The Essentiality of Mathematics in Counterterrorism Operations within the United States

Jacob Knox
Campbell University
Buies Creek, NC 27506
jtknox0104@email.campbell.edu

Abstract

With terrorism as one of the United States' tops security concerns, many changes have been implemented in American counterterrorism operations over the past few decades. Specifically, these changes have occurred in the development of statistics and mathematical modeling in American decision-making processes, focusing on course of action development for large scale decision making. A framework is placed forward outlining the requirements for creating a statistical analysis or numerical model. Once a framework is placed forward, common systems used in different organizations were introduced into the argument. These systems include CARVER + Shock, ORM, and TEVA. After each system is analyzed and compared, recommendations for improving implementation of these systems are interjected.

Key Words: Course of Action development, large-scale decision making, statistical analysis, mathematical modeling, numerical modeling, CARVER Shock, TEVA, ORM, counterterrorism, national security

Introduction

In the 2015 *Worldwide Threat Assessment of the US Intelligence Community* produced by the United States (US) Office of the Director of National Intelligence (ODNI), Director of National Intelligence James Clapper lists terrorism as the United States' third global threat for 2015 (Clapper, 2015). Specifically, Clapper lists Sunni extremists in the Middle East, as well as homegrown terrorists in Western regions, as a threat to national infrastructure and concern for counterterrorism (CT) organizations. (Ibid). While it is logical that terrorism would be listed as one of the top threats for the US intelligence community, it is important to note that the past fourteen years have involved drastic changes in US counter terrorism strategies to combat this developing threat. After 9/11, the US has endeavored to change operational doctrines, internationally reallocate defense forces, and refocus international relationships to better eradicate terrorist groups that are detrimental to US national and international interests.

Within the reconstruction of the US CT strategy, the US has transformed many systems to help maximize CT operations. These systems include revamping intelligence operations, standardizing different operational methods between organizations, reallocating resources to support CT operations, and creating unilateral control measures between nations, to list a few. While many security professionals focus on what some would consider popular components of CT operations, such as direct action operations or critical infrastructure, one crucial function is often overlooked and disregarded because of the culture within the CT community leading professionals to prioritize techniques based on how appealing they seem, not how effective they are.

The role of mathematics in counterterrorism operations is overlooked daily, specifically in the application of statistical analysis and mathematical modeling. The intent of this paper is to provide the reader an overview of the foundations of statistical analysis and numerical modeling, outline how modeling and analysis are used in counterterrorism operations, and to help the reader understand current numerical systems used by the US when employing CT operations. Before one can begin to understand the basics of mathematical analysis in security operations, one must first understand why an organization or government would want a mathematical analysis system or numerical situation model in CT operations. Mathematics in relation to security operations is vital for two essential operations: research and development (R&D) and data analysis.

R&D simply is the engineering and development of new technologies. The leader in US R&D operations is the Defense Advanced Research Projects Agency (DARPA), paving the way in engineering focused on national defense (DARPA, 2015). On the other hand, mathematics is also essential for data analysis. While DARPA focuses on using mathematics to produce tangible products that can be used in physical operations, *data analysis*, also known as *statistical analysis*, can be used for almost any application within any organization. Simply speaking, statistics is the practice of numerically describing a situation or inferring information by mathematically analyzing past data in an effort to make some sort of present organizational decision (Walpole, Myers, Myers, & Ye 1-17). On the other hand, *situation modeling*, also known as *mathematical modeling*, is similar to statistical analysis, but instead of inferring information, it attempts to predict outcomes using past information (Snijders & Bosker, 1-9). Simply speaking, statistical analysis looks to the past using collected data to observe past trends or try to extrapolate present information, whereas situation or mathematical modeling uses the same past data to flexibly predict the end state of a situation.

