Paper Submission for:
12th International Command and Control Research and Technology Symposium:
"Adapting C2 to the 21st Century"

Title of Paper

"Counterterrorism Tactics: A Model of Cell Dynamics"

Suggested Track Topics

Networks and Networking (Track 2)
Modeling and Simulation (Track 3)
Organizational Issues (Track 5)

Author

ENS. Kathleen Giebel "STUDENT"

Point of Contact

ENS Kathleen Giebel

Organization

Joint Command, Control, Computers, Communication and Intelligence
Navy Postgraduate School
Monterey, CA

Address and Contact Details

584 C Michelson Rd
Monterey, CA 93940
USA
Tel: (831) 233 8876
Email: kagiebel@nps.edu

Counterterrorism Tactics: A Model of Cell Dynamics

Kathleen Giebel
JC4I / Navy Postgraduate School

Abstract

Terrorist organizations continue to receive significant attention in academic, policy and operational circles. *Modus operandi* of various terrorist organizations have been studied extensively, and extensive databases, such as ITERATE, collate details about terrorist attacks, to include the types of technology used by the terrorist organization and the number of resultant casualties. Surprisingly, however, a generalized model of how terrorist organizations plan their attacks is unavailable in the extant literature. Drawing from organizational theory, particularly the command and control literature and the case study methods, this paper posits a generalized model of terrorist attack planning. By extending this model into the counterterrorism domain, I then consider how to more optimally detect terrorist attacks.

Introduction

Terrorist organizations continue to receive significant attention in academic, policy and operational circles. *Modus operandi* of various terrorist organizations has been studied extensively, and large databases, such as ITERATE, collate details about terrorist attacks. Such details include the types of technology used by the terrorist organization and the extent of resultant casualties. Surprisingly, however, a generalized model of how terrorist organizations plan their attacks is unavailable in the extant literature. Drawing from organizational theory, particularly the command and control literature, and through synthesis of three case studies, this paper posits a generalized model of terrorist attack planning. By extending this model into the counterterrorism domain, I then consider how to more optimally detect terrorist attacks.

Definitions

Definitions of terrorism have received significant scrutiny and debate, with little resolution (Wikipedia, Definition of Terrorism). For the purpose of this work, I use a definition

developed by the US Department of Justice, which defines terrorism as "the unlawful use of force or violence committed by a group or individual against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives." (Grimmer, 2007) Efforts by representatives of the state to prevent or deter such unlawful uses of force or violence will be classified as counterterrorism. Thus counterterrorism, in this work, includes efforts to hinder the formation of terrorist cells, impede the planning that may lead to terrorist attacks and finally prevent the execution of attacks.

Organizational and Open Systems Perspective

This paper focuses on terrorism at the organizational level in order to examine how the *work* of terrorism is conducted, rather than a societal level that might seek to explain why terrorism comes into existence under particular circumstances. Consistent with emerging trends in the literature (Thomas, Kiser and Casebeer, 2005, Ch. 1), this paper views terrorist organizations with an open systems perspective, recognizing that terrorist organizations both draw from and influence the environments in which they are situated (Thomas, Kiser and Casebeer, 2005, Ch. 11). Through understanding the flow of resources and feedback across the boundary between terrorist organizations and their environments, counterterrorism analysts may be able to more optimally interrupt the work processes upon which terrorist organizations depend for successfully producing terrorist attacks. Creating such an understanding involves answering questions such as:

1. What do terror cells require or prefer within their environment in order to be successful?

2. How can law enforces and surveillance teams detect and destroy these preferences?
3. Are there things that can be placed within an environment in order to assist authorities and continue to deter terror cells?

Applicability of Case Study Method

Terrorist organizations have been described as complex, adaptive systems (Roberts, 2006), responding to changes in their environment. However, any functional terrorist group or cell must operate within the confines of their environment and resources, as such the feasible space of their actions and behaviors is bounded, and selection of tactics is limited. Thus one advantage of the case study method is that since these cells act independently, any correlation or consistency one finds between how groups conceive, plan, resource, and execute their operations suggests that social or environmental factors, not shared leadership, is primarily responsible for discernible. By abstracting past attempts at terrorist attacks, a generalized model of the cell's actions should emerge. This generalized model, in turn, will assist counterterrorism professionals with developing or enhance tactics to interdict future terrorist attacks.

