JOURNAL OF
EMERGING INVESTIGATORS

Article

A statistical comparison of the Simultaneous Attack/ Persistent Pursuit Theory against current methods in counterterrorism using a stochastic model

Paarth Tara, Preeti Tara
Eastern Alamance High School, Mebane, North Carolina

SUMMARY

Though current strategies in counterterrorism are somewhat effective, various counterinsurgency theorists have raised doubts about the true efficacy of current methods. Established current strategies are fundamentally flawed, with an overemphasis on eliminating leaders and highly connected agents. Colonel Derek Jones, a counterinsurgency theorist, proposed the Simultaneous Attack/Persistent Pursuit (SAPP) Theory as a superior alternative to current methods. In this strategy, attacks are conducted equally across all fronts of a clandestine intelligence network, from which connections are pursued with further attacks. To determine whether current methods are more or less effective in counterterrorism than the method proposed by the SAPP Theory, a stochastic computational model was developed to represent a traditional eastern clandestine network for an isolated sub-cell of a terrorist organization. Attacks were modeled through the loss of agents within specific components of the network. After an analysis of relevant literature discussing the efficacy of current methods in counterterrorism, we hypothesized that the SAPP model would lead to a greater reduction in the number of terrorist attacks than other methods. We simulated five attack strategies, with each strategy being simulated for thirty trials, and the resulting final number of attacks of the terrorist network was recorded. Through four two-sample t-tests comparing each of the four non-SAPP strategies to the SAPP model, we concluded that the SAPP model was significantly more effective in reducing the final number of terrorist attacks. This demonstrates the comparative advantage of utilizing the SAPP model, which may prove to be critical in future efforts in counterterrorism.

INTRODUCTION

With a growing influence of terrorist organizations worldwide, human life and global peace are increasingly threatened throughout the world. These terrorist organizations often structure themselves in clandestine cell systems, which are a type of decentralized intelligence network in which individual members are not fully aware of either their role in the network, nor the existence of members outside of their localized group of agents (1). This research aims to understand both the nature of clandestine networks and strategies for combating these networks through computational methods.

Many terrorist organizations throughout the world have decentralized intelligence structures (2). Though many other intelligence systems are heavily dependent on leaders and plentiful connections between members (or agents), clandestine cell systems tend to place less of an importance on both of these components.

Most clandestine practitioners adopt clandestine networks in an effort to be resistant to the compromise—in the context of this research, the elimination of members through counterinsurgency—of agents within a network. Components of a clandestine network are isolated from one another to ensure that individual cells do not compromise information. This decentralized method of operation—referring to the nature of an intelligence structure to be arranged in such a manner that there are multiple leader agents distributed throughout the network, each with significant independence and control over localized portions of the whole network, yet bound together through their affiliation with the terrorist organization—also ensures that individual agents are sometimes unaware of their purpose in the network, uninformed of other members, and are unconnected to vital components of the network. Clandestine cells also place less of an importance on the loss of individual agents within a network, making the process of rebounding from an attack far more efficient.

Before analyzing strategies to combat these clandestine cell systems, it is important to differentiate between the various types. Western clandestine cell systems are more hierarchical in structure (**Figure 1**), with a more defined structure than eastern counterparts. Eastern clandestine cell systems are more loosely distributed (**Figure 2**), with many components of the network being structured in a ring-like form. In this research, we only considered eastern clandestine cell systems, for they are more closely linked to the form of major eastern terrorist organizations, which are the primary sources of modern global terrorism (1).

Due to the specific characteristics of clandestine networks, many counterinsurgency theorists question current strategies in counterterrorism (1, 3). Jordan *et al.* stated that these

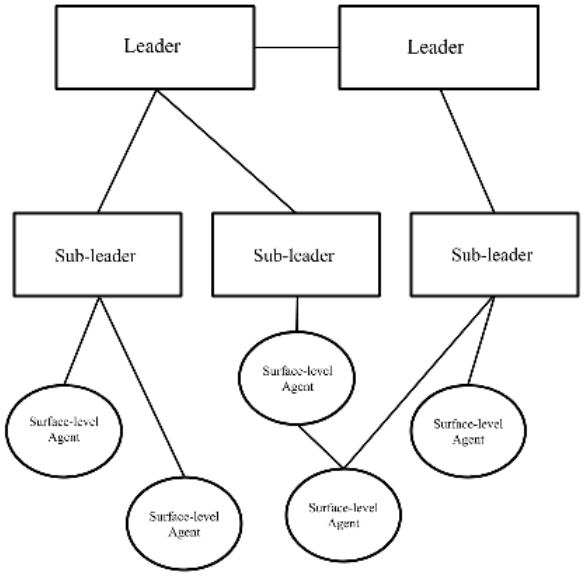

Figure 1. An abstract model of a western clandestine network. Boxes and circles both denote individual agents, and the text inside the enclosures indicates the position of the agent within the network. Lines from one enclosure to another indicate a connection. Connections occur from leaders to agents and from agents to agents in the real world. However, only the former is shown.

