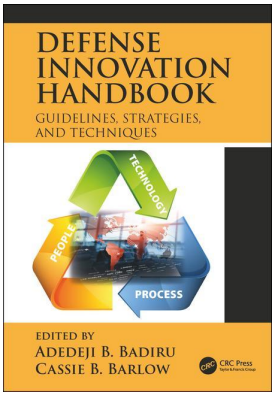

Defense Innovation Handbook
Guidelines, Strategies, and Techniques

Adedeji B. Badiru, Cassie B. Barlow

Innovation in systems framework for intelligence operations

Publication details
https://test.routledgehandbooks.com/doi/10.1201/b22181-23
Adedeji B. Badiru, Anna E. Maloney
Published online on: 04 Sep 2018

chapter twenty three

Innovation in systems framework for intelligence operations

Adedeji B. Badiru and Anna E. Maloney

Contents

Introduction

Since September 11, 2001 (9/11) homeland security concerns have dominated the national agenda. Amidst unprecedented tragedy, many government agencies rapidly initiated a vast array of security improvements as stop-gap measures to protect critical facilities, transportation systems, and other infrastructure. As the country and the Intelligence Community (IC) adjust to the "new normalcy," it is logical to question whether

- The right things are being done to deter, detect, prevent, or mitigate future terrorist attacks.
- Too much or too little effort, and too many or too few resources, are being applied.
- New technologies will help deter attacks or simply cause the attacker to use a different, but equally effective, means to achieve the same result.
- All the factors that impinge on national security are being factored into intelligence decisions.

These are logical questions. No one can state definitively what should or should not be done to detect and prevent terrorist attacks, but some level of consensus decision-making will have to occur. It has been shown that effective homeland security is not just a matter

of technological gadgetry; but also of an effective high-fidelity decision process. It is the position of this paper that a systems-based adaptive risk-based approach can help improve decisions, particularly decisions that must be based on uncertain information. Systems Risk-based Decision-Making (SRBDM) can help decision makers (users) address these questions and a wide range of other related questions.

For example, the US Navy (Navy) is using a risk-based approach to evaluate and implement an interdependent suite of antiterrorism (AT) capabilities aimed at increasing the Navy's ability to deter, detect, and respond to terrorist threats. While many capabilities already exist and others are being developed, the Navy must make decisions on how to allocate resources in a resource-constrained environment to best manage the risks associated with security threats. The Commander, Navy Installations (CNI) has sponsored efforts to link the results of a risk-based model with classic operations research modeling to help optimize the allocation of limited resources among many Anti-Terrorist (AT) capabilities. The prototype Navy model (at that time) was not comprehensive and did not adequately cover all decision factors; but it did demonstrate the feasibility of developing an adaptive risk-based resource-allocation decision tool for homeland security application. Although the AT capabilities were considered individually, significant dependencies exist between some capabilities due to the integrated performance expected from the systems that will be implemented to reduce the overall threat of a terrorist attack. For example, certain robust command and control actions rely heavily on information management and display infrastructure, and on communication capabilities between various Naval and civilian agencies. Therefore, the benefits associated with improved command and control systems cannot be fully realized without also addressing infrastructure needs related to information management and communication. This presents the following challenges:

1. How to directly incorporate interdependencies into a risk model?
2. How to determine the benefit (reduction in risk) that might be derived if a particular capability is only partially implemented?
3. How to change the assessment of overall risks and adjust strategies given the two-player nature of intentional attacks?
4. How to incorporate intelligence (both HUMINT and SIGINT) into AT decision-making?
5. How to ensure an integrative continuity of the AT strategy?