The growing concern among counterterrorism specialists is the presence of homegrown terror cells. "[There] was a shift from an al Qaeda operational model based on an "all-star team" of operatives that was selected, trained and dispatched by the central leadership to the target, to an operational model that encourages independent "grassroots" *jihadists* to conduct attacks, or to a model in which al Qaeda provides operational commanders who organize grassroots cells. We refer to this shift as devolution because what we are seeing now is essentially a return to the pre-9/11 model." (Burton, 2006) As such an examination of case studies prior to the attacks on September 11th are equally as imperative as those chosen after the attacks on the World Trade Center and Pentagon. It now becomes useful to analyze how they (the terrorists) have operated in

the past. I have analyzed certain terror cells throughout the last decade whose plots have been stopped prior to execution in hopes of finding certain environmental commonalities throughout each cell. One restriction that I placed on the selection process of cells chosen, due to time constraints, is that some member of the cell had to be prosecuted in an open court thus making documents open to public record and unclassified in nature. I chose two before the Patriot Act and the remainder after the Act in hopes of identifying any obvious environmental changes simply due to the presence of more restrictions. The goal is to choose a variety of different cells in hopes that any trends observed will not be dependant on the type of cell or plot attempted.

With that in mind this thesis will conduct primary research into the following three thwarted terrorist attacks: Brooklyn Bridge attack by Iyman Faris, the Millennial Bombings at the Los Angeles Airport and Operation Bojinka a plan in the mid-90's to attack airliners over the Pacific Ocean along with a series of simultaneous attacks around the world. Occasionally, I will make reference to other thwarted terrorist attacks however primary research will be placed on the terror plots outlined above. Directly stated this paper using case studies of thwarted attacks as a primary source material, will investigate if a basic model of terrorism action will emerge that can assist in developing or enhancing US counterterrorism tactics?

Case Studies

This section explains each case study and its contribution to the more generalized model.

LAX Airport Plot

The first plan being discussed is the proposed attack by Ahmed Ressam. With his cell, Ahmed designed a plot to attack the Los Angeles Airport in California; this plot is also more commonly referred to as the Millennial Bombing. Although originally conceived by a cell formed at an Afghani training camp, ultimately the Millennial Bombing was carried out by one

man, Ahmed Ressam. He was to design a bomb in Canada that would be carried across the border and driven down to the target. Ressam would load this bomb into a suitcase and leave it unaccompanied in the airport with the bomb detonating on a predetermined timing device. Fortunately, Ressam was interdicted at the US border in Washington where a conscientious border patrol was concerned and started asking questions. Once Ressam suspected he was receiving additional scrutiny, he tried to flee but was apprehended.

There are a variety of reasons that made this plot a strong candidate for this research project. Primarily it is ideal for today's situation due to its affinity toward an airport as a target. Commercial aviation and airports as large public spaces have long been significant targets for terrorist groups ("Security Alert," 2007). Additionally, this plan was organized and produced outside the US and with the deadline of the plot approaching the cell attempted to move inside the US borders, another significant concern of counterterrorism specialists, particularly when those cell members are coming across one of our two adjacent borders: Canada or Mexico. A final interesting factor in this particular plot is the fact that the majority of this plot was planned and executed by one man: Ahmed Ressam.

Brooklyn Bridge Plot

The second plot that will be analyzed is the attempt to destroy the Brooklyn Bridge by Iyman Faris. This plot was already conceived by top members of Al Qaeda leadership including Khalid Shaikh Mohammed and Majid Khan but was placed upon an independent member, Faris, to research its validity. Iyman, a citizen of the US, was tasked by members of Al Qaeda leadership to return to the US to see if it was possible to use certain tools to derail a train while simultaneously destroying the Brooklyn Bridge. Upon his return to the United States, Faris conducted independent research to discover ways to carry out this plan. However, authorities

were tipped off and Faris was apprehended for conspiring with known terrorists. Ultimately, Faris emailed leadership in Al Qaeda with a coded message that meant there was too much security for the plan to actually work and all planning stopped.

This plot was chosen in particular because it is much different from the other two plots that it has been planned after the attacks on September 11th. Although this plot never left the researching phase, it did show a significant amount of communication between cell members and Al Qaeda hierarchy which is not necessarily as prevalent in other plots. By having so much communication present, methods are able to be analyzed for patterns.