current strategies are too focused on the elimination of network leaders (3). These strategies are flawed because clandestine cell systems used by terrorist organizations often utilize their leaders to establish ideological unity (1). The group ideology of a terrorist organization motivates its actions and establishes a common purpose across all of its members (1). Without this group ideology, the organization could not function as effectively, for the decentralized nature of the organization would make it difficult to unite various components of the network under one common purpose. It is the job of the leaders of these organizations to enforce this ideological unity across the organization. Therefore, most leaders in these types of terrorist organizations rarely serve an operational role¬—one in which they conduct logistical and managerial tasks—instead opting to solely focus on establishing ideological unity across the organization. Through this, while it becomes clear how the rationale develops that eliminating the leaders of these types of terrorist organizations may lead to a reduction in the ideological unity of the organization, this strategy would not significantly affect the operational aspects of that organization.

Similarly, some counterinsurgency theorists claim that current strategies place an overemphasis on eliminating agents with large numbers of connections, as it is perceived that these agents have greater importance (1). Jones stated that these efforts only act to "cull the herd of poor clandestine practitioners" (1). Though in other intelligence networks, highly connected agents might be of greater importance than less-connected agents, this is not the case in clandestine networks. Instead, these networks aim to isolate components of the organization, especially those with vital roles. It is because of this that important agents are often less connected, as to minimize the probability of their compromise—that is, to minimize the probability of their elimination from the network due to a counterinsurgency effort (1). Those with larger amounts of connections are often highly prone to being compromised, and thus given less important roles, for they are less experienced clandestine practitioners. It is through this analysis that Jones asserted that current strategies in counterterrorism have failed to truly eliminate vital components of clandestine organizations, instead eliminating relatively useless agents of the organization (1). Through these criticisms, clandestine theorists have proposed novel strategies in combating terrorism.

The Simultaneous Attack/Persistent Pursuit (SAPP) Theory is a superior alternative to current methods in counterterrorism (1, 2). The SAPP Theory asserts that the simultaneous attack on all fronts of a clandestine terrorist network, followed by the pursuit of connected agents, will lead to the greatest damage to a clandestine system (**Figure 3**).

To compare the Simultaneous Attack/Persistent Pursuit (SAPP) Theory with other methods of counterterrorism, we developed a stochastic computational model of a clandestine network. Our model represented a traditional eastern clandestine network of an isolated sub-cell of a terrorist organization. We hypothesized that the SAPP Theory would lead to a statistically significant decrease in the number of terrorist attacks an organization was able to commit over a standard period of time, when compared to other strategies of counterterrorism. Our results supported our hypothesis, leading to the conclusion that it is probable that the SAPP

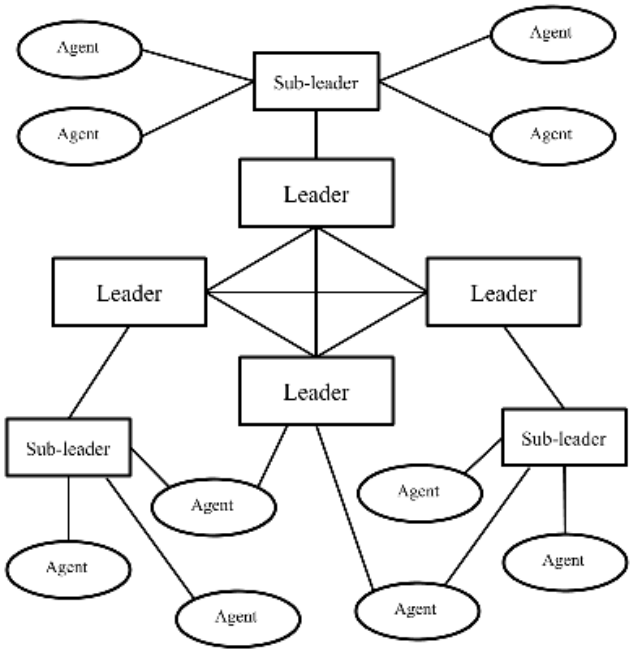

Figure 2. An abstract model of an eastern clandestine network. Boxes and circles denote individual agents, and the text inside the enclosures indicates the position of the agent within the network. Lines from one enclosure to another indicate a connection. Both leader-to-agent and agent-to-agent connections are shown.

