Journal of Strategic Security

Volume 5
Number 1 *Spring 2012*

Article 9

A Systems-Based Approach to Intelligence Reform

Austen Givens
Utica College, adgivens@utica.edu

pp. 63-84

Recommended Citation

Givens, Austen. 2012. A Systems-Based Approach to Intelligence Reform. *Journal of Strategic Security*, 5 (1): 63-84.
Available at: http://scholarcommons.usf.edu/jss/vol5/iss1/9

A Systems-Based Approach to Intelligence Reform

Abstract
The terrorist attacks of September 11, 2001 prompted the most comprehensive changes to the U.S. Intelligence Community (IC) since its creation via the National Security Act of 1947. Recent structural and organizational reforms, such as efforts to enhance information sharing and recruit speakers of hard-target languages, have also triggered new challenges to successful transformation. In light of the systemic problems facing the IC, this paper argues that systems engineering, a discipline increasingly useful in organizational change, offers a more efficient, holistic approach to the intelligence reform process than the status quo. Systems engineering views the IC as an integrated and interdependent system, whose value is primarily realized through the relationship among its components. The author makes the case that a systems-based approach to intelligence reform can enhance effectiveness while reducing the risk of unintended consequences.

Journal of Strategic Security
Volume 5 Issue 1 2012, pp. 63-84
DOI: 10.5038/1944-0472.5.1.5

Published Quarterly by Henley-Putnam University Press
with support from the University of South Florida Libraries

A Systems-Based Approach to Intelligence Reform

Austen Givens
Utica College, New York

Abstract

The terrorist attacks of September 11, 2001 prompted the most comprehensive changes to the U.S. Intelligence Community (IC) since its creation via the National Security Act of 1947. Recent structural and organizational reforms, such as efforts to enhance information sharing and recruit speakers of hard-target languages, have also triggered new challenges to successful transformation. In light of the systemic problems facing the IC, this paper argues that systems engineering, a discipline increasingly useful in organizational change, offers a more efficient, holistic approach to the intelligence reform process than the status quo. Systems engineering views the IC as an integrated and interdependent system, whose value is primarily realized through the relationship among its components. The author makes the case that a systems-based approach to intelligence reform can enhance effectiveness while reducing the risk of unintended consequences.

Introduction

The United States' post-September 11 approach to intelligence reform is not working out as expected. The National Commission on Terrorist Attacks Upon the United States, widely known as the 9/11 Commission, published a series of recommendations for intelligence reform in 2004. The Commission called for creation of the Director of National Intelligence (DNI) position, which four individuals have occupied in six years' time.[1] It also suggested establishing the National Counterterrorism Center (NCTC) as an interagency coordination hub for all terrorism-related information, yet a recent report describes the NCTC as organizationally parochial and lacking operational strength.[2]

The Commission's emphasis on information sharing led to a proliferation of electronic databases and networks across multiple agencies and departments, including the Homeland Security Information Network (HSIN), the Homeland Secure Data Network (HSDN), and Intellipedia, and extension of the Department of Defense's SIPRNet to state-level fusion centers.[3] Incredibly, these databases and networks were not created to interact with one another. Seven years after its inception, the Information Sharing Environment (ISE), an interagency office set up to facilitate critical data exchange within government, has not addressed information sharing in the IC in a focused manner, and lacks a clear plan for future organizational development.[4] Despite new financial hiring incentives for qualified candidates, efforts to recruit intelligence officers with proficiency in hard-target languages have proceeded at a glacial pace; as recently as 2009, a U.S. Senate committee noted that the cadre of IC personnel capable of understanding Pashto, Dari, or Urdu is "essentially nonexistent."[5]

The current piecemeal approach to intelligence reform, which addresses problems in relative isolation from one another, is clearly not producing the results we anticipated. It appears that changes in a given area of intelligence reform cause unanticipated issues in other respects. How can we better understand and address what is happening here?

