Developing STORM, a Methodology for Evaluating Transit Routes of Transnational Terrorists and Criminals

Mark T. Clark and Brian Janiskee

> **"The IFA asked the group to assess why terrorist groups or criminal transnational organizations select certain transit countries for their purposes."**

Introduction

In July 2008, a California State University (CSU) consortium became the first academic organization to accept a "challenge project" from the NSA's Institute for Analysis (IFA). A challenge project consists of a question for which the IFA seeks a fresh answer from outside the Intelligence Community (IC). The grant process begins with individual NSA analysts who approach the IFA with particularly vexing questions. IFA then evaluates these for their importance, timeliness, and suitability to outside research. Once the IFA approves a question for a challenge project, the question is reframed to make it suitable for open-source research by whatever group is assigned the grant.

Challenge projects vary in complexity. Some involve a direct, one-time answer to a highly specialized question. Others, however, are more extensive and require the group taking the challenge not only to answer the question but also to provide a reproducible methodology. Customarily, these challenges are contracted out to private firms. However, the IFA recently opened the process to universities identified by the Office of the Director of National Intelligence (ODNI) as "Intelligence Community Centers of Academic Excellence" (IC CAE).[a] The CSU consortium is one of these centers and accepted the first such challenge offered to a university group.

The Problem

The project CSU took on was labeled the "Transit Country Problem." In a nutshell, the IFA asked the group to assess why terrorist groups or criminal transnational organizations select certain transit countries for their purposes. The report was due in the spring of 2009.

[a] Through its ICCAE program office, the ODNI awards grants competitively to universities nationwide to develop and diversify the pool of potential applicants for careers in intelligence. As of this writing, 17 universities participate in the program. The California State University IC CAE program is unique in that it is a consortium of seven California state universities in southern California. For more information in the ODNI's Intelligence Community Centers of Academic Excellence program, please see: http://www.dni.gov/cae/index.htm.

All statements of fact, opinion, or analysis expressed in this article are those of the authors. Nothing in the article should be construed as asserting or implying US government endorsement of an article's factual statements and interpretations.

Our approach from the beginning was to incorporate the challenge project into classrooms.

Our initial goal in CSU was to focus on the terrorist component of the problem and only later develop a methodology to include criminal organizations.

The Approach

In thinking about how we would meet the challenge, we decided to answer the question collaboratively by exploiting what we believe in the CSU IC CAE is a comparative advantage in collaborative work. First, we had experience in working collaboratively as a consortium of seven universities in the CSU system on the goals and objectives of the IC CAE grant received from the ODNI in September 2006.[a] This relationship requires the coordination of faculty, staff, and students across seven campuses, in different disciplines, and in very different academic cultures.[b] As importantly, the director of the program must coordinate the efforts of the consortium with the CSU Chancellor's Office and the ODNI. Second, we have a diverse talent pool of faculty and students—in graduate and undergraduate programs—who specialize in the following key subject areas: terrorism, intelligence studies, research methods, the sociology of terrorism, and geographic information systems.

Given the academic mission of the CSU consortium, our approach from the beginning was to incorporate the challenge project into classrooms. The faculty members who participated in the project ensured that the project would add significant academic value to the student experience.

Three courses seemed to fit best the scope and subject matter in the challenge. Two were in the graduate program in national security studies at CSU San Bernardino. One was in the undergraduate sociology program at CSU Northridge. The two graduate courses selected at CSU San Bernardino were Tracking Terrorism and American Foreign Policy. The undergraduate course selected at CSU Northridge was Sociology of Terrorism. On standby at CSU Long Beach, we had faculty and graduate assistants available for any geographic information systems (GIS) work we may have needed.

Organization

Our initial organizational structure for the project was in place by September 2008. (Our report was due to the IFA in January 2009.) The director of the CSU consortium served as the overall coordinator. The three course instructors were team leaders responsible for supervising the research process in each class. These instructors divided their classes into research subteams to further analyze specific elements of the research question. A graduate student provided assistance to the director. Later, another faculty member was brought in as a principal analyst.

Getting Started

Representatives of the IFA came to Southern California to brief the faculty and students on the transit country project and the contribution the consortium could make to solve the puzzle. For one class—the graduate course on American Foreign Policy—the IFA representatives were present for the first class meeting. The professor introduced the consortium director, who told the students about the challenge project and the role they would play in it. After the director's background discussion of the project, the IFA representatives addressed the class. They made it clear that this was an opportunity for the students and faculty to work on a real

[a] The seven universities include the following California State University system campuses: Bakersfield, Cal Poly Pomona, Dominguez Hills, Fullerton, Long Beach, Northridge, and San Bernardino. The program is directed out of CSU San Bernardino's national security studies (MA) program, which is housed in the Department of Political Science. Please see: www.csu-ace.org.