The foundation of understanding why statistical analysis and numerical modeling is needed in CT operations is rooted in US doctrine for large-scale decision making. Each component of US defense operations has some sort of system in place for making large-scale decisions. When analyzing decision making within the US Department of Defense (DoD), each branch uses different yet similar processes. The US Army, Air Force, and Marine Corps, generally speaking, use a process called the M*ilitary Decision Making Process* (MDMP), whereas the Navy uses a process called *Commander's Estimate of the Situation* (CES) (Anderson and Slate). These methodologies have minor differences, but one common attribute is that of the development of courses of action (COA's) (Ibid). A *course of action* is simply a method by which the organization can face a given problem or scenario (Ibid). Within a decision making process, organizations create multiple COA's and compare them to determine which has the highest likelihood of success and is most in line with the intended operational outcome (Ibid).

Advanced COA development and analysis looks to statistics and mathematical modeling to fine tune small details and develop the best COA for a situation. For obvious reasons, the exact methods in which US operational forces use analysis systems are controlled. However, information regarding the Soviet implementation of similar systems during the early phases of the Cold War is easy to find. Key decision makers within the Soviet Union during the 1970's saw the importance of a standardized numerical analysis method within decision making, therefore implementing systems for maximizing logistical operations, assessing COA's, and even anticipating what enemies of the Soviet Union were trying to accomplish using numerical systems (Druzhin & Kontorov 17-42, 80-124, 200-227). Ultimately the Soviets lost the Cold war. A major contributing factor to the Soviet Union's demise was their inefficiency in logistical

systems and decision-making processes (English 607-626). That being said, one cannot deny that a foundational piece of any organization's success is rooted in being able to make advantageous operational decisions. Numerical analysis in COA development allows an organization to make such decisions.

The Process of Mathematical and Statistical Assessment and Analysis

Before understanding the basic systems the US uses for analyzing COA's, one must first understand the principles of analyzing a situation. The principles of analysis and modeling are fairly straightforward and similar in principle. First, one must specify what is involved in the analysis and what is being analyzed. An example of this could be trying to determine if parental influence plays a positive or negative influence in homegrown terrorist extremism. The outcome for the example is to determine whether parents encourage or discourage extremism in their children. To determine the outcome, one must specify which components of parental influence to analyze. Components could include average daily interaction of parents to children, personal religious extremism and/or preference of parents, religious involvement of parents with children, parental profession, geographic location, parental sympathy towards extremist groups, as well as any other factors that may contribute to an objective observation.

After establishing the components, the analyst must establish some system of measurement for each component. There are three primary ways of assigning values for each component: nominal, ordinal, and continuous (Lee & Femoye). *Nominal* measurement simply measures the existence of something (Ibid). For example, a nominal data point could be whether a parent is a US citizen or not. Collecting data regarding the US citizenship of a parent is a yes-no question, therefore a one is assigned if the parent is a US citizen and a zero is assigned if the parent is not a US citizen. *Ordinal* data uses a predetermined discrete system to measure something based on a scale created by the analyst (Ibid). Using the previous data example, a zero could signify the parent is from the US, a one the parent is the citizen of a US ally, a two the parent is from a country that is neutral towards the US, and a three the parent is a citizen of a country that is hostile towards the US. Lastly, *continuous* data measures what can be numerically measured in its natural state (Ibid). Examples of continuous data could be age, time, speed, or anything that can be naturally observed with a specified level of certainty. The foundational difference between ordinal and continuous data is that ordinal data is discrete, meaning it can only be represented by whole numbers. Continuous data, however, is comprised of natural data, which will be hindered by the specified observational accuracy.

Once the objective of analysis has been established, the components have been defined, and the systems have been put in place to measure each component, the next step is to collect data. This is the most time-intensive but arguably most important part of analyzing data or creating a model. The most important concepts to note about data collection are that of collection practices and the idea of normality. Data collection is more important than any other portion of an analysis or model because data ultimately gives the useful end product. Nonetheless, it is important that the collecting party have systems in place for data quality control and for measuring whether data was collected correctly. A tainted data point could affect the total accuracy of an analysis or model, thus minimizing the effectiveness in analyzing COA's.

Additionally, it is important to consider the idea of normality within data collection. According to the Central Limit Theorem, a fundamental theorem guiding statistical operations, more data points used in a statistical analysis produce a more natural representation within the

analysis (Siegrist). In simple terms, the more data the better the analysis will resemble what is actually happening. When a data sample contains at least thirty data points, the analysis can be considered "normal" (Ibid). This is important to note because the accuracy of a model or analysis can be directly related to the amount of data used.