Operation Bojinka

Finally, Operation Bojinka was a plot masterminded by the infamous Al Qaeda leader Khalid Shaikh Mohammed (KSM) and his nephew Ramzi Yousef. It was a compilation of a many different plots all brought together under one overriding plot called Operation Bojinka. Under this plot there would be at least ten airliners targeted and destroyed with ready made bombs brought on board by cell members. Additionally, one of those planes would possibly be used to crash into a strategic US target like a CIA or FBI buildings. Simultaneously there would be an attack on the US Embassy in Manila and a subsequent assassination of the Pope who would be visiting Manila at the same time. The cell worked out of an apartment that was near the US Embassy in Manila; the tenants were very suspicious and were reported to often have chemical burns on their hands. Although it is not common knowledge why authorities began to watch this apartment, ultimately cops raided the building and discovered more than enough evidence to determine what the full story was. This plot reached a test execution phase before being discovered, one operative tested airport security by bringing a bomb 1/10 the planned size, assembling it in the bathroom, placing it under a seat and getting off at the next stop. During the

next leg of the trip the bomb exploded, killing the man in the seat under which the bomb had been placed. A handful of other passengers were injured.

The reason this paper uses Operation Bojinka is primarily due to the sheer size of this plan, this plot was a huge undertaking by the Manila cell. It exemplifies a typical Al Qaeda plans which are generally quite elaborate being made up of many different pieces all working together with detailed planning and coordination, as well as and extensive pre-execution rehearsal and testing. This also creates a situation that provides for large amounts observable evidence. As stated above, it uses an airplane crash as part of the plot which is also ideal since today's larger plots are including scenarios very similar to part of Operation Bojinka's objectives. Additionally it was planned and designed before the attacks on September 11, 2001 and the introduction of the Patriot Act. Some school of thought suggests that since the Al Qaeda's hierarchy has now been disrupted and its leadership hidden away that the terror cells of today have actually reverted back to pre-September 11th style plots. Plots that are given a big picture but then details are left to individual cells and their hierarchal leadership thus it is most beneficial to study these plots. (Burton, 2006)

Existing Policy

This chapter will be brief, but its intent is to provide the reader with some insight as to what counterterrorism specialists have as resources and assets in their fight against terror threats within the United States. It will also briefly discuss the response that counterterrorism authorities have when responding to threats, for example what biases and opinions they might have when presented with a given scenario. According to the Uniting Against Terrorism

Conference, the broad solution to combating terrorism is presented in a short compact list of solutions presented below.

- Denying access to financial support
- Denying access to weapons
- Denying access to recruits and communications by stopping internet use
- Denying access to terrorist travel
- Denying access to terrorist intended targets

The primary change to counterterrorism measures took place under the institution of the US Patriot Act. The Patriot Act was put in place in direct response to the attacks that took place on September 11, 2001.

The institution of this act increased surveillance of communications within and outside the US. However, provisions allowed via the Patriot Act are very specific in terminology to ensure civil liberties are not infringed. In doing so, it allows authorities a "narrowly defined process" to have electronic surveillance in serious cases such that it can trace the source and destination of calls and other forms of communication but only allows identity of participants to be revealed, nothing more. Additionally it eased restrictions on surveillance of communications (any method) and foreign intelligences outside the US along with giving increased funding to the FBI for surveillance purposes.

One thing the US quickly discovered after the attacks on September 11th as a very successful tool in combating terrorism was the tracking of financial transactions. As such, the Patriot Act enacted policies to combat corruption of financial institutions and to prevent money laundering. Another major concern prior to the September 11th attacks but brought to new heightened attention is border control. There were a number of changes that the Patriot Act put in place in response to this security hole. First it restricts border access to close access to foreign terrorists. It also heightens border control to detain and remove terrorists and to prevent alien

terrorists from entering the US, specifically from Canada. Finally, it made it easier to capture and deport those caught.

Additionally the Patriot Act encourages the cooperation and communication of intelligence and law enforcement agencies within the US government. One step towards that end was the creation of the Department of Homeland Security. In the hope of encouraging information flow to increase, this act increased awards to those who assist in information assisting with terrorist cases while also authorizing "sneak and peek" search warrants along with permitting nationwide and perhaps worldwide execution of warrants in terrorism cases. Finally it lengthens the statute of limitations applicable to crimes of terrorism to give counterterrorism authorities extra time to create a case against suspected criminals.