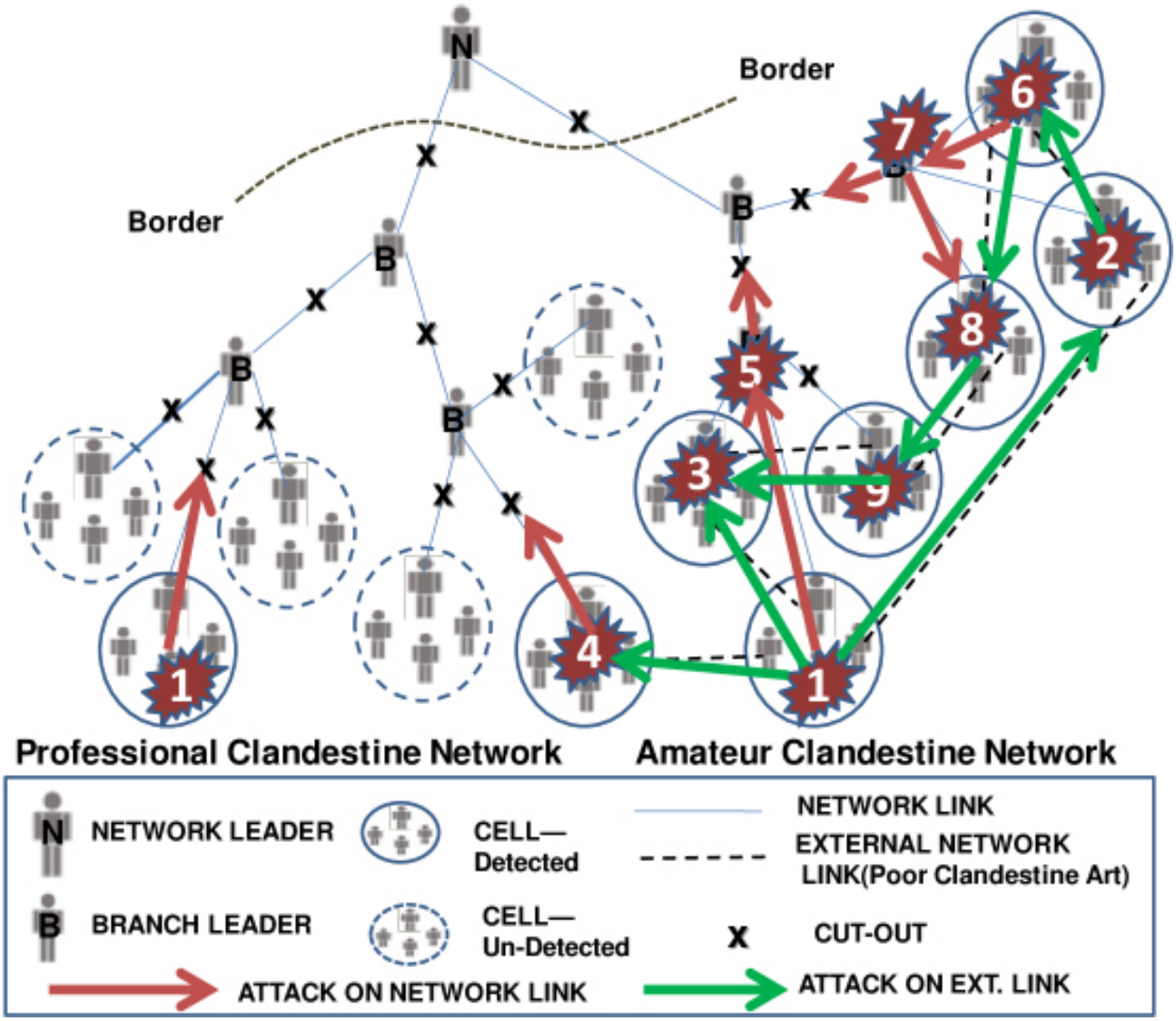

Figure 3. Visualization of pursuit through a clandestine network. Figure adapted from Jones (1). Agents are denoted with illustrations of people. Circles indicate that the agents within the enclosures are in individual units (referred to as cells). In appearance, undetected cells are solid, while detected cells are dotted. Lines between agents and cells denote connections. Solid connection lines indicate a strong link, while dotted lines indicate a weak link. Connections with dotted lines are easier to compromise. The label of the character "N" on an agent indicates that they are the leader of this portion of the clandestine network. The label of the character "B" on an agent indicates that they are a sub-leader of this portion of the clandestine network. The label of the character "X" on a connection indicates that it has been compromised. Solid red arrows indicate a counterinsurgent attack on a connection, while solid green arrows indicate a counterinsurgent attack on an agent or cell. SAPP Theory is demonstrated in this figure; the existence of multiple arrows indicates a simultaneous attack on all fronts of the exposed network, while the existence of multiple layers of arrows indicates a pursuit of agents through the network.

Theory is more effective in counterterrorism than current methods.

RESULTS

We developed a computational model to simulate a clandestine sub-cell network, and then applied various treatments onto the model to simulate different attack strategies. The simulated sub-cell network contained 4 simulated components: a propaganda cell, a recruitment logistics cell, a central logistics cell, and an operations cell. Using this model, it was possible to observe differences in the efficiency of the terrorist sub-cell network, operationally defined by the final number of terrorist attacks performed by the simulated terrorist network.

We ran the attack strategy associated with each of five treatments—Treatment O (attacks are only performed on the operations cell), Treatment P (attacks are only performed on the propaganda cell), Treatment C (attacks are only performed on the central logistics cell), Treatment R (attacks are only performed on the recruitment logistics cell), and Treatment S (attacks are performed using the SAPP strategy)—for 30 iterations and recording the final number of terrorist attacks

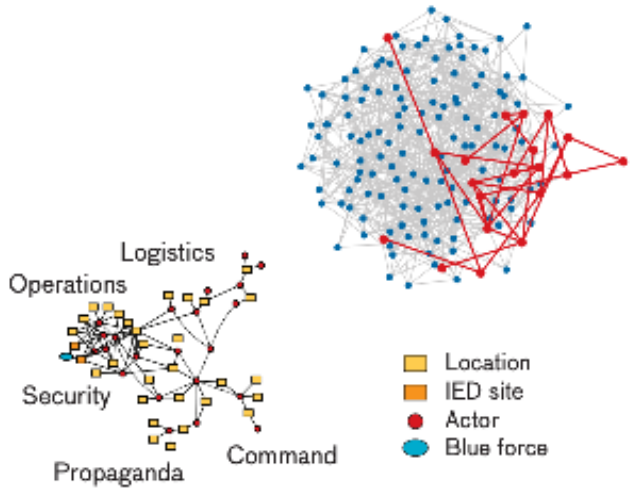