Once data has been collected, the analysis can be conducted or the model can be created. The most important thing to note in data analysis is the difference in approach between statistics and modeling. Statistical analysis is methodical, disciplined, and rigid to create a semi-objective end product. An analysis focuses more on the process of observing the data to gain information. Modeling is much more non-sequitur, dynamic, and creative to produce a situationally-applicable product. In the process of creating a mathematical model, more often than not, certain processes are blatantly disregarded in the attempt to create a more applicable product.

After the creation of an analysis or a model, the analysis or model must be verified. This can be done one of two ways: comparing future predictions against past data or comparing future predictions against future data. While both verifications are self-explanatory, it is important to note that the accuracy of an analysis or model determines its usefulness. If the statistical analysis or model has been determined to be useful, it can be implemented into an operation. If the analysis has been determined to be inaccurate, the end state of the analysis must be changed to reflect the analysis or the analysis as a whole must be disregarded.

Application in Current Operations

As mentioned earlier, the processes of statistical analysis and mathematical modeling are essential for decision making in United States counterterrorism operations. After understanding the basics of creating a statistical model, one might ask what systems are used in decision making for risk assessment in course of action development. Before one can understand the different systems used, one must understand the basic categories of these systems. There are four basic systems for analyzing a threat. These include a matrix system, a component system, a statistical system, and a hybrid system. A *matrix system* views each component within a scenario as dependent, meaning each factor contributes to the other. Each component is assumed to be related to the other, thus affecting the outcome of the analysis. A *component system* views each component within the scenario as independent, meaning the outcome of the scenario is determined by the sum of the components. Component systems are implemented when there is little or no correlation, proven or unproven, between the components. A *statistical system* focuses on trends and ranges produced from a statistical analysis of past data. Statistical systems are usually used to aid less-complicated decision making or in creating a component or matrix system. A *hybrid system* is a system that uses matrix, component, or statistical systems together in combination to produce a more accurate end product.

With the types of systems loosely established, one can begin to understand the different systems used by the US to assist in decision making. Due to the variability within each system, the US has adopted many analytical systems to assist each organization in making decisions best tailored to their operational focus. Common systems put in place by the US include, but are not limited to, CARVER + Shock, Risk Analysis and Vulnerability Assessment (RAVA), Operational Risk Management (ORM), Five Step Model, Threat/Vulnerability/Risk (TVR) model, and Threat Ensemble Vulnerability Assessment (TEVA) Model (Cupp & Spight). For the purposes of this article, the only systems to be discussed are CARVER + Shock, ORM, and the

TEVA model. These three models give clear examples of a component system, a matrix system, and a statistical system.

The CARVER + Shock (CS) model for assessing a threat is a component system that breaks a situation into seven components to determine a situation's threat level. It is used by US Special Operations Forces (SOF) and the US FDA (Cupp & Spight). The seven components of this system are condensed into the acronym CARVER + Shock, which stands for criticality, accessibility, recuperability, vulnerability, effect, recognizability, and shock (Helferich 2010). Each component is considered independent from another and measures some attribute of a situation to model the threat. *Criticality* is a measure of economic and public impacts; *accessibility* is the ease of access to the potential target; *recuperability* is the potential target's ability to recuperate after an attack; *vulnerability* is the ease of successfully accomplishing an attack on the given target; *effect* is the magnitude of loss after an attack; *recognizability* is how easy the potential target is to recognize; and *shock* is a measure of the social and psychological reaction of an attack on the given target (Ibid).