[b] The disciplines include computer science, criminal justice, geographic information systems, political science and sociology at the undergraduate level, and national security studies at the graduate (MA) level.

question in need of fresh answers. To put it mildly, the students were surprised and a little intimidated by the prospect of researching the challenge. Once they got into it, however, the students were energized by working on the question in the classroom, knowing that there would be a final report to the IFA and, if the quality was good enough, that it would contribute to the overall mission of the IC. We made clear to the students that each professor would be free to approach the challenge in his or her own way and that the students were allowed, indeed encouraged, to explore novel approaches.

On the second day of the IFA visit, we held a video teleconference (VTC) from the San Bernardino campus to brief the faculty researchers on the other campuses about the challenge project. We conducted two more VTCs that fall involving the same teams to ensure we were on track and to discuss issues or answer questions that arose during the students' research. At no time, however, did anyone from the IFA ask for or intimate an "acceptable" outcome for the project. Representatives repeatedly indicated they wanted our research to be genuinely free of influence from an "IC" perspective. To that end, faculty who had access to Intellipedia and proprietary sources of information rigorously avoided using that data or steering students toward it. Furthermore, IFA representatives reiterated several times that even a "failure" to find an acceptable answer to the challenge would be a useful answer in itself.

Faculty who had access to Intellipedia and proprietary sources of information rigorously avoided using that data or steering students toward it.

One Question, Three Research Teams: Diversity of Viewpoint and Redundant Systems

The research approaches the faculty took were unique. For the American Foreign Policy class, the faculty decided to have students research eight different countries as potential transit points and three major pathologies that could be associated with potential transit countries. Some students approached the question with the nation as the object of analysis, while others made a specific pathology the object of analysis, following the trouble wherever the research led. The eight countries were: the Bahamas, Brazil, Bulgaria, Canada, Georgia, Romania, Serbia, and Turkey. The three pathologies were weapons smuggling, nuclear materials smuggling, and human trafficking. Students were divided into country study teams and pathology teams. The teams were expected to provide weekly reports to their professors.

For the Tracking Terrorism class, the professor changed the definition of a key term, and then organized teams of students to conduct research. The professor thought that the term *transit country* was not particularly well defined. He developed a new term: "*terrorist node of operation* (TNOP)." He defined a TNOP as "a physical area possessing certain geographic, structural, and sociopolitical characteristics making it useful for a terrorist organization to operate." The professor thought the term *transit country* implied a subset of countries that was too small and the term itself was too narrow to answer the question fully.

The professor then divided the students into three teams. The first, the Terrorist Threat Group Team, looked at the question from the point of view of the terrorist group. This resembled the focus of the pathology team in the American Foreign Policy class. The students on the Terrorist Threat Group Team followed the research results to wherever they led, without having in mind a particular set of TNOPs. The second group, the TNOP Focus Group, looked at specific countries in particular regions—such as the Middle East, Europe, North and Trans-Saharan Africa—to determine what qualities they had that would make them useful to terrorists. The third group, the Exploitation Team, had access

We decided on multiple approaches … to cast the net widely to capture as many good ideas as possible.

to the ongoing research of the first two teams. Its job was to synthesize the results into a coherent report.

The third class to participate in the challenge project was the Sociology of Terrorism course. As was the case with the other two classes, the professor took yet another approach. He organized the research project so students would develop something resembling a transit countries indicators and warnings (I&W) model. He then used four measures by which the students could evaluate chains of transit countries for the movement of terrorist groups. The measures were guns (arms smuggling and dealing), drugs (traditional routes for the movement of illegal drugs), human trafficking, and corruption.

The professor also recommended that students engage in two novel approaches. The first was "internet treble hooking." A single student or group of students would monitor open source information from a specific country for activities once that country was deemed to be a potential conduit for illegal transit activities. The second approach was "spark plugging." This involves a targeted dialogue—on message boards, for example—with specific experts familiar with a particular country or activity under consideration.

We decided on multiple avenues of research for two reasons. First, we wanted to cast the net widely to capture as many good ideas as possible. The multiple approaches taken to this problem would help ensure thoroughness in research and avoid some of the inherent biases that may come from a single approach. Second, we wanted to ensure the delivery of a product. With three separate groups working on the project, a research roadblock faced by one class would not, accordingly, jeopardize the whole endeavor.