It is helpful to think about the IC as a collection of interconnected, interdependent components whose collective output—intelligence products—is more valuable than the sum of its parts. This arrangement is known as a system. An example from everyday life might help illustrate its fundamental principles. A working car engine consists of pistons, metal, wires, fuel, spark plugs, oxygen, hoses, and pumps. Removing or changing any of these components will impact the engine's ability to function properly. What happens, for example, if we cut two wires at random and stuff wet sponges into an engine hose? Naturally, the engine ceases to function as it should. The engine itself is a system whose components work together, harmoniously and interdependently, producing horsepower to propel a vehicle. By snipping wires and clogging hoses, we affect not just the engine components we touch, but the entire engine. Understanding the IC as a system, rather than as a collection of loosely connected personnel, agencies, departments, and technologies, demands the consideration and resolution of challenges in a systemic fashion. A systems-based approach considers intelligence reform through the lens of systems engineering, a

DOI: <p>http://dx.doi.org/10.5038/1944-0472.5.1.5</p>

discipline that holistically addresses the complex interplay of system-wide variables to produce effective outcomes. This method, for example, recognizes that hiring practices in one agency can affect information classification in another. Similarly, a systems-based approach weighs the need for additional hard-target linguists in light of the current processing time for security clearances. This strategy is more consistent with the actual organizational dynamics of the IC, in which reform-related decisions have far-reaching impacts beyond a given office or department, and therefore offers a more effective means of strengthening the IC.

This article, then, will argue that a new, systems-based approach to intelligence reform can bolster the efficiency and effectiveness of the intelligence reform process. First, it provides a brief overview of the IC's history, including key reform initiatives stemming from the 9/11 terrorist attacks. Following this discussion, the article examines systems engineering, its current use, and its possible implications for intelligence reform. A hypothetical example of the ways in which systems engineering's principles can apply to intelligence reform follows, illustrating the systems architecture of the IC itself. The paper concludes with a summary of the potential policy implications for systems engineering in intelligence reform, and a brief discussion of the need for future research in this area. The implications of this new understanding and approach to intelligence reform may be useful to scholars of intelligence studies, government policymakers, and IC practitioners.

The Intelligence Community before and after 9/11

Forged by the National Security Act of 1947, the IC emerged from the post-World War II need for government-wide coordination of intelligence activities.[6] The Act's passage led to establishment of the CIA, which centralized and aligned previously disparate responsibilities for the collection, analysis, and dissemination of critical national security information within government.[7] Through the information demands of subsequent conflicts and incidents—Korea, Vietnam, the Cold War, Gulf War I, the first World Trade Center bombing, and others—the IC increased in size and scope.

The terrorist attacks of September 11, 2001 changed the nature of intelligence in the United States. Cultural and legal barriers between traditionally foreign intelligence-oriented agencies and law enforcement organizations began eroding, spurred on by passage of the Patriot Act in 2001, as well as the Intelligence Reform and Terrorism Prevention Act of 2004. The 9/11 Commission offered additional recommendations for reform, including calls for creation of the Director of National Intelligence (DNI)—a central figure overseeing the administration of the entire IC.[8] Other suggested reforms were creation of a National Counterterrorism Center (NCTC), more robust information sharing across government, and stronger incentives for recruiting foreign language speakers in the intelligence profession.[9] All of these suggestions have, to varying extents, been implemented. Other new developments, including the formation of over seventy intelligence fusion centers nationwide, and initiatives to improve processing of applications for security clearances, complement these efforts.[10]

Yet execution of the reforms is encountering complications. Turnover plagues the DNI position.[11] A recent report describes the NCTC as risk-averse.[12] There are few IC hard-target language experts.[13] Agencies across the IC adjudicate security clearances—which permit employees to handle classified information—in different ways, depending on the organization issuing the clearance.[14] Fusion centers, which function as critical information hubs bridging the federal and local levels of government, continue to draw criticism for ineffective governance and personal privacy concerns.[15] Using the current approach, well-intentioned changes to the intelligence apparatus seem to have had unforeseen consequences.

An opportunity exists for the IC to implement critical reforms using a more comprehensive method of problem solving. Rather than addressing issues independently, a systems-based approach views intelligence reform as a rich mosaic of interconnected components. Employing such a strategy, decision makers model choices and their potential ramifications in a holistic manner. This reduces the risk of unintended negative consequences and helps achieve previously unrealized organizational synergies across government.

Why Systems Engineering?