Background

Researchers all over the nation are developing, testing, and integrating advanced signal-processing, image-processing, and data-processing technologies for high-fidelity sensing systems. Improved technologies will increase reliability and accelerate the speed at which data is transmitted from sensing systems to humans, who monitor and analyze the data. Badiru and Maloney (2017) present a conceptual framework for an innovative application of a systems engineering model to intelligence operations. Intelligence on terrorist activities will always be incomplete and imperfect. Intentional planned attacks involve two opponents with competing objectives. Each opponent will consider the options and objectives of his adversary in formulating a strategy, and will change his strategy based on what his opponent does or what he expects him to do. Although it is clear that some terrorists are willing to die while attacking a target, there is no evidence to suggest that a terrorist will deliberately attack a target if he perceives that he will fail in the attempt. Therefore, making a target invulnerable to a particular mode of attack

will not necessarily put the terrorist out of business; rather, it may cause him to consider other targets or modes of attack. Therefore, taking action to reduce a specific threat may increase the likelihood that an alternative target will be attacked. These are all issues that must be addressed from a systems perspective within the realm of effective human decision-making; not just from a technical assets point of view, as embodied in the DEJI model (Badiru 2012, 2014).

Decision-makers must be aware that terrorists will adjust attack modes and adopt strategies that will exploit vulnerabilities in a dynamic manner. Actions designed to reduce vulnerability to a specific attack mode must not only be considered to ensure that they are effective; their impact on other scenarios must also be considered. Myopic focus on safeguards for a specific target or attack mode could simply shift the risk to other targets or attack modes, and could actually increase overall risk. The research question is posed as follows:

> Can an effective systems-based methodology be devised that will effectively **Design**, **Evaluate**, **Justify**, and **Integrate** the trade-offs between risk and costs, acknowledge the interdependencies in resource-allocation decisions and the integrated nature of systems execution, respond in a timely manner to counter strategies perceived to have been made by the terrorist adversaries, take into account the imperfect and incomplete nature of intelligence on terrorist activities, and effectively guide resource allocation decisions so as to minimize the overall threat of an intentional attack?

In the approach of this paper, we recommend using the systems-based DEJI model, which has been applied to a variety of practical problems (Badiru 2012, 2014) dealing with designing, evaluating, justifying, and integrating problem parameters and factors. Figure 23.1 illustrates the basic structure of the DEJI model.

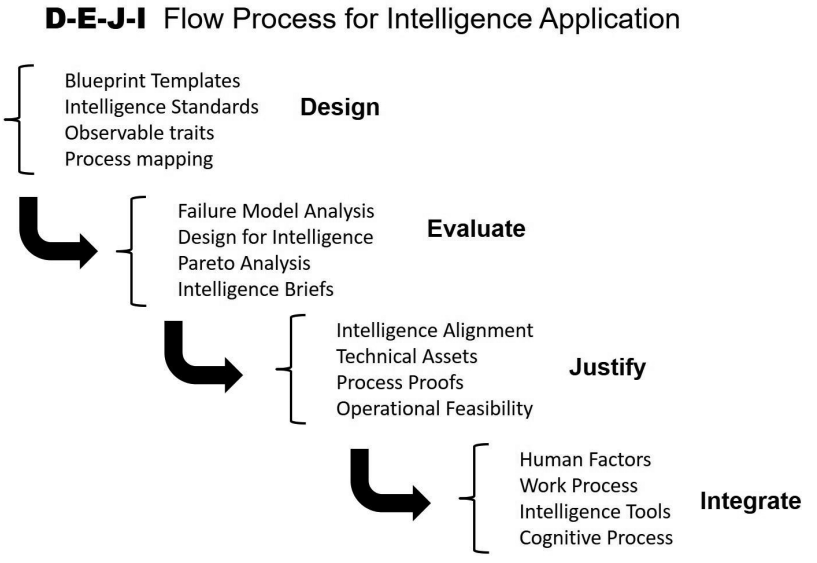

Figure 23.1 DEJI model for intelligence analysis.

The research problem has two components:

- The *risk assessment* part in which benefits (defined as reduction in the risk of attack) are moving targets that must be continuously re-evaluated based on current intelligence and dynamically fed into a capital budgeting model for strategy development and adjustment.
- The *resource allocation* part in which decisions are generated as to which capabilities should be implemented, and at what level, in order to minimize the overall threat based on the most recent systems risk assessment.