We took our responsibility to deliver a product with the utmost seriousness. Redundancy would allow us to carry on if one part of the project, for whatever reason, was interrupted.[a]

As a multicampus consortium, though we collaborate on the overall goals of the ODNI grant, we allow individual differences to flourish. We seek to benefit from different disciplinary approaches and different educational cultures on our campuses and leave plenty of room for local innovations. Notwithstanding our experience in collaboration, we had never attempted to collaborate on such a large project before and, frankly, did not really know whether one or more approach would actually produce something of value or whether one or more faculty members would shepherd their projects to timely conclusions.

As the fall term came to an end and the three teams were in the process of delivering their final results, the overall coordinator of the project faced the task of getting a single product to the IFA. We would not be satisfied with a straightforward compilation of several reports for the IFA. We sought to integrate the classroom research products into a single approach with a reproducible methodology. The director of the CSU program feared that this would expose the biggest potential weakness in our collaboration—a lack of cohesion. We needed to forge the answers achieved in the three approaches into a single answer with a robust methodology that could be useful to intelligence analysts in their day-to-day work.

[a] The need for redundancy was very nearly realized. One of the participating professors, a military reservist, was unexpectedly recalled to active duty. He received news of this just a few weeks before the project deadline. Fortunately, he insisted on seeing the project through to completion and his final class report was turned in two days before he shipped out. In this instance, we did not suffer a failure in one of our systems, but we had confirmed the wisdom, in projects of this scope, to expect the unexpected and to take organizational steps to ensure that a product is delivered.

The need for a principal analyst for a multi-team project like this became evident early in the process.

Three Research Teams, One Product: The Role of the Principal Analyst

Fortuitously, however, one faculty member who was aware of the process but uninvolved in classroom research for it offered his services at the right time to help integrate the reports. He also brought to the table considerable methodological skills. We had promised to have something by late January, so this individual had to work overtime during his winter break to develop our final approach. In collaboration with the coordinator, usually by phone, but also over lunch, our principal analyst read, analyzed, and synthesized faculty and student reports—well over 400 pages—into a creative, and useful methodology we called STORM (Security threat, Target, Operation, Resources, Movement pattern).

The need for a principal analyst for a multiteam project like this became evident early in the process. Students across all groups quickly discovered that a significant number of open source metrics were bad, corrupted, or simply unreliable. For example, the subject of human trafficking is fraught with difficulties. Some countries try to combat it, others ignore it, and still others hide it. Yet every student group reported finding metrics for it. More troubling, the definition of human trafficking was found to be different across databases. In some databases, anyone involved in the sex trade was counted as part of the overall human trafficking pattern. In others, anyone who ever accepted "pay" for sex acts were not counted as victims of human trafficking, even if they were first forced into sex slavery. Moreover, only a few nations try to track it and those that do—like the United States, which has spent over $371 million since 2001 on this issue—have no assessment on whether such efforts have prevented any human trafficking. The same was true for databases on political corruption, arms smuggling, and drug smuggling. So, when the principal analyst began evaluating all the data, it became clear to us that we needed to substitute qualitative proxies for poor, incomplete, or unreliable quantitative measures. But the proxies he identified had to be able to accommodate quantitative data of high quality, once they could be identified.

STORM

The methodology's name, STORM, served as a mnemonic device to help analysts methodically identify potential "nodes of operation."[a] In coming up with the acronym, we, in essence, determined that asking questions about transit countries was not the preferred first step. The concept of a transit country implies that there are a limited number of countries that can act as conduits for terrorist or criminal activity. Instead, we thought that any country in the world could serve as a transit country, depending on a number of conditions. In the STORM process, we first had the analyst ask questions about the group, its goals, its objectives, and its resource needs before asking which countries might become transit countries, or nodes of operation.

The different approaches to the problem paid off here as well. After having developed the term *terrorist node of operation* in one class, the principal analyst determined that it suited the purposes of the overall report better simply to use *node of operation* to include terrorist groups and criminal transnational organizations.

Second, we also determined that because open-source data can be corrupted, we used qualitative proxies for various pathologies. For example, if the data for arms trafficking are bad, qualitative proxies such as the presence of civil wars or insurgencies could be used. (A

[a] See the unclassified Intellipedia article on transit country and the report, "STORM: A Methodology for Evaluating Transit Routes for Terrorist Groups and Criminal Transnational Organizations" at https://www.intelink.gov/wiki/Transit_Country. The IFA has authorized its distribution on the public Intellipedia.