Figure 4. Inspiration for the structure of the simulated terrorist sub-cell. Figured adapted from Smith *et al.* (6). On the top right, the overall arrangement of the complete covert network is visualized. On the bottom left, a portion of that network is compartmentalized into five sections: Operations, Logistics, Security, Propaganda, and Command. Yellow boxes indicate physical locations within the network. Orange boxes indicate the existence of improvised explosive devices (IEDs). Red circles denote agents, or members of the terrorist organization. Blue circles represent sites where access of surface agents is available for counterinsurgency. The structure of this section of the covert network serves as an inspiration for the clandestine network in this research.

(A_{final}) at the end of 50 time steps for each iteration. These treatments were partially inspired by a model representing terrorist organizations as covert networks (**Figure 4**). We selected the amount of iterations to ensure the condition for sample-size was met to perform a two-sample t-test on any two of the treatments. Generally, the number of terrorist attacks (A_{final}) progressed linearly as the simulation proceeded for every iteration of every treatment. The specific rate of the linear progression differed between trials.

In this study, the probability of the elimination of an agent (member) from each cell differed. There was a 100% probability of removing an agent from the operations cell, a 90% chance of removing an agent from the propaganda cell, a 70% chance of removing an agent from the recruitment logistics cell, and a 20% chance of removing an agent from the central logistics cell. These probabilities were determined with the consideration of the inherent security some cells provide to their agents, which is related to how close agents within a cell have to interact with entities outside of the terrorist network. Members of the operations cell have to interact directly with entities outside the network, while agents from the propaganda cell have to interact less directly with those entities. Members from the recruitment logistics cell have to only collect and train incoming agents, which causes them to have an even less chance of being compromised. Members of the central logistics cell have mainly managerial roles, giving them little necessity to interact with the outside world. These probabilities were some of the most critical parameters in this experiment.

