers received a few infusions of cash before the attack. However, because we do not have a firm date for these events, we could not include this information in our dataset. Consequently, for any single case, we cannot plot the timing of *all* the activities by phase that we know must have occurred before the attack.

With these issues in mind, we plotted the data on the graph below (Figure 1).

Figure 2 takes the same data and shows a bracket for each phase. The center of the bracket is the mean and the edges are two standard deviations from the mean.

Figure 2 suggests that the nine phases we identified fall into three stages. Beginning with the phases most remote from the attack, we might say that our sample shows that Stage I consists of phases 1-3 (planning, training and networking) and takes place a year or more in advance of the attacks. Stage II, (phases 4 and 5: recruitment and financing), takes place six months to a year or so in advance of an attack. Finally, Stage III consists of phases 6-9 (operational planning, weapons procurement, logistical preparation, and operational preparation) occur closest to the attack, typically only a few months before it occurs.

Figures 3, 4, 5, and 6 present the data in a similar way, except they only include smaller subsets of the data (al-Qaeda attacks in Figures 3 and 4, and maritime attacks in Figures 5 and 6).

In terms of patterns that emerge, we must first re-iterate that the limited number of cases and their non-random selection urge caution in interpreting the results of the research. As a generalisation, we can say that the phases and stages follow in what might be described as an operationally logical pattern. Recruiting and building general operational capabilities occurs first, often months and even years in advance of a particular operation. Operational phases connected to a specific operation take place closer to the event, usually months, but sometimes only weeks or days before the attack. Sometimes a triggering event unconnected or at least not directly connected to the individuals preparing for attacks (an arrest or political event, for example) leads the terrorists to launch an operation that they have been planning.

The pattern for all of the cases also held up for subsets of the data. For instance, as Figures 3-6 show, al-Qaeda attacks and maritime attacks were fairly consistent with the overall pattern, although with some exceptions.