The methodology was sensitive to potential changes in a group's condition, goals, membership, or planned operations.

qualitative proxy is one that is highly correlated to bad or suspect behavior.) We also provided a methodology, or template, by which analysts can assess the relative importance of certain countries to various groups, depending upon a number of conditions discovered by first working through the STORM process.

The methodology was sensitive to potential changes in a group's condition, goals, membership, or planned operation. As each component of the process changed, the potential nodes of operation for that group could change as well. In addition, the methodology could be used to plot potential nodes of operation for all terrorist and criminal groups: past, present, or future under varying conditions. Furthermore, the STORM methodology is scalable, so that future iterations could involve not only national units of analysis but regional and local ones as well.

Our one major disappointment was our inability to use our GIS Team. We simply ran out of time. We were unable to complete the project early enough to give our geographers time to work with the results. Part of this was due to the unfamiliarity that most of our researchers have with the capabilities of GIS. Another element was our selection of the country as the unit of analysis. During our VTCs, our geographers told us that if the country is the unit of analysis, then a spreadsheet approach would be sufficient; that GIS can help when the analysis focuses on sub- or transnational activities. Our selection of the country as the unit of analysis from the beginning, however, was in part a direct response to the assumptions behind the challenge question itself: that there is a distinct subset of all states in the international system that can be classified as transit countries. The question itself biased our approach in answering the challenge.

The three reports became one. We sent the IFA our final product on time and briefed it to them by VTC in January 2009. Involved were representatives from the IFA, several senior intelligence professionals from the ODNI, coparticipants at the various campuses, and a group of students and faculty at the CSU San Bernardino campus, where the VTC was broadcast. While the researchers answered pointed questions from the IFA, it became clear to the participants that the project was well-received and had been a success. The students in attendance, many of whom had been intimidated at the first briefing in September, were excited to witness the project's successful completion, but beyond that, they were elated that intelligence professionals evaluated the results as highly as they did.

In April 2009, the project coordinator and principal analyst delivered a briefing on STORM at NSA headquarters in Fort Meade to a packed room of analysts. The briefing was also recorded for future training. The methodology received high praise from that group as well. The following was all we needed to hear about the mood of the analysts as they left the briefing: we were told that the analysts came in skeptics but went out believers. (See IFA director's letter on facing page.)

Lessons Learned

The lessons we learned in this collaborative effort could be helpful to those working on similar projects. *For the project itself—and we imagine for intelligence analysts in general—the question drives the research.* How a question is posed can lead to biases in how to answer it. As mentioned above, the research strategies in all three classes were designed specifically around countries as the units of analysis and the assumption that there were likely to be clear indicators of what makes a country a "transit country." Realizing that the concept of a transit country was too limited, we followed our instincts and recast our approach to better capture the phenomenon under question. This reassessment of a key term in the question itself was, in and

Letter from the Director of the Institute for Analysis at NSA, Donn L. Treese.

To the faculty and students of the California State University Intelligence Community Center of Academic Excellence:

Very well done. What I see in this project is a very good microcosm of what we actually do and, even better, an insight into the way it should be done.

For the former, like us, your students and faculty were somewhat daunted by the task and the lack of specificity right up front. They were asking themselves exactly what was expected and where do they get started. What kind of data is available? Where might it lead me? Sounds familiar to an analyst. Does the question make sense? Also familiar to an analyst. What happens if I get this wrong? Not enough analysts ask themselves this question.

For the latter, what you described is a near perfect union of disciplines and collaboration. It was very smart, in my opinion, to involve others (even though time ran out, you had them on the hook) and not present any predisposed ideas or biases. Even more so, instilling this behavior as the best way to achieve a task such as this, to me, is the best outcome of this whole project.

I must add that your presentation at NSA was very well received. I heard comments to the effect that this tradecraft would indeed be incorporated into the daily analysis activities of a number of attending analysts. One discussion even focused on automation of this methodology. In short, this work was very well received.