Proposed methodology

Given the wide range of attack scenarios (i.e., possible terrorist targets and attack modes), and the uncertainty associated with each scenario, the benefit provided by a particular resource allocation can be difficult to predict. However, we can establish a structured methodology to evaluate the risk benefit for each capability based on how each capability might change the threat, target vulnerability, or consequences (TVC) for each scenario.

Design section

Under the DEJI model approach, the Design aspect relates to the resource allocation model as formulated in the following large-scale nonlinear mixed binary integer programming problem:

I = set of counterterrorism capabilities

T = set of funding cycles (e.g., fiscal years)

J = set of funding sources = $\{1,2,3,4\}$

e.g., funding source 1 = capital works; 2 = research/development;

3 = procurements; 4 = operations/maintenance

x_{ijt} = proportion of full funding allocated to capability i from

funding source j in time period t

$\phi(x_{i4t})$ = utility function; expressed as the % benefit derived as a function of

funding level (% of total funding) in time t – applied only to

operations/maintenance funding source

$$y_{it} = \begin{cases} 1, \text{ if capability } i \text{ is deployed at time } t \\ 0, \text{ otherwise} \end{cases}$$

$i \in I \quad j \in J \quad t \in T$

c_{it} = reduction in risk (threat) achieved by fully implementing capability i in time t.

Objective: Maximize the reduction in the risk of a terrorist attack.

$$Max \quad \xi = \sum_i \sum_t c_{it} y_{it} \phi(x_{i4t})$$

1. Appropriation Limits (Budgets from each funding source cannot be exceeded).
2. Dependencies Across Funding Sources (e.g., sequencing of spending).
3. Dependencies Across Time Periods (e.g., sustaining funding commitments).
4. Dependencies Across Capabilities (e.g., funding prevention before detection).
5. Contingencies (either/or, if a then b).
6. Deployment (only allocate funds to deployed capabilities).
7. Bounding (force minimum funding levels if appropriate).
8. Structural (e.g., linearization, binary).

The proposed model consists of the modules shown in Figure 23.2.

Evaluation section

The capital budgeting class of problems, including uncertainty and risk, has been investigated from numerous perspectives. Recent work includes the use of fuzzy numbers to estimate uncertain returns, a modified weighted average cost of capital methodology to project returns, pooling of risks across multiple projects, analytic hierarch process (AHP) as a decision framework, zero-one integer programming to accommodate sequencing decisions in a dynamic environment, an integrated approach that combines risk management with capital budgeting, a methodology for selecting projects in high risk R&D environments, goal programming for decision making in an uncertain environment, a generalized dynamic capital allocation methodology using distortion risk measures, sensitivity analysis as a tool applied to capital budgeting under uncertainty and risk, and game theory combined with Monte Carlo simulation for timing resource allocations in a homogeneous commodity market.

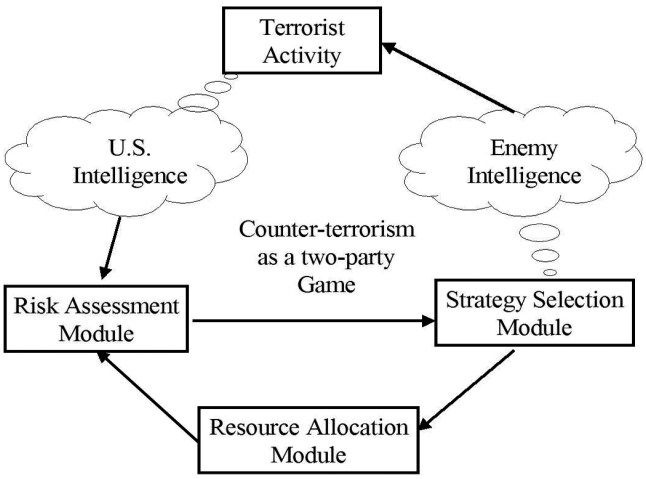

Figure 23.2 DEJI systems modeling for intelligence problem abstraction.