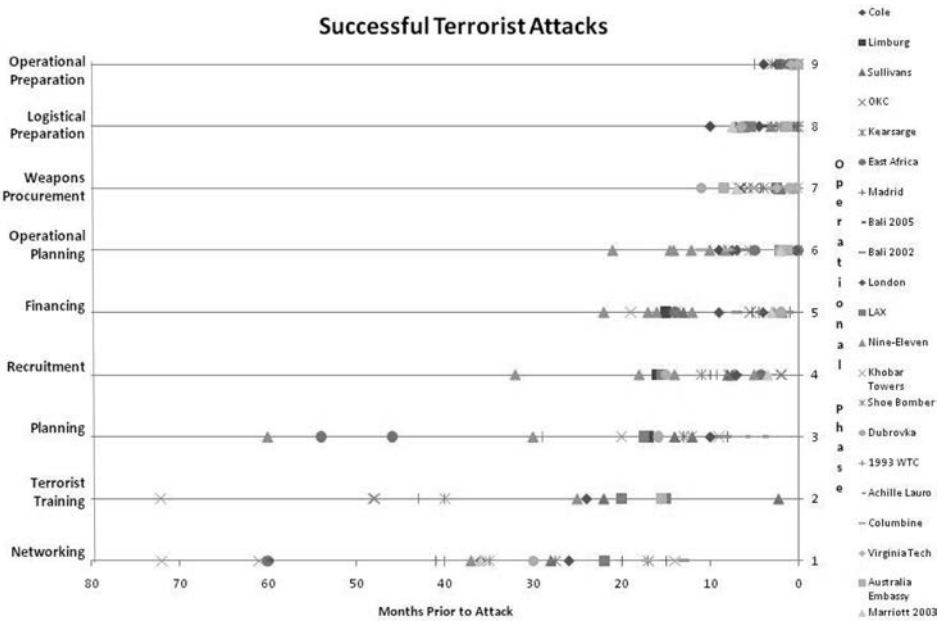

Figure 1 – Successful terrorist attacks

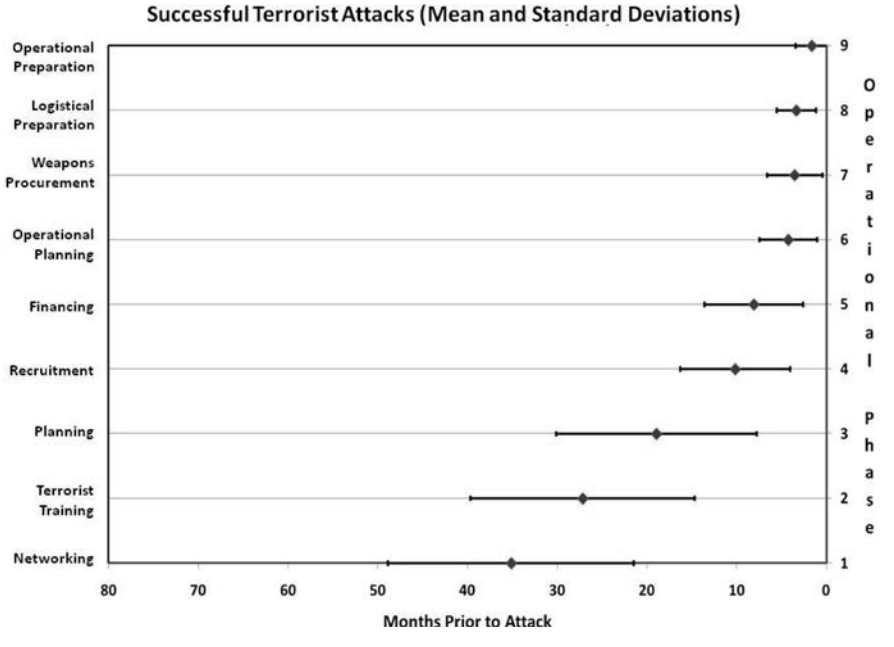

Figure 2 – Time brackets for each stage

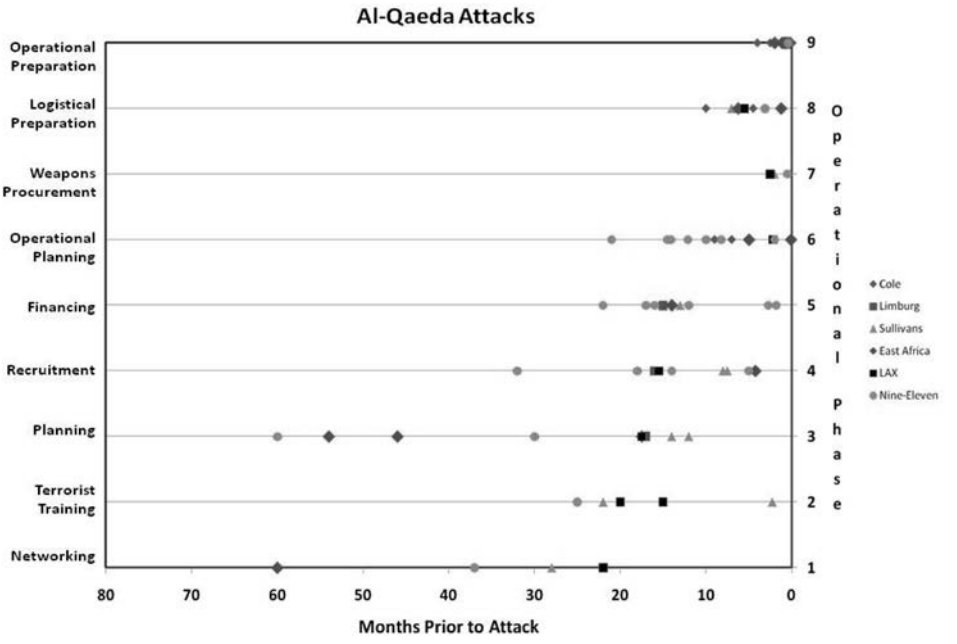

Figure 3 – Al-Qaeda attacks

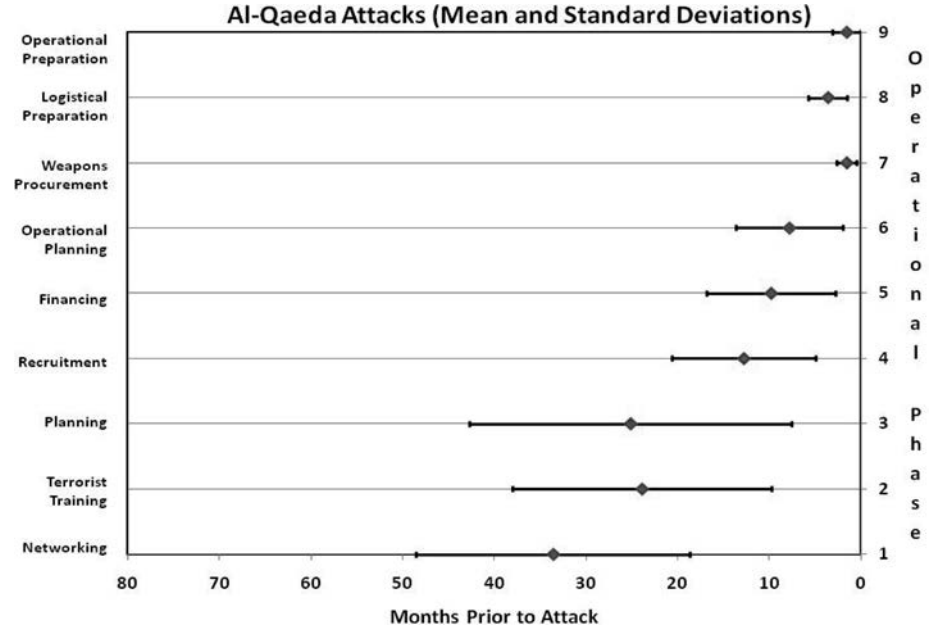

Figure 4 – Al Qaeda attacks mean and standard deviations

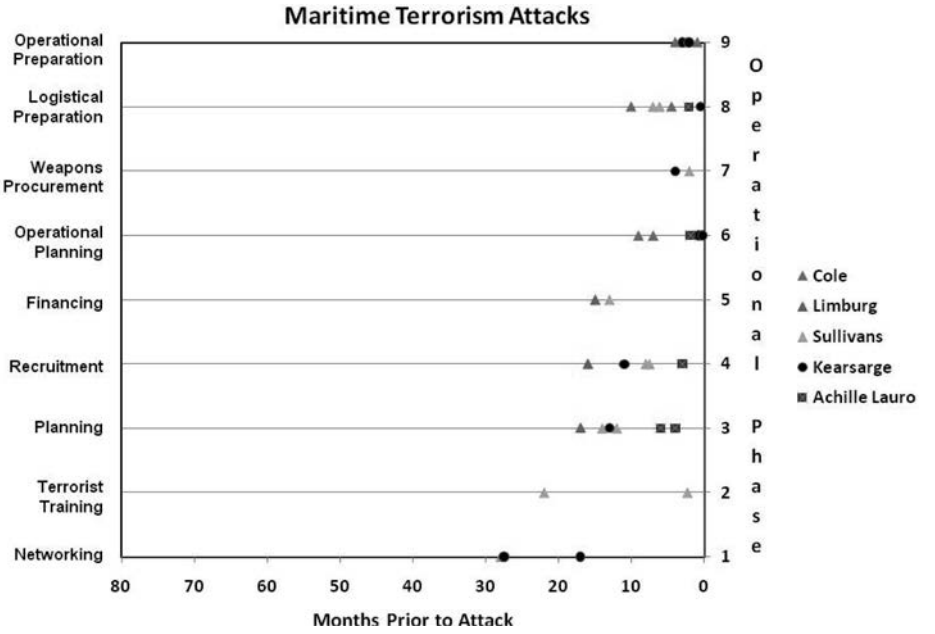

Figure 5 – Maritime terrorist attacks

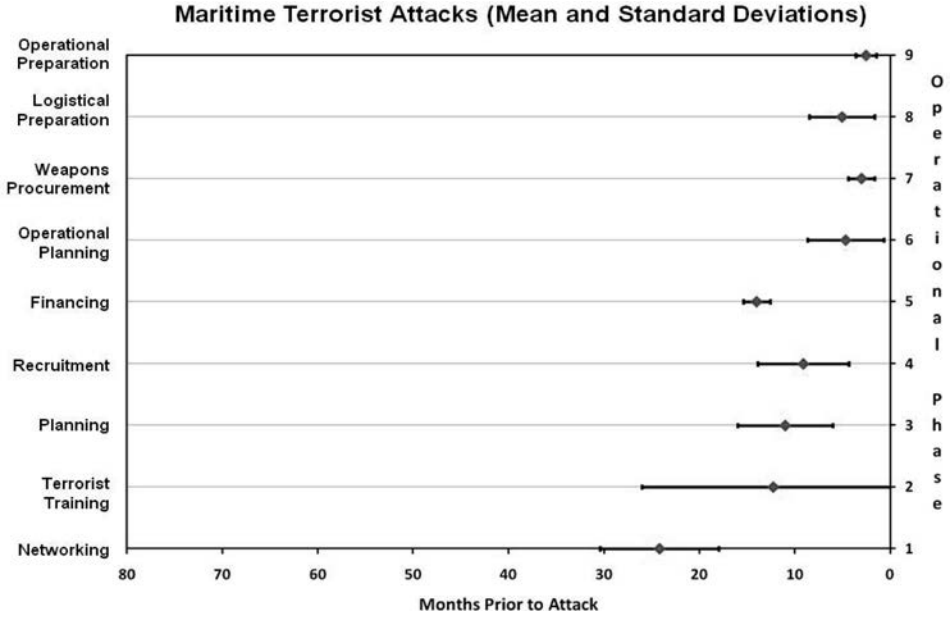

Figure 6 – Maritime terrorist attacks mean and standard deviations

Although a general pattern emerged, we could not identify any critical pathways. The phases did not always occur according to the general pattern. While there is a general logic to the ordering of the phases, there is no reason to expect that they must necessarily be in the same order for all cases. Also, if a group had carried out a previous attack, then the pattern was foreshortened because the group had already built its capability and so lead times before an attack could be shorter. Of the twenty-three cases we examined, eight were second or later attacks by the same group (Achille Lauro, Cole, Limburg, Kearsage, Dubrovka, Marriott Hotel, Australian