CS is processed through a software package due to its complexity but offers a formidable threat assessment for COA development. The strength of CS lies in the independence of what is being analyzed or modeled. CARVER + Shock breaks a situation into different aspects that are individually unrelated but cumulatively form a thorough assessment of a situation. Additionally, CS can be adopted to analyze a multitude of scenarios. As mentioned earlier, CS is used by US SOF and FDA, enforcing the applicability of this system. Information regarding the specifics of how SOF uses CS is limited, but when looking at what CS analyzes, it's apparent why Special Operations Forces would use CS. CS can be used to determine the threat of a guerrilla force undermining an anti-American government, assess the likelihood of a terrorist cell attacking an operations center, or even find a weakness within American systems that an aggressor may try to exploit. While CS has many strengths, one weakness is the difficulty in meeting the component criteria, or collecting data. One cannot measure the recuperability of a target without having past experience regarding recovery for an organization. The nature of the data requirement for CS can cause the analysis conflicts because of the difficulty in collecting quality data.

Advancing to an example of a matrix system, the most predominant matrix system used in US operations is ORM, which stands for Operational Risk Management (Cupp & Spight). ORM is used by many components of the US military as well as state and local organizations and focuses on breaking a situation or operation into components where each section progressively builds upon the previous section to formulate an end assessment for decision making (CNIC). Operational Risk Management is commonly used on a work sheet where the results are compared against published tables to give an overall risk assessment. There are five steps to completing ORM for a situation. One must identify the hazards of a situation, assess said hazards, make risk controls, implement controls, then supervise and refine as needed (Ibid). When looking at a scenario or situation, one will first list all potential hazards that may arise during execution of the operation. It is important to note that when identifying hazards, all hazards much be identified. These could include hazards that are thought to be insignificant to hazards that are blatantly obvious. Once the hazards have been listed, they must then be assessed. The assessment includes the severity of the threat and the likelihood of occurrence (Ibid). The severity of a threat refers to the damage incurred if the hazards were to take place, and the likelihood is fairly self-explanatory. Making risk controls is simply coming up with ways to minimize the likelihood or severity of what is considered to be a risk. Once the controls are made, the controls are implemented and overseen as needed.

ORM has one key strength that sets it apart from other systems, in that it provides a hasty system for developing changes and minimizing risks in an operational environment. Because ORM systematically identifies each risk, it gives key decision makers the ability to prioritize different threats that need to be mitigated over others. On the other hand, ORM does not give as thorough an assessment as CS or other similar systems. ORM does not consider other parts of the system that may be a threat, but are not related to a singular component.

The last system to consider is a statistical system. The Threat Ensemble Vulnerability Assessment (TEVA) model is a statistical system that is used primarily by the US Environmental Protection Agency (EPA) to evaluate certain environmental threats (Davis & Janke). The TEVA model follows the statistical/mathematical model creation cycle and the end product is a model/evaluation providing a general range of expected outcomes for the scenario (Ibid). For example, the US EPA uses TEVA in conjunction with certain environmental sensors to collect data for water purity in a given region outside of a manufacturing center (Ibid). As the data is collected, a TEVA model is continuously produced to determine if water purity in a given area is going to remain safe or become dangerous due to external factors.

TEVA is a strong system for producing a forecast for when a region will reach a critical state. As data is collected, TEVA builds a long-range projection of the outcome. While the system collects data, the long range projection begins to narrow due to the previously mentioned principle of normality. Because TEVA produces an initial projection, policy makers can begin planning without fine details. Tentative planning in this manner allows decision makers to maximize time and make a more thorough decision. On the other hand, the weakness to TEVA is its statistical nature. While TEVA will give the most probable outcome of a scenario, decision makers understand that the most probable outcome is not always the actual outcome. TEVA does not give many outcomes for decision makers, reducing the decision makers' effectiveness in making a dynamic decision.

Conclusion

The idea initially placed forward in this paper is that mathematics is essential for counterterrorism operations within the United States. After building a framework for the different operational uses of mathematics, why mathematics is needed in large-scale decision making, the process of analyzing and modeling a scenario for course of action development, and the different analysis systems used within the US, it quickly becomes apparent that mathematics and mathematical analysis are essential for national security on all levels. Mathematics is used in US security operations for research and development and analysis. Research and development is producing essential defense engineering, while analysis is using mathematics to quantify information.

Analysis plays a large part in large-scale decision making within US operational doctrine. Specifically, analysis assists decision makers to test courses of action and determine the best route to take when facing a decision cross road. The steps of analysis/modeling, which are key to understanding the information quantification process, were shown to be establishing what the outcome should be, identifying what parts are involved, collecting data, analyzing data, producing a product, testing a product, then either publishing or refining said product.