The institution of the Patriot Act has admittedly caused many changes, however one other aspect of change that should be at least briefly discussed is the recent institution of something called the 1% doctrine, a term coined by Vice President of the United States, Dick Cheney. In response to activities on September 11, 2001 our current Vice President, enacted what would later become known as the 1% doctrine. This doctrine follows that if there is even a 1% chance of an attack when presented with intelligences we are to treat it as if the intelligence was true and imminent especially in the case of WMD. The 1% doctrine has made the world of intelligence gathering and reactions to that intelligence an entirely new reality. The CIA and its counterparts are in constant search for information that may or may not be there and they are under constant pressure to have that information yesterday.

The first question these communities are asked is when searching out intelligences, what exactly are they looking for. A question not so easily answered. But then one must follow that query up with how will you track whatever it is that they are looking for, a more daunting task

than the previous. Based on this new doctrine, when these communities happen to find anything at all, no matter its significance or validity, if there is but a one percent chance that the information is true or imminent the information is to be treated as certain.

In response to the submission of such a finding, the information is to be forwarded on to the FBI or some sort of local terrorism task force for the larger cities if that intelligence is targeting a risk within the United States. The problem is that the FBI is designed as a justice system for the US Federal Government, as such it does not process information at a fast pace. Everything that is submitted is treated as something that may have to be used later in a court of law. As a result, the FBI is now overloaded with information that by its very nature it tries to track and file away. They can barely get through the first page of one report before seven more come in from a myriad of other intelligence communities.

Thus it is easy to see that a drawback to this type of policy is that it creates an environment that places an enormous amount of pressure and responsibility on intelligence and law enforcement communities to find information before its too late. That responsibility goes both ways, so when they act on information that is incorrect it wastes time and resources while undermining any credibility that agency has. However, if they were to respond differently and wait for indisputable proof it might be too late and the attack will have already taken place by the time they can respond. Conversely, the benefits to this policy are that it provides response to the slightest divergence from the normal thus ensuring that the probability of discovering a terror plot is greatly increased from the alternative, a 99% percent doctrine.

Directly after events on September 11th the United States was able to use certain tracking technologies to trace email, cell phone calls and money trails to locate members of Al Qaeda and other terror cells that might have presented a threat to the United States. However, over time

these terror networks have adapted and changed to combat ways that were previously effective in targeting them. Since events on 9-11 there has been a shift in who we are looking for; prior to 9-11 we had terrorists entering the United States attempting to attack landmarks. However, today a rising concern is the possibilities of homegrown, self-directed terror cells, having actual US citizens plotting against their own government which is considerably harder track. Terrorist organizations are now looking for local defectors so they do not need fake identification; specifically, "Al Qaeda values operatives that have lived within the US" (Wikipedia, Majid Khan). Additionally, terror networks are attempting to not use technology that is traceable such as cell phones and email. The threat of homegrown terror cells also makes it more difficult to follow the financing of terror plots since many of these cells are becoming self-financed.

As the United States moves forward in the pursuit of terror cells within and outside their borders, they are confronted with a few major obstacles. The director of the FBI said it best, "We don't know what we don't know" (Klaidman). Although our intelligence communities are able to bring in information, parse it and send it back out at incredible speeds other agencies like the FBI are not set up as efficiently and thus there is delay in response time. There needs to be more direction in what exactly counterterrorism authorities are looking for, the next few chapters take a look at this proposition.

Generalized Model

This section describes the generalized terrorism attack model. When confronted with such overwhelming information against the United States, they must look to what they do have control over: their environment. Organizational contingency theory, deriving from open systems theory, suggests that regardless of size, orientation or mission, terrorist organizations operate within the confines of their environment and resources. Combined with Tilley's observations about repertories of contention, it follows that the feasible space of terrorist organizations' actions and behaviors is bounded, and selection of tactics limited. There seems to be reoccurring evidence that terrorist organizations tend to plan simultaneous and large-scale attacks with most attacks being based on previously successful attacks. This is a very good thing since this means more evidence and cues to look for. "Killing as many as possible seems to have been the paramount criterion in most of the plans". (Jenkins, 2006). "Although many of the schemes appear to be drawn from the same playbooks as the terrorist attacks that did occur" (Jenkins, 2006). In the following pages, this paper suggests that a plot can be broken down in lifecycle by phases based in environmental cues.