Embassy, Bali 2005). As we should expect, in these cases the preparatory phases are shortened. Still, operational planning, weapons procurement, logistical preparation, and operational preparation, what we called above Stage III, occurred several months before the attack and sometimes ten to twelve months before.

Indications and warnings

While understanding the general pattern of preparation before a terrorist attack is useful, it would be most valuable if it could be used as an indicator of an upcoming attack. Specifically, if we assume that a terrorist plot follows the larger pattern (and this is admittedly a big and perhaps problematic assumption), can we predict when the attack itself is likely to occur? In our dataset, we have two cases of pre-empted attacks – the Fort Dix plot and the JFK Airport plot, both in 2007 – that offer a test of this proposition. Because the plotters were arrested before an attack could take place, we could not plot them on the same scale as the other attacks (where the x axis is time before the attack). Instead, the events are plotted chronologically. Both of these cases (to the time arrests put an end to them) fit within the overall pattern developed from the other attacks. In fact, based on the overall patterns found in other cases, we could estimate that the attacks would likely have occurred 2-4 months or so after the plotters were arrested. Figure 7 shows the JFK plot and Figure 8 shows the Fort Dix plot.

From a practical standpoint, there are several challenges to finding indications and warnings of future terrorist attacks. For example, some of the activities described in this paper may occur without having any ties to terrorist activity or terrorist groups. Also, some activities might not be observable to intelligence agencies. To be able to better judge the quality of indicators, Greg Treverton proposes that potential indicators be evaluated according to their uniqueness and visibility.[1] Unique indicators of terrorism are those that cannot be explained by other types of activities. For our purposes, weapons procurement and operational preparation (constructing the bomb, altering the vehicle, making a martyr video) are probably the most unique because there would be few reasons for non-terrorists to engage in these acts. Other activities, such as financial flows and logistical preparation (e.g. renting a