Once the steps of analysis were established, the types of models were introduced and an example for certain systems was presented. The four systems mentioned are a component system, a matrix system, a statistical system, and a hybrid system. Three of these four systems

presented in detail to provide an overview of each type of model's uses, strengths, and weaknesses. While some of the listed systems are better suited for long-term analysis, and others are better suited for hasty decision making, one can observe from the listed model that each assists decision makers implement the best control measures in large-scale decision making.

After getting a surface view of mathematical analysis in US security operations, two things become apparent. First, it is critical that policy and decision makers stay well informed before making large-scale decisions. Second, it is critical that policy and decision makers are given information that has been analyzed from a multitude of angles. A thorough analysis comes from looking at data from all angles versus a single perspective. Running a situation through CS alone will give a great understanding of the precise threat in a situation but will fail to prioritize which factors need to be addressed first. Likewise, using TEVA alone will produce a recommendation that is solely based on data analysis rather than an interdependent system. In order to maximize decision making in security operations within the US, policy makers must begin to maximize the use of multiple systems in course of action development rather than focusing on a single system. A COA analyzed using CS, ORM, and TEVA is more likely succeed than a COA analyzed by a single system. It is recommended that in order to improve COA analysis within US security operations, multiple sections must run different analyses simultaneously to offer as many options as possible. Overall, current operations have yielded favorable results and can be expected to repeat this success if they proceed accordingly, but unilateral analysis will maximize the effectiveness of decision making as well as improve overall operational success. Operations must be shifted to accommodate multiple analyses, thus providing a stronger framework for making an operationally and organizationally sound decision.

References

"About DARPA." Defense Advanced Research Projects Agency. 2015. Accessed November 9, 2015.

Anderson, Joseph, and Nathan Slate. "The Case for a Joint Military Decisionmaking Process." The Air University. September 1, 2003. Accessed November 10, 2015.

Clapper, James R., *Statement for the Record Worldwide Threat Assessment of the US Intelligence Community Senate Select Committee on Intelligence*, Washington: Office of the Director of National Intelligence, 2015

Cupp, Shawn, and Michael Spight. "A Homeland Security Model for Assessing US Domestic Threats." Kaplan University. December 1, 2004. Accessed November 13, 2015.

Davis, Michael J., and Robert Janke. "Development of a Probabilistic Timing Model for the Ingestion of Tap Water." Journal Of Water Resources Planning & Management 135, no. 5 (September 2009): 397-405. Environment Complete, EBSCOhost (accessed November 15, 2015).

Druzhinin, V., and D. Kontorov. Decision Making and Automation: Concept, Algorithm, Decision. 1st ed. Moscow: United States Air Force, 1972. 17-42, 80-124, 200-227.

English, Robert D. 2011. "'Merely an Above-Average Product of the Soviet Nomenklatura'? Assessing Leadership in the Cold War's End." International Politics 48 (4-5): 607-626.

Helferich, Omar. "Combating the Impact of Product Counterfeiting: Defining the Growing Risk to Supply Chain Cost and Service Performance." Michigan State University. September 23, 2010. Accessed November 13, 2015.

Lee, Carl, and Felix Famoye. "Data Types and Possible Analysis Techniques." CMU SPSS On-Line Training Workshop. 2015. Accessed November 12, 2015.

"Operational Risk Management." CNIC. Accessed November 13, 2015.

Siegrist, Kyle. "The Central Limit Theorem." Random: Probability, Mathematical Statistics, Stochastic Processes. 2015. Accessed November 12, 2015.

Snijders, Tom, and Roel Bosker. Multilevel Analysis: An Introduction to Basic and Advanced Multilevel Modeling. 1st ed. Thousand Oaks, California: Sage Publications, 2003. 1-9.

Walpole, Ronald, Raymond Myers, Sharon Myers, and Keying Ye. Probability & Statistics for Engineers & Scientists. 9th ed. Boston, MA: Pearson, 2012. 1-17.