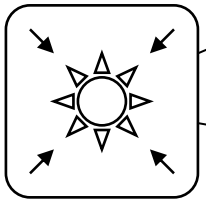
Conception Time: months to years

"Top Down"
- Major Contributors have an idea
- Disseminate idea in training camps

– OR –

"Bottoms up"
- Individuals have an idea
- Validate it through a 'major contributor'

Discuss Details Time: 2-3 meetings over a few weeks



Decision to pursue plot concept

Major details decided

Time: 7-8 months

Major Contributors

- takes care of financing

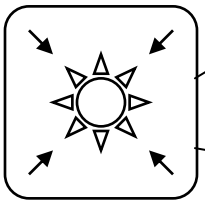
Planning Cell created

- Plans the operation
- Figures out details

(not necessarily the executors)

Decision to acquire resources

Time: 2-3 meetings over a few weeks



Plot details are established

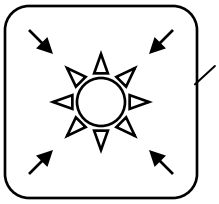
Check back with headquarters

Acquire Resources Time: 2-3 months

Major Contributor's
- Responsible for financing
- Responsible for false ID's

Execution Cell created
- Planning cell may / may not consist of executing cell
- Decides / researches resources needed
- May acquire ordinary supplies

Decision to execute Time: days



- Contact stops

Execution Time: weeks to days

- No communication between headquarters and cell
- Traceable resources acquired
- Cell relocates to location of target
- Test Execution
- Execution

Conception

The general timeline for the conception of a plot is varied and will be dependant on a myriad of factors including who makes up the cell and what the target might be. However, we can generalize conception of the ideas to come from two different sources, bottom-up or top down. In terms of this paper, an idea that is conceived *bottom up* is when a member of a cell or an independent member creates an idea initially and then that idea is approved by a leadership figure. The Millennial Bombing is an example of this type of plot. Conversely a plot that is considered *top down* is one that is conceived by the authorities of an organization and then delegated to cell members for execution. The plot to destroy the Brooklyn Bridge would be an example of a top down plot conception.

During the conception of a plot there will be one or more meetings that are usually private and led by leadership figure. These meetings can take place within the US or abroad, especially at training camps where brainstorming is highly encouraged. From this brainstorming, regardless of source, a rough sketch of an idea or plot will emerge. At this point there is nothing concrete, just a series of ideas that may or may not be recorded.

At this stage there will be an easily identifiable leader since the cell or what is formed of a cell has not been created and members have not bought in yet.

Decision to move forward with concept / Discuss Details

This phase is crucial in the development of a terror cell, but will not take very long to come to a conclusion, since it will only consist of a meeting or set of meetings, generally a short period of time. There will be very specific people involved with this phase including, whoever the financer (or future financer) of the plan, plotters or cell members, and the leadership or

management. As stated above, this meeting will be pushed by a leader to move forward, there will still be a single point of failure at this phase since by neutralizing the agitator (the individual pushing a decision) or by stopping the financing all plans must be called off or at the very least postponed. In some cases one individual may represent multiple portions of members present in this meeting. For example the leadership of a cell might also be financing their ventures. The most important result of this phase is that there is general consensus by all members to move forward. At the conclusion of this phase and the onset of the next will be an excellent point of infiltration for counterterrorism specialists, as the terror cell will be looking for field experts in whatever field their plot may require.

Acquire resources

This period of cell development does not have an exact length although its beginning an end is specifically defined as the point in which the cell decides to stop brainstorming and concedes on one plot to move forward with and then ends as the cell decides that all resources and preparation is complete. This phase can be considered the most easily observed since this is the point in the lifecycle of a terror cell where the cell will concentrate all its energies on preparing specifically for the execution of the plot thus time is spent acquiring all the resources, people and skill sets necessary to execute the plan. As such it is hard to pinpoint an exact amount of time since in many cases this is directly dependant on what the plot consists of and the amount of effort needed to execute the plan. Counterterrorism authorities must be aware that even though these illegal activities are occurring, the terror cell will be continually trying to assimilate themselves into the population as much as possible during this phase.

By now the individuals involved have changed, the primary focus will be on the terror cell specifically and not on individuals like management or financers, thus the command structure at this phase can be considered very horizontal as opposed to a hierarchal structure. This phase is for the actual team to verify the validity of their plan being executed. Generally, each cell member will have a specific role in the plan and will only focus on that role; as such there is not much corroboration between cell members unless a certain portion of the plan overlaps.