1 Treverton, G. (2009). *Intelligence for an age of terror.* Cambridge: Cambridge University Press, pp. 41-48.

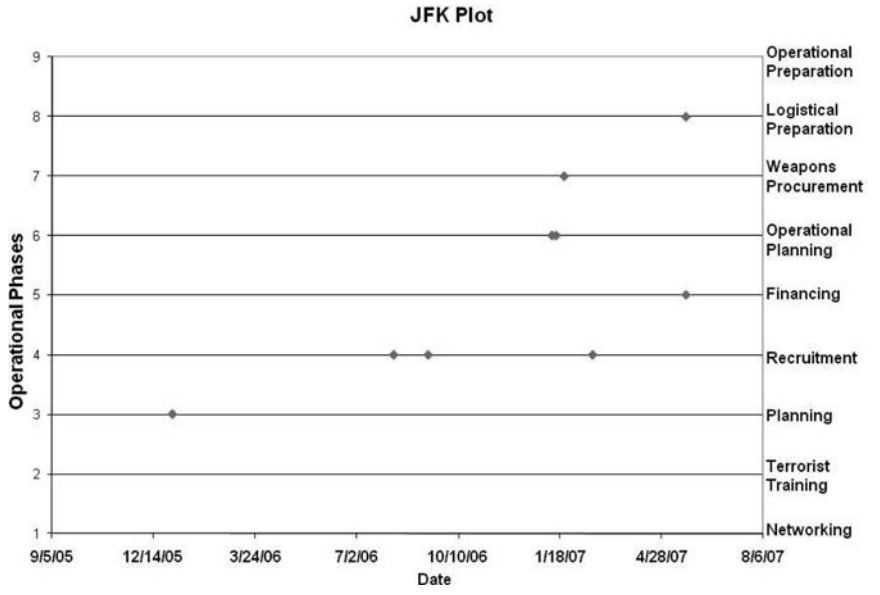

Figure 7 – The JFK plot

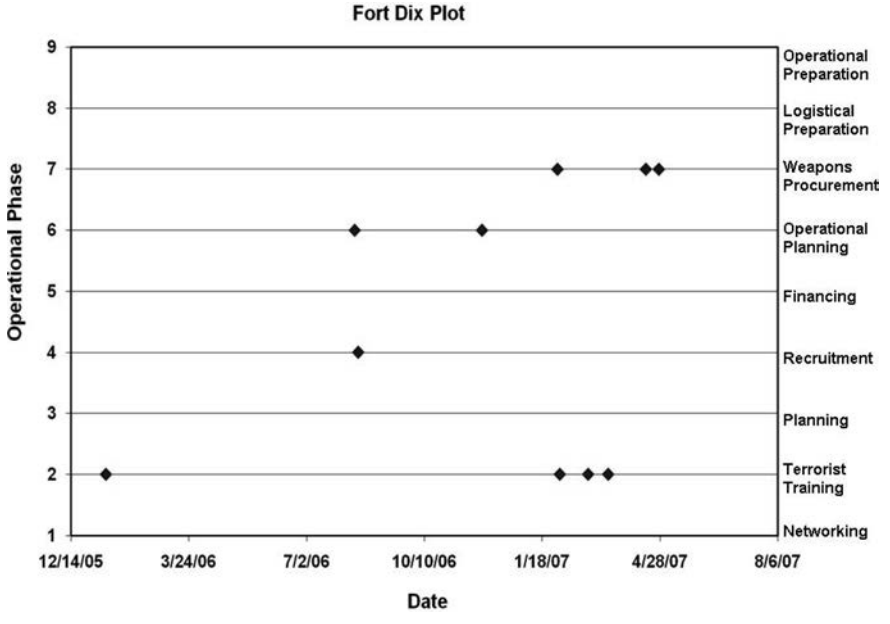

Figure 8 – The Fort Dix plot

storage unit), are less unique because they might be done by people uninvolved with terrorism. Visible indicators are those that are easily observed by security forces (law enforcement, military, intelligence). Among our phases, attack-specific recruitment may be visible if it involves the movement of would-be terrorists across

borders (e.g. the 1998 embassies bombings), financing may be visible if funds are moved through the formal banking system, weapons procurement may be visible if the purchase of explosives and precursor materials is monitored, and logistical preparation may be visible because activities like vehicle and safe house purchases are often in the public record. Of course, indicators that are both visible and unique are the best, but this does not often occur. Nevertheless, Treverton's criteria are useful for evaluating the relative merits of the different phases as possible indicators of future attacks.

Conclusion

In sum, we have collected data on twenty-three different attacks and coded the information on their pre-attack activities according to our nine phases. We have found that the cases follow a general pattern, yet there are outliers to the pattern. In general, however, the three overall stages we identified do seem to represent a necessary order. Some broad plan, along with networking and general training (Stage I) occur usually more than a year before an attack and are necessary before recruiting and financing (Stage II) can occur, which usually happens between six months and a year before an attack. Finally, operational planning, weapons procurement, logistical preparation, and operational preparation (Stage III) occur closest to the attack, typically only a few months before it occurs. This general staging is robust across types and scales of attacks and suggests that it might be used as an indication of the timing of possible future attacks.