The intelligence reform process is better understood by viewing the IC as a system, rather than as a series of related components. The widely respected International Council on Systems Engineering (INCOSE) defines a system as:

> "...(a) construct or collection of different elements that together produce results not obtainable by the elements alone. The elements, or parts, can include people, hardware, software, facilities, policies, and documents; that is, all things required to produce systems-level results. The results include system-level qualities,

DOI: <p>http://dx.doi.org/10.5038/1944-0472.5.1.5</p>

> properties, characteristics, functions, behavior, and performance. The value added by the system as a whole, beyond that contributed independently by the parts, is primarily created by the relationship among the parts; that is, how they are interconnected."[16]

Under this definition, the IC's true value to intelligence customers is in the relationships among its components. People, processes, technologies, and organizations work together in a dynamic fashion to produce intelligence products that permit leaders to make better-informed decisions. Understanding the IC as a dynamic, interconnected system—rather than a loose-knit collection of agencies, people, technology, and knowledge—can lead to more robust insights into intelligence reform.

Indeed, resolving systemic challenges in the IC demands a correspondingly holistic approach to problem solving, rather than reform efforts executed in relative isolation from one another. Systems engineering offers a potential means to effect organizational change that takes into account the totality of variables influencing the IC reform process.

Systems engineering can be defined as:

> "...(a)n engineering discipline whose responsibility is creating and executing an interdisciplinary process to ensure that the customer and stakeholder's needs are satisfied in a high quality, trustworthy, cost efficient and schedule compliant manner throughout a system's entire life cycle."[17]

Scholars and practitioners in systems engineering generally utilize a seven-stage process, regardless of industry, in approaching problem solving. In this systems engineering model, however, variation appears to be the essence of the requisite steps and their principles tend to be mimicked across the discipline.[18] While experts depict each step as discrete and linear in orientation, overlap and nonsequential progress exist in each phase of the process. Systems engineering's functions in this seven-stage process are: State, Investigate, Model, Integrate, Launch, Assess, and Reevaluate, often summarized using the acronym SIMILAR.[19] Preparing a child's school lunch offers a simple illustration of this process at work.

Bobby, aged seven, needs a midday meal at school (Problem). Rummaging in the refrigerator, Bobby's father, John, identifies three possible options for his son's lunchbox—a peanut butter and jelly sandwich, a caesar salad, and leftover lasagna. John pauses, recalling that two nights ago Bobby barely feigned interest in a caesar salad at dinner. He is unsure of his son's interest in lasagna, but knows from past experience that peanut butter and jelly sandwiches tend to meet with Bobby's approval (Investigate Alternatives). John then prepares the sandwich, employing a small system of whole wheat bread, peanut butter, strawberry jelly, a table knife, and a bag (Model the System). He also assembles a small container of carrot sticks, a blueberry yogurt cup, and an apple. He places all of these items in the lunch box (Integrate), closes it, hands it to Bobby, and sends him on his way to school (Launch the System). Later that evening at the dinner table, Bobby tells his father that he enjoyed the lunch, but would prefer potato chips instead of carrot sticks next time. He rates the lunch an eight out of a possible ten points (Assess Performance). John briefly considers including potato chips in Bobby's next lunch, but dismisses the idea under the disapproving gaze of Bobby's mother (Reevaluate). Table 1.0 provides a brief summary of the core concepts associated with each of these steps.

Table 1: The Systems Engineering Process

Systems Engineering Process Phase	**Core Concepts Associated with Phase**
State the Problem	A top-level description of the functions a system must perform is provided, addressing questions of "what," not "how." Problems are clearly defined.
Investigate Alternatives	Alternative designs are created and evaluated based on multiple criteria, including performance, schedule, cost, and risk. Preferred options are modeled and evaluated, creating simulation data for analysis. Trials are ultimately run on the model system of choice.
Model the System	The preferred alternative is expanded and used to manage the entire system life cycle.

DOI: <p>http://dx.doi.org/10.5038/1944-0472.5.1.5</p>

Systems Engineering Process Phase	**Core Concepts Associated with Phase**
Integrate	The system is integrated into other systems with which it must interact. The outcome of effective integration is improved efficiency.
Launch the System	The system is "run" and begins to produce products. In industrial processes, parts are purchased at this stage. Care is taken to ensure that those operating the systems are familiar and comfortable with their functions. Interface with other systems may trigger "co-evolution" of multiple systems over time.
Assess Performance	The system is evaluated using performance metrics, ideally quantitative in nature. Measurement enhances control, and control leads to improvements.
Reevaluate	The system's outputs are observed, and this information is used to modify the system, its inputs and outputs, or the process itself.[20]