Early on in the phase the cell will acquire non-suspicious resources like piping or timers and will begin training such as tactical military training or learning how to fly a plane in the example of the September 11th attackers. Additionally, even though they will not purchase traceable items like explosives, they will at the very least research where and when to buy those items.

Decision to execute

This phase can be considered the point of no return, if a terror cell progresses to this phase their chances of following through and being successful is very high and strongly dependant only on the efficiency to which they can execute their own plans. In other words, there is little that can be done in this phase by counterterrorism authorities in the area of prevention. This phase, like the decision to acquire resources is very short, but also quite critical. Once again the terror cell must all agree that they have planned enough and are ready to move forward with the last portion of their plan: execution.

In terms of command and control the cell will momentarily return to a hierarchal structure before returning back to an asymmetric control structure. There will be contact with

the cell leadership and financing to ensure that they are still allowing this plan to proceed and there will often be an exchange of money for the last few resources specifically those resources that are traceable. The idea is to wait as long as possible to acquire those items to give counterterrorism authorities the least amount of time as possible to respond to any alerts. During this phase there will also be test executions, for example in Operation Bojinka there was a minor explosion on an airliner simply to test security. Other common tests are to leave bags or vehicles unattended with nothing in them just to see how long it would take someone to notice them.

An interesting aspect to this phase is that once the cell has received approval from their leadership all communication with those individuals is severed. They are now acting as an independent group and will carry out the rest of the plan without external input. Thus when the cell has acquired there last minute resources like explosives and feel satisfied that there test executions (if there are any) were acceptable they will gravitate directly into the execution phase.

Execution

The final phase is completed within weeks of the end of the last phase and as stated earlier will have no observable communications. At this point the cell can be treated as well trained separate entities each completing their portion of the plot within the parameters decided upon during earlier phases. This phase can be likened to a well oiled machine; there is no need for discussion or preparation only action. Once again there is very little counterterrorism specialists can do to prevent this phase except for hope that the security measures in place are enough to stop any plan that might be attempted.

Conclusions

Information in this section is supported partially by information not included in this rough draft submission but will be further substantiated in future submissions.

"Where as once we would have caught a robber red-handed and that would have been enough to satisfy the legal case, we now have to stop and ask ourselves, who is this robber? … Is he stealing to feed a drug habit? OK, who is he buying his drugs from? Or is he robbing to raise funds to buy guns for a gang? Which gang? Who are his associates? Or is he part of organized crime or something else? The aim is to drill down into crime to get a complete picture of the crime landscape in your community."(Block, 2006) Chief Barton from the Los Angeles police department explains the issue of fighting the war on terror within our own country quite well in this previous quote. As result of this paper a law enforcement officer or an intelligence analyst can now look at a situation and know what to look for. Furthermore, given certain feedback from the environment they will be able to see how progressed a certain plot may be.

In general we see that information provided to counterterrorism authorities is extremely dependant on connectivity and information flow. "The government's so called war-on-terror is about making friends" (Suskind, 2006, 48). In order to be successful in our attempts to combat the war on terror there needs to be an emphasis on ensuring that information flow is frequent, stable and secure from the top most member of the CIA down to the law enforcement officer in the New York City subway. Being able to rely on informational cues in the environment means that someone has to be there to observe such changes, thus if one person observes something out of the ordinary he needs to be able to inform anyone necessary to ensure that the proper response is completed in enough time to make a difference. This type of response can only be accomplished when communication pathways are open and frequent.

By looking at the three given case studies and analyzing these research points in depth we were able to see some overarching similarities or points of interest that counterterrorism specialists should highlight. First and foremost, these individuals moved through the United States security system by using fake identification and stolen goods. In two of the case studies there was travel to or from Afghanistan for a meeting or some kind of training. Upon their return to the United States Iyman and Ressam each brought a large amount of cash with them to start their resource acquisition phase. In Ressam's case, he also brought back chemicals that would later be used to construct a bomb.

Once the cell was in place they would use coded language to communicate. Iyman Faris used a language that was given to him by his superiors such as gas station for metal cutting torches or a mechanics shop for train derailment tools. This is not the first time we have seen coded language, other cases have used coded language as well. (Suskind, 2006 155-57). Ressam would simply speak in Arabic if he did not want to be understood.