For the set of 30 values of A_{final} for each of the 5 treatments, we recorded the values of the sample size, mean, standard deviation, and standard error (**Table 1**). We performed t-tests on each individual treatment compared to Treatment S (**Table 2**).

Through the utilization of an α=0.01 significance level (as to minimize the probability of a Type I error), we established significance for each of the four two-sample t-tests. However, because multiple t-tests were made, erroneous results were more probable, and thus it was necessary to use multiple-testing adjustment of the significance level. To accomplish this, we used the Benjamini-Hochman Procedure. We used a standard false discovery rate of 5% throughout this procedure. We then recorded the critical values, ranking, adjusted p-value, and significance after the Benjamini-Hochman procedure for each of the four two-sample t-tests (**Table 2**). Through this, we determined significance for all two-sample t-tests, hinting that Treatment S was more effective in decreasing the value of A_{final} when compared to the other treatments.

DISCUSSION

The results from this experiment showed that the differences between the value of A_{final} for Treatment S and the values of A_{final} for the other treatments were statistically significant, supporting the hypothesis that the SAPP Theory was more effective in decreasing the number of terrorist attacks an organization was able to conduct when compared to other methods. We found that Treatment S was more effective in decreasing the number of terrorist attacks than any of the other treatments. Because Treatment S represented the SAPP model, we were able to support the hypothesis that the SAPP strategy would lead to a greater reduction in the number of terrorist attacks. It is important to understand that this data was only derived based on simulated attacks on a specific simulated configuration of a terrorist sub-cell. Because of this, further experimentation is necessary to decisively implement new strategies in counterterrorism.

The probabilities of the successful elimination of agents (members) from each cell in the model were critical parameters in the experiment. In order to simulate the security some cells inherently had from counterinsurgency attacks when

Treatment	N	Mean	SD	SE
Propaganda	30	70.4	4.95	0.9
Recruitment Logistics	30	70.6	4.11	0.75
Central Logistics	30	69.4	4.55	0.83
Operations	30	69.07	3.65	0.67
SAPP Theory	30	60.6	18.6	3.4

Table 1. Arrangement of all five treatments in this experiment with their associated sample size (N), mean of A_{final}, standard deviation (SD), and standard error (SE).

Rank	Treatment	Original P-value	Critical Value	Adjusted P-value	Significant at FDR = 0.05
1	Propaganda	0.004	0.0125	0.016	Yes
2	Recruitment Logistics	0.004	0.025	0.008	Yes
3	Central Logistics	0.008	0.0375	0.01067	Yes
4	Operations	0.01	0.05	0.01	Yes

Table 2. Arrangement of each treatment which was compared with Treatment S (SAPP Theory) with its rank, Original *p*-value, critical value, Benjamini-Hochberg Adjusted *p*-value, and significance. The Benjamini-Hochberg procedure was followed to ensure statistical significance when comparing the SAPP treatment group with all other treatment groups, and the critical value statistic is an intermediary value necessary to determine significance using the Benjamini-Hochberg procedure.

compared to others, we differed these probabilities across different cells (1). We determined the specific values used in this experiment with a combination of arbitrary intuition and academic evidence (1, 4).

A possible source of error in this research was the randomness which was introduced because of the nature of our stochastic model. It was possible that the recorded data occurred due to random chance. However, the randomness of this model would probably not have played such an important role, for 30 trials were taken to minimize the effects of this.

One of the largest possible sources of error was the model design itself. Though we designed the model with consideration of available scholarly information, it was possible that it did not truly reflect the realistic structure and conditions of an eastern clandestine terrorist network. This model was only one of many different types of models which could have been made to simulate a clandestine terrorist network. Because of this, further development of new models, as well as an increase in the amount of available information about real-world clandestine networks, is necessary. Only estimations of terrorist networks could be made computationally with the limited amount of information available. In order to minimize this source of error, it would be necessary to conduct further experiments on other models of clandestine terrorist networks, especially if future research and military disclosures reveal further insight into the nature of these networks.