Leveraging the above process, systems engineering works to increase the efficiency and effectiveness of processes as diverse as aircraft production, the operation of elevators in high-rise buildings, and management of the global steel industry.[21] Focusing on both product and process, systems engineering can provide greater insights into the steps used to produce a finished product, as well as into the functions required to create it. Systems engineering's comprehensive approach to problem solving considers as many factors and variables as possible related to the issue under consideration. In this sense, it reduces the risk of missteps and unintended negative consequences.[22] Widely applicable in industrial design and technology-oriented professions, the tenets of systems engineering are receiving widespread recognition as potential tools for informing and improving organizations.

Currie and Willcocks provide a case study of business process reengineering (BPR) at the Royal Bank of Scotland (RBS). While loosely linked to systems engineering, BPR tends to focus on organizations per se, rather than organizations in the broader context of relationships and connections with other entities.[23] Their findings identified two challenging areas affecting institutional reform: use of "legacy" technology systems, as well as structural divisions between information technology (IT) and business units within RBS. In this regard, Currie and Willcocks' work is instructive in developing greater understanding of the engineering principles' applicability to organizational change.

Rechtin addresses the principles of systems engineering in a broader discussion of rules governing behavior in the U.S. Government. He states that the Department of Defense (DOD) is only as strong as we choose to make it. The organization balances a delicate tension among military personnel, civilians, industry, and citizens; maintaining this balance, Rechtin argues, is essential to effectiveness.[24]

Kopach-Konrad et. al describe the relevance of systems engineering principles for improving complex patient care in health-care settings.[25] This description later echoes in proceedings from the prestigious Mayo Clinic in 2009.[26] Framing the use of systems engineering in health care, particularly by such a noteworthy organization, underlines the discipline's emerging acceptance in facilitating organizational change.

Valerdi, Nightingale, and Blackburn explore systems engineering in enterprise analysis, a flexible concept referring to the evaluation of systems in a wide range of areas and disciplines, including organizational values, operations, person-to-person interactions, and information technology.[27] Their scholarship works to advance understanding of systems

DOI: <p>http://dx.doi.org/10.5038/1944-0472.5.1.5</p>

engineering beyond its traditional application in the manufacturing and industrial sectors.

In a 2006 white paper, the Armed Forces Communications and Electronics Association (AFCEA) describes the potential benefits of systems engineering in the IC, but this discussion occurs in the context of technology acquisition, rather than community-wide reform. The paper's thrust, however, speaks to the value of systems engineering in resolving issues that transcend the IC as a whole.[28]

Cooper notes that, in seeking to enhance analytical capabilities, the IC is better described as a living ecosystem than a traditional system. He states this is so because the IC consists of numerous interacting entities, nonlinear feedback loops, and specific functional niches reflecting temporary environmental adaptation.[29] While the notion of an ecosystem provides another way of examining the IC, a systems-based approach to community reform necessarily adopts a comprehensive approach to problem solving.

The literature demonstrates numerous potential organizational benefits to employing systems engineering concepts as tools for improving effectiveness. These include clarifying problems, identifying institutional objectives, modeling decision-making processes, reducing duplication of effort, eliminating low-value chokepoints, providing increases in efficiency, and potentially achieving cost savings. In meeting the complex challenges of intelligence reform, officials in government, the private sector, nonprofit organizations, and individual citizens can benefit from these and other by-products of systems engineering.

To establish a framework for analysis of the potential impact of systems engineering on intelligence reform, Figure 1 lists systemic challenges in the IC taken from recent open-source analyses. This list is not comprehensive but, rather, serves to define the scope of intelligence reform for the purposes of this paper.