In each case study there is a certain progression with the cell development and known weaknesses for that stage. By realizing those weaknesses exist, counterterrorism specialists can use that information to their advantage to exploit that limitation. In order to be successful with terrorist attacks there needs to be an increase in communication. Teach passengers on a plane what to look for or to notice when someone has been in the restroom for an inordinate amount of time. Make sure that the traffic cop knows what to look for when stopping a suspicious car or replying to someone's luggage being stolen. Notice drug rings that are growing or acting abnormally, in general know who you are tracking. The job is on every citizen to know what to look for and how to respond once that discovery is realized, that is the only way to fight terrorism.

Works Cited

Block, Robert. "An L.A. Police Bust shows New Tactics for Fighting Terror." Terrorism Open Source Intelligence Report 262.TR262A05 (2007): 25 JAN 2006. Terrorism Open Source Intelligence Report. Wall Street Journal <http://www.wsj.com>.

Burton, Fred. "Al Qaeda in 2007: The Continuing Devolution." Terrorist Intelligence Report 27 DEC 2006 Stratfor <http://www.stratfor.com/products/wtr/read_article.php?id=282341>.

Grimmer, Pat. "In Search of Al Qaeda, Glossary and Identifications." Frontline. 2007. WGBH Educational Foundation. <http://www.pbs.org/wgbh/pages/frontline/teach/alqaeda/glossary.html>.

Jenkins, Brian Michael. "Unconquerable Nation: Knowing our Enemy Strengthening Ourselves." Terrorism Open Source Intelligence Report No. 260.Item 3 (2006): 7 JAN 2007. <http://www.rand.org/pubs/monographs/2006/RAND_MG454.pdf>.

Klaidman, Daniel, et al. "Al Qaeda in America: The Enemy within." Newsweek 23 JUN 2003 2003 Hindu Vivek Kendra Database <http://www.hvk.org/articles/0603/173.html>.

Major General John S. Cowings, US Army. "The Environment of Strategic Leadership and Decision Making." Strategic Leadership and Decision Making. Ed. Industrial College of the Armed Forces. 1st ed. Washington D.C.: National Defense University, 1999. Chapter 1, Section 4. Air War College: Analysis and Decision Making. http://www.au.af.mil/au/awc/awcgate/awc-thkg.htm#analysis. 12 DEC 2006 <http://www.au.af.mil/au/awc/awcgate/ndu/strat-ldr-dm/cont.html>.

Roberts, Brad Dr. "Terrorist Campaigns: What can Deterrence Contribute to the War on Terror?" "Terrorist Campaigns: What can Deterrence Contribute to the War on Terror?". MIT Securities Study Program, 26 FEB 2003. 12 DEC 2006 <http://web.mit.edu/SSP/seminars/wed_archives_03spring/roberts.htm>.

"Security Alert: Planes are Still Targets." CNN 16 OCT 2003 2003, sec. US: 11 JAN 2007 <http://www.cnn.com/2003/US/10/16/homeland.alert/index.html>.

Suskind, Ron. The One Percent Doctrine, Deep Inside America's Pursuit of it's Enemies since 9/11. New York: Simon&Schuster, 2006.

Thomas, Troy S., Stephen D. Kiser, and William D. Casebeer. Warlords Rising, COnfronting Violent Non-State Actors. Lanham; Boulder; New York; Toronto; Oxford: Lexington Books, 2005.

Uniting Against Terrorism: Recommendations for a Global Counter-Terrrorism Strategy. Vol. A/60/285. United Nations: General Assembly, 2006. 12 DEC 2006 <http://www.un.org/unitingagainstterrorism/contents.htm>.

Wikipedia Contributors.

"Definition of Terrorism." Wikipedia, The Free Encyclopedia. 29 JAN 2007 2007. Wikipedia, The Free Encyclopedia. N/a. Wikipedia Contributors. 05 FEB 2007 <http://en.wikipedia.org/w/index.php?title=Definition_of_terrorism&oldid=103987873>.

"Majid Khan (Guantanamo detainee)." *Wikipedia, The Free Encyclopedia*. 19 Jan 2007, 03:50 UTC. Wikimedia Foundation, Inc. 22 JAN 2007 <http://en.wikipedia.org/w/index.php?title=Majid_Khan_%28Guantanamo_detainee%29&oldid=101718055>.