These results indicate that it is important to continue studying clandestine terrorist networks computationally. Though these results on their own will not fully prove that the SAPP model is more effective than current strategies, the repetition of this experiment, as well as similar experiments, is necessary for the development of more complete results. This research can serve as a foundation for future research into the utilization of computational methods in studying clandestine networks.

Many questions about the nature of clandestine networks remain. Information on the true structure of many terrorist networks, as found in the real world, would be significantly important in the development of this field. The role of ideological uniformity in such an organization, the growth and development mechanics of full clandestine terrorist networks, as well as the comparative advantages of different types of strategies in counterterrorism are all important topics in this field of research which need to be studied in order to offer truly important and influential results. Without further research and experimentation of this model, as well as similar models, it is not possible to definitively assert that certain strategies for counterterrorism are superior to others. Nevertheless, this research provides very important results on the efficacy of the SAPP strategy when compared to current strategies in counterterrorism and presents a basis for discussions in the future on the use of computational tools in the efforts to optimize counterterrorist efforts.

METHODS

The code of the model used in this research was programmed in Python 3.6 and is available on GitHub (5).

Past research has shown five major components in a covert network, as shown in **Figure 4**—a network which attempts to conceal information about its structure and function from outside of the network: operations, logistics, security, propaganda, and command (6). Similarly, Li Bo, *et al.* gave an outline of five components of a sub-cell structure in a terrorist network: the action cell, the conduct cell, the resource cell, the recruit cell, and the training cell (4). Through these inspirations, the general model of the clandestine sub-cell in this research contained four components: the operations cell, the propaganda cell, the recruitment logistics cell, and the central logistics cell. The operations cell contained agents and resources which would be used to conduct simulated terrorist attacks. The propaganda cell dispersed propaganda to aid in the recruitment of new agents. The recruitment logistics cell aided in the collection and training of new recruits in the organization. The number of agents in the propaganda and recruitment logistics cell influenced the number of agents added into the organization after each time step of the simulation. The central logistics cell collected resources, directed attacks, provided ideological unification, and directed humans and weaponry throughout the network. Both the number of agents and resources in the operations cell and central logistics cell influenced the probability and frequency of successful terrorist attacks. In this simulation, each time step represented a single unit of time passing in the simulation. Equivalence to the length of this time step in the real world could not be determined without specific information about the form, function, and history of a particular terrorist organization.

$$G(\phi,\lambda) = \left\lceil \left\lfloor 1.2^{\phi} \right\rfloor \cdot \left(\frac{\left\lfloor \frac{51}{1+e^{-0.27(\lambda-15)}} \right\rfloor}{100} \right) \right\rceil$$

Figure 5. Mathematical equation of the *G*(ϕ,λ) equation.

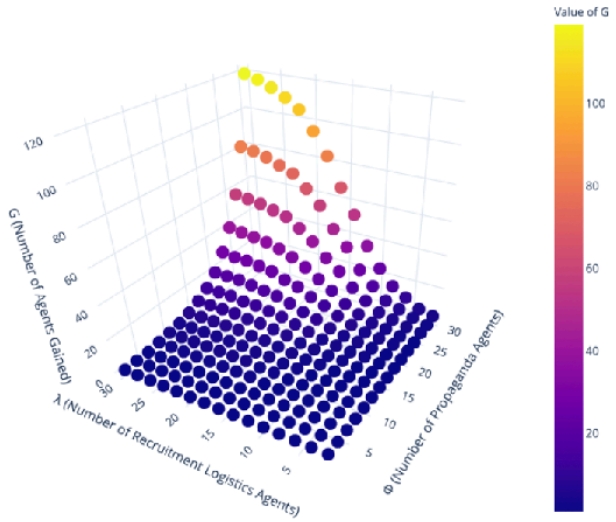

Figure 6. A three-dimensional scatter plot representing values of the G function for a total of 225 value-pairs of ϕ and λ. ϕ ranges from 2 to 30, increasing by steps of 2. λ ranges from 2 to 30, increasing by steps of 2. *G* ranges from 1 to 119.

We applied five treatments to this simulated network. Treatment O only attacked the agents in the operations cell. Treatment P only attacked the agents in the propaganda cell. Treatment R only attacked the agents in the recruitment logistics cell. Treatment C only attacked the agents in the central logistics cell. Treatment S attacked all cells of the network pseudo-randomly, with each cell being given an equal probability to be attacked, leading to a relative equivalence in the attack distribution across all cells of the network. In this case, the best representation of current strategies was with Treatments O and C, while the best representation of the SAPP strategy was with Treatment S (1, 2).