Figure 1: Areas of intelligence reform under examination

1. Bridging gaps in information sharing between intelligence agencies and law enforcement organizations in the United States[30]

2. Integration of electronic information sharing networks in the classified and unclassified domains[31]

3. Increasing the operational vis-à-vis coordination-oriented activities of the National Counterterrorism Center (NCTC)[32]

4. Recruitment of hard-target language speakers as intelligence officers for the United States Government (USG)[33]

5. Streamlining the process for conducting background investigations and issuing clearances for access to classified information[34]

A Systems-Based Approach for Intelligence Reform

Utilizing the SIMILAR process outlined in the previous section, and considering the areas of intelligence reform in Figure 1, what follows is a simple depiction of systems engineering at work. This hypothetical outline is not to suggest that a single, comprehensive solution to intelligence reform exists, nor does it imply that the information below represents the definitive answer to vexing institutional challenges. Some of the hypothetical steps listed below have, in fact, been attempted or implemented. Instead, the outline's purpose is to underscore the potential benefits of employing a systems-based, comprehensive approach to intelligence reform, rather than one in which the IC resolves problems in a more piecemeal fashion. These benefits are realized primarily in reducing duplication of effort, streamlining operations, and avoiding missteps by anticipating technical and organizational complications.

State the problem: Intelligence information must be effectively collected, analyzed, and disseminated among all members of the IC and its partners, with a view toward empowering leaders to make well-informed decisions.

Investigate alternatives: A federal interagency working group (hereinafter Group A) convenes to address the problem in a collaborative, systems-based manner. After examining the problem and gathering stakeholder input, Group A's recommendations are to employ a combination of organizational and technological changes to improve information sharing.

DOI: <p>http://dx.doi.org/10.5038/1944-0472.5.1.5</p>

These include developing a network of interconnected databases across the classified and unclassified domains, as well as modifying the organizational roles played by the NCTC. Additionally, the working group recommends renewed emphasis on hiring intelligence officers with proficiency in hard-target languages to facilitate the collection of vital human intelligence (HUMINT).

Modeling these proposed solutions identifies problems of technology connectivity across the IC that are both hardware- and software-related. Group A notes access issues related to security clearance levels; for example, top-secret clearances with the Federal Bureau of Investigation (FBI) are not necessarily compatible with top-secret clearances issued by the Department of Defense (DOD).[35] Additional projections identify that the NCTC's staffing model, in which IC agencies detail representatives to the NCTC, leads to an organizationally parochial approach to intelligence fusion that ultimately perpetuates the status quo.[36]

Through collaborative discussions, Group A begins to understand that the need to recruit speakers of hard-target languages is complicated by circumstances related to language acquisition itself. Speakers of Arabic, Persian, Vietnamese, and other hard-target languages often associate with native speakers who are not necessarily U.S. citizens. This is typical, as interacting with native speakers is crucial to developing proficiency in these languages.[37] During a background investigation before the issuance of a security clearance, procedures require that candidates identify the foreign nationals with whom they regularly associate.[38] Depending on the closeness of the relationship and frequency of contact, this factor can prolong the clearance adjudication process.[39] In extreme cases, the association could prevent otherwise qualified, trustworthy candidates from being issued a security clearance.[40] Thus, highly qualified U.S. citizens, proficient in hard-target languages and seeking employment with the IC, may be screened out due to the relationships that helped them develop their linguistic proficiency.

Group A then develops alternatives. These include developing a single electronic portal for the IC, leading to multiple compartmentalized information databases. All databases are designed to be uniformly searchable by keyword, not unlike a sophisticated Internet search engine. Search results appear for all users, listing brief summary information from all databases. Access to compartmentalized information, however, must be specially requested if outside one's immediate domain of responsibility.

The role originally envisioned for the NCTC is modified, in that its scope, reach, and organizational authority are made similar to that of the ODNI itself. The NCTC would directly recruit and hire personnel to bolster organizational autonomy and impartiality. The NCTC is further empowered to share unclassified and classified information throughout the IC, and is given organizational authority to direct the exchange of terrorism-related intelligence across the federal government.

Group A finds that investigations of security clearance applicants' relationships with foreign nationals cannot be reduced or eliminated without creating significant gaps in operational security. Therefore, the need for hard-target language speakers in the IC can be met in a robust manner only by expanding foreign language education programs. Accordingly, a proposal is developed for a national initiative geared toward training future teachers of hard-target languages. If the proposal is successfully implemented, the number of hard-target language programs in elementary and secondary schools would expand substantially nationwide.

Model the system: The prospect of modifying the NCTC's organizational role and authority within the ODNI, as well as a streamlined information database system, are modeled and tested. Issues of software coding for access to the IC portal arise and are resolved before deployment. Clearance compatibility issues remain problematic, prompting an interagency study of potentially migrating to universal clearance standards that are centrally adjudicated by a new office within the ODNI. Plans for a new federal initiative for hard-target language instruction, comparable to the renewed national emphasis on mathematics and science instruction during the Cold War, are drafted for presidential review.