What I hope your students bring to my agency when they get here is simple enough, I think: I need them to understand that egos are not helpful; that even though we typically are tasked individually, we must find and work with others to get the best intel product on the street; we often have incomplete data sets and no time to complete them; open and creative thinking is a staple of the job; and to ask for a better question if the one received lacks sensibility. One more thing: The job is to understand the past, work the present, and suggest the future. Some analysts get 24 hours to do that. Some get 24 months. What you all accomplished during a semester is indeed pretty remarkable. Thanks for your role in ushering this along to its great outcome.

of itself, a contribution to the dialogue. By encouraging our teams to be creative, we were able to come to this important result. Since we were asked to provide a perspective outside of the IC, we were not afraid to seek an unconventional approach. This is a key lesson. *Follow the data where they lead, even if they compel one to alter a key premise of the question itself.*

Building in redundancy in a research design can be useful for a variety of reasons. Doing so helped us avoid reliance on only one person or class, with its higher potential for failure. But redundancy also gave us multiple angles on our subject. Having different faculty members apply different ways to get at our challenge revealed the depth of the problem associated with relying on the open-source data. Across all classes, students found problems with the data that faculty members had believed would be necessary for solving the challenge. Having multiple approaches also helped us avoid problems associated with the potential bias of a single approach. We also had an added feature to ensure the integrity of the process. By permission of the two CSUSB instructors, the project coordinator solicited weekly reports on the research progress from two students who were not aware of each other's efforts, keeping the process honest.

An overall coordinator, a shepherd for the whole project, was useful as well. In fact, it is hard to see how the project could have come together without the unobtrusive, guiding hand of one person with a vested interest in completing it. The coordinator organized the VTCs, checked up on the process through his two classroom contacts, offered help and encouragement to the professors, and maintained communication with IFA representatives. Furthermore, he was able to bring in a principal analyst, who stood outside the three in-class projects. When the principal analyst was brought in to evaluate the research and integrate it into a coherent whole, the coordinator worked with

It was important for the students to realize that, despite [the uncertainties], the faculty and students would be expected to produce a result—just as any working analyst must.

the analyst to discuss the ideas and strategies the analyst would bring to the product. In addition, the coordinator advised the principal analyst on how best to present this information to the eventual consumers of the product.

In retrospect, after the challenge was completed and briefed to the IFA, *the faculty agreed that it was good for students to see the research process in its entirety because the process resembles the way in which faculty members conduct their research and, we imagine, how intelligence analysts conduct theirs as well.* It was important, pedagogically, for the students to grasp fully the uncertainties, and anxieties, of a research process in which there is no predetermined outcome and there is a high level of uncertainty about whether the research will be academically useful or accepted by their peers. Yet it was also important for the students to realize that, despite this, the faculty and students would be expected to produce a result—just as any working analyst must.

Finally, it helps to have people who bring their "A-game" to the project. No one person's ego stood in the way of the project as a whole. Everyone—from the faculty and student researchers, to the coordinator, to the geographers who waited for an opportunity to help, to the principal analyst—wanted the project to succeed. All were willing to admit where they believed their efforts or their research or research design was weak in the supporting reports. In an environment where egos sometimes get in the way of success, this was a huge factor.

Conclusion

Where will we go from here? Our efforts to collaborate are only beginning. We envision more opportunities to bring more faculty and students into future challenge projects. We are also testing how to make Wikis—with their capacity to accommodate multiple authors and ability to show changes over time—available for collaborative efforts. At the CSUSB campus, we annually produce a mock, competitive National Intelligence Estimate in our graduate program. We use a two-team format—Teams A and B—in which students represent different IC agencies on their team. We have been doing these NIE exercises for more than a dozen years.[a] In the past, the students have worked on the NIE in the traditional fashion, each individual writing his or her own paper, with the final team product being a compilation of the papers. This year, we intend to collaborate through the use of a Wiki, to simulate the type of collaboration that Intellipedia offers to analysts in the IC.

As a test, the coauthors of this article worked on this manuscript using Wiki technology. Each entry by a coauthor was tracked and was immediately available to all who had access to the site. Through this we hoped to find out what works and what does not and why. Our ultimate goal is to have more students who can bring the new tools of Web 2.0 to potential careers in the IC. In the process, we are also learning new and better ways to collaborate.

❖ ❖ ❖

[a] Our PSCI 621: Strategic Intelligence course requires students to learn photographic interpretation, the writing of the *President's Daily Brief*, and the team research approach in a competitive NIE. Each year, the instructor selects a new topic based on reasonable approximations of real-world problems. For example, over the past several years, our NIEs have included *The Prospects for China's Domestic Stability over the Next Five, Ten and Fifteen Years*, *Russia After the Election*, and this year, *North Korea After Kim Jong-Il*.