The number of terrorist attacks which occurred in a certain time step depended on the number of agents within the central logistics cell and the operations cell. For each terrorist attack to occur, four agents were required from the operations cell, while only two agents were required from the central logistics cell. This means that a total of six members from the central logistics and operations cell were required to conduct a terrorist attack. Depending on the number of agents within each of the two cells, the maximum possible number of terrorist attacks would be conducted. Each terrorist attack had a 70% chance of being successful. If a terrorist attack was successful, the number of terrorist attacks in the simulation was increased by 1 (A := A + 1). If not, the number of terrorist attacks remained constant.

We represented the number of agents entering a terrorist network through the $G(\phi,\lambda)$ function (**Figure 5**). ϕ represented the number of agents within the propaganda cell, while λ represented the number of agents within the recruitment logistics cell. With consideration of the nature of eastern clandestine terrorist networks, we determined that an increase in the number of agents in the propaganda cell would lead to an exponential increase in the number of individuals available for recruitment (4). It was also determined that the recruitment logistics cell would always perform only to a threshold in its recruitment efforts, as going beyond that threshold would risk an increased probability in the members of the cell being compromised (4). Thus, we determined that the percent of the available pool of recruits which would be recruited would be determined by the capacity of the recruitment logistics cell to operate, which was operationally defined as the number of agents within the Recruitment Logistics cell, or \lambda. Thus, we developed a logistic expression based on the value of \ lambda was to return a value between 0 and 50%, depending on the number of agents within the recruitment logistics cell. We multiplied this expression with the exponential expression of the propaganda cell and put the result through a ceiling operator. The logistic expression contained a flooring operator in order to ensure that the value of the expression remained between 0 and 50%. We floored the exponential expression arbitrarily. The flooring or ceiling of the exponential expression, as well as the overall expression, would not have mattered for the general results, as they would have only produced relatively small deviations. We added $G(\phi,\lambda)$ agents into the network, with each agent being assigned to a component pseudo-randomly, and with equal probability of entering each component. When computing the value of $G(\phi,\lambda)$ across a range of values of ϕ and λ, it was possible to see that the value of G was a product of a logistic and exponential expression (**Figure 6**).

For every time step, we removed a random number of agents—operationally equivalent to members of a terrorist organization— (from 0 to 3) from the components of the sub-cell network by the treatment applied. This variation was used to simulate the security some cells inherently have when compared to other cells (1).

The model started with eight members in the operations cell, six members in the propaganda cell, six members in the recruitment logistics cell, and four members in the central logistics cell. Optimal initial conditions for this simulation, in this context, referred to the conditions which best allow for the minimization of the time it takes to perform the simulation fully. We determined the initial values for each cell through testing the optimal initial conditions of the simulation on our system.

ACKNOWLEDGEMENTS

I would like to thank my science and math teachers, especially Mrs. Shelley Casey and Mr. Brian Ewbank, for consistently supporting my work.

Published: December 1, 2020

REFERENCES

1. Jones, Derek. *Understanding the Form, Function, and Logic of Clandestine Cellular Networks: The First Step in Effective Counternetwork Operations*. Defense Technical

Information Center, 2009, *Defense Technical Information Center*, apps.dtic.mil/sti/pdfs/ADA505161.pdf.
2. Jones, Derek. *A Military Theory for Destroying Clandestine Insurgent and Terrorist Organizations.* United States Army War College, 2017, https://publications.armywarcollege.edu/pubs/3434.pdf.
3. Jordan, Jenna. "Attacking the Leader, Missing the Mark: Why Terrorist Groups Survive Decapitation Strikes." *The MIT Press Journals*, 28 May 2014, www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00157.
4. Li, Bo, *et al*. "Agent Based Modeling on Organizational Dynamics of Terrorist Network." *Hindawi,* 11 Nov. 2015, www.hindawi.com/journals/ddns/2015/237809/.
5. hello.py. isef2020, commit b6eb7bcac0a66b70e80964f320a6cfb33a80c751, Paarth Tara, 2020. GitHub, https://github.com/VioletIzHere/isef2020/blob/master/hello.py.
6. Smith, Steven T., *et al*. "Covert Network Detection." *MIT Lincoln Laboratory,* Jan. 2013, www.ll.mit.edu/sites/default/files/page/doc/2018-05/20_1_4_Smith.pdf.