The desired methodology will allocate resources sequentially across competing highly interdependent projects, where each project may be partially funded, with non-linear utility functions that are dependent on the counter-moves of an intelligent adversary. A model to allocate resources to combat terrorism must address all these issues from an overall systems perspective. Developing such a model requires the integration of mathematical programming, stochastic processes, risk assessment, and classical game theory.

1. There is an urgent need for decision tools that will reduce the threat, help decision makers to spend public money more wisely, and rapidly respond to changes in the threat due to actions by the terrorists.
2. The integrative nature of the proposed model represents an application of established research to new areas of expertise.
3. The use of a decision model that directly links resource allocation strategy dynamically with counter-moves by a terrorist adversary, factoring in the imperfect nature of intelligence information and the political process, has largely been untested.

Because acts of terrorism can be vastly different, widespread, and involve ever-changing methods, analysis of information needs to be performed every step of the way. Those who gather intelligence need to realize that some information is more vital to national security and the analysts themselves need to take into account the very human aspect of terrorism. Humans are irrational at best, especially when angry and trying to get a point across. Analysts in today's world need to be trained in the art of analysis, not just specific topics or regions. Analysts nowadays must have a global perspective that was not needed during the predictable days of the Cold War. Additional funding to analysis is vital. This funding would allow additional analysts to keep an eye on small threads linking bits of information to potential terrorist attacks. While the large amount of information possessed by the IC is impressive, national security interests are only protected if that information is transformed into intelligence.

We are no longer in a Cold War world. In our world, terrorist organizations are proud of their blatant disregard of humanity. The IC can no longer fund specialists like they could in the mid to late twentieth century. When the United States had one large, known enemy, it was possible for analysts to pick a specialty and stick with it their entire career. Now it is nearly impossible to have specialists on every threat to the US. From Russia, China, and North Korea, we face states that would like to see the United States taken down a peg; from the Islamic State of Iraq and the Levant, Hezbollah, and Boko Haram we face non-state actors with no limitations on their cruelty and barbarism.

Justification section

Assuming a set of predetermined strategic scenarios, risk-based payoff values will be developed and evaluated using a modified risk-assessment procedure and appropriate statistical procedures. The best strategy can be found by solving a mixed (randomized) strategy game problem based on the payoff matrix obtained from the Risk-assessment Module. The optimal solution of a Linear Programming (LP) formulation will represent the probabilities for each strategy to return the best expected payoff value. Based on the optimal solution from the Strategy Selection Module, the predetermined strategies can be prioritized. The objective of the proposed resource allocation model is to maximize the reduction in the risk of a terrorist attack, and can be formulated as the large-scale nonlinear mixed binary integer programming problem.

The money it takes to build a new satellite is astronomical compared to the money it takes to hire on additional analysts to different intelligence agencies. As stated by Best (2015), "Unfortunately, sophisticated political and social analysis is often not emphasized in intelligence agencies, especially within the Defense Department, that are focused on technical collection and direct support to operational commanders." The US government is setting the IC up to fail should policy-makers not fund what the IC deems necessary. The cost is very low when it comes to linking intelligence agencies and allowing them to share their information and analysis. The way the IC had grown to be so bureaucratic and have immense tangles of red tape can be reversed only if policy makers decide that information sharing between agencies is as vital as many IC members claim.

Integration section

This section is presented as a hypothetical case example of the importance of integration in intelligence analyses.

Hypothetical case example 1: More attention to human intelligence in order to augment signals intelligence

The intelligence community, including the armed forces, has focused the majority of their research, time, and money on Signals Intelligence (SIGINT) while leaving Human Intelligence (HUMINT) without sufficient attention and funding. Though SIGINT worked wonderfully during the Cold War to decode and decrypt Soviet messages, the developing world has seen a rise in non-state actors threatening the United States. These non-state actors utilize the exponential growth of social media and the internet. Because there are entirely too many pieces of information circulating every day, vital information can fall through the cracks. SIGINT cannot, and should not, be responsible for keeping track of all signals. Therefore, HUMINT should come back into the spotlight. The intelligence community should put a renewed focus on quality over quantity.

Many countries around the world have developed high-performing and gainful human intelligence agencies. Though these nations tend to use tactics considered inhumane or illegal, places like Russia and Israel have found a way to gather relatively secure sources in places where SIGINT is no longer the best option. The United States needs human intelligence in order to be better prepared to deal with small terrorist cells and lone-wolf attacks. While the United States values human rights and should not go to cruel measures to secure information, the US needs to understand the importance of intelligence "boots on the ground."

In many ways, Signals Intelligence intrigues people. Congress is fascinated by new technology and likes to physically see what they are funding. This emphasis on SIGINT, however, is not always the most cost effective. Human intelligence, though occasionally subject to manipulation and deception, can provide data and information that signals intelligence cannot. A human being can see if a person looks worried while talking to different individuals or takes extra caution crossing a certain stretch of the road. A human being can detect when a voice seems weary or cautious. A human being can begin to bond and build relationships with people who hold vital information. While reading communications and listening to recordings is wonderful for quantitative information, the United States is in dire need of qualitative information if there is any hope in staying two steps ahead of her adversaries. As the Head of Intelligence Collation Management at the North Atlantic Treaty Organization's mission in Sarajevo,

Palfy (2015) said it best when he stated, "… increased collection does not necessarily or automatically lead to better intelligence outcomes."

We can look to history to compare and contrast SIGINT and HUMINT. During the Cold War, missions like the Bay of Pigs had many pictures and technical information about Soviet intervention in Cuba, but there was very little focus on HUMINT. Had the United States noticed that the Cuban people did not want to overthrow Castro, they may have been spared the embarrassing blemish on the Kennedy administration.

The implementation of this shift in concentration would not likely be difficult. The most time consuming and difficult step in the process would likely be funding approval from Congress. The Congress people would likely be unhappy to cut funding to Signals Intelligence because, in many cases, creating technology used for SIGINT brings in money and jobs to their constituents back home. As long as Congress approves the reassignment of funds, integrating this new policy should be smooth. SIGINT should continue to be funded, of course, because of its vital role in the information age.

Conclusion

This paper has presented a conceptual framework for the application of a systems approach to addressing systems challenges. Although no specific problem is tackled in the paper, the framework can give readers in the intelligence community an expanded idea of how to design, evaluate, justify, and integrate intelligence strategies. In recent years, sensor-based systems have increased in development and applications. The variety and diversity of HUMINT and SIGINT systems necessitate the application of a systems approach. This paper has introduced the application of the DEJI model by proposing the use of HUMINT as an integrated augmentation of SIGINT.

References

Badiru, A. B. (2012), Application of the DEJI model for aerospace product integration, *Journal of Aviation and Aerospace Perspectives (JAAP)*, 2(2), 20–34, 2012.

Badiru, A. B. (2014), Quality insights: The DEJI model for quality design, evaluation, justification, and integration, *International Journal of Quality Engineering and Technology*, 4(4), 369–378.

Badiru, A. B. and A. E. Maloney (2016), A conceptual framework for the application of systems approach to intelligence operations: Using HUMINT to augment SIGINT, *American Intelligence Journal*, 33(2), 41–46, 2016.

Best, R. A. (2015), Intelligence and US national security policy, *International Journal of Intelligence and CounterIntelligence*, 28(3), 449–467. doi:10.1080/08850607.2015.1022460.

Palfy, A. (2015), Bridging the gap between collection and analysis: Intelligence information processing and data governance, *International Journal of Intelligence and CounterIntelligence*, 28(2), 365–376. doi:10.1080/08850607.2015.992761.