Integrate: In-house training programs are created throughout the IC surrounding use of the IC-wide information sharing portal, the NCTC's revised role, and the clearance office. Internal education within the IC regarding these initiatives works to help foster a "culture of sharing" among collectors and analysts. IC human resource officers are also coached on enhancing relationships and developing contacts with local school districts, in addition to college and university-level foreign language departments.

Launch the system: The IC information sharing portal, enhanced NCTC, and central clearance office within the ODNI formally open for business. With presidential encouragement and congressional approval, funds are dispersed to launch the new Nationwide Language Acquisition Initiative.

Assess performance: Thirty-, sixty- and ninety-day reviews of all initiatives quantitatively measure performance against predefined metrics. Deficiencies in implementation are identified and swiftly corrected, while

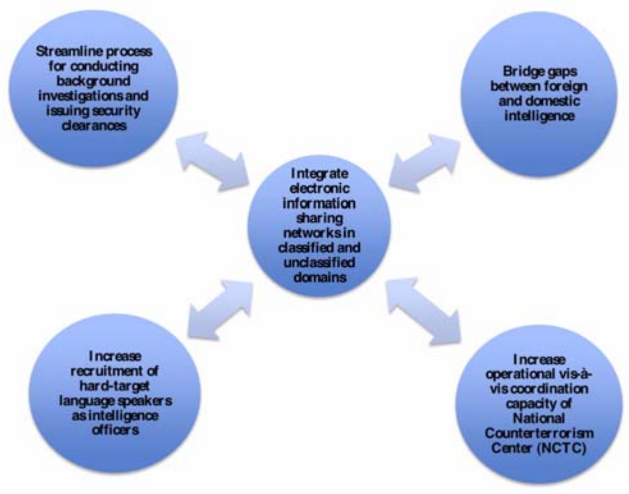
DOI: <p>http://dx.doi.org/10.5038/1944-0472.5.1.5</p>

the benefits accrued are publicized throughout the IC and to government leaders.

Reevaluate: Annual organizational performance assessments quantify the effectiveness of these initiatives, and lead to further changes and modifications where needed.

While the systems decision pathway suggested above would not necessarily be linear or continually progressive, it presents a hypothetical example of improving intelligence sharing in a holistic way. By modeling alternatives to solutions before their launch, agencies and organizations are better able to understand the potential ramifications of changes throughout the system, and to fine-tune their approaches to organizational modifications accordingly. Solution modeling also reduces duplication of effort (for example, multiple, un-integrated information sharing databases) and potential missteps (for example, the NCTC being staffed by employees on temporary detail who are not imbued with a sense of "loyalty to sharing," but rather with "loyalty to the home agency").[41] Importantly, a systems-based approach to intelligence reform is consistent with the interconnected nature of challenges within the IC. Each of the five systemic challenges listed in Figure 1 impact one another. Consequently, efforts to change one variable will have cascading effects on the remaining four. Figures 2 and 3 show this concept.

Figure 2.0
Inter-relational Dynamics Among Diverse Challenges in Intelligence Reform


Streamline process for conducting background investigations and issuing security clearances
Bridge gaps between foreign and domestic intelligence
Integrate electronic information sharing networks in classified and unclassified domains
Increase recruitment of hard-target language speakers as intelligence officers
Increase operational vis-à-vis coordination capacity of National Counterterrorism Center (NCTC)

In simplified form, Figure 2 depicts the interrelational dynamics among the five intelligence reform factors listed in Figure 1. For example, viewing intelligence as a system, we see the process for streamlining background investigations for security clearances has an effect on the integration of electronic information sharing networks. This integration impacts the process of streamlining background investigations for clearances. In the former case, universal-standard clearances, adjudicated through a single office that transcends the entire IC, should theoretically facilitate greater, faster access to information on IC computer networks. Under this new theoretical standard, questions of whether a given agency's clearance permits an IC analyst to view information classified by another agency are moot. In the latter instance, integration of networks helps drive the streamlining of the security clearance adjudication process by demanding greater uniformity in clearance standards for ease of access and use.

This two-way relationship holds among all five factors depicted in Figure 2. Any one of these intelligence reform issues, if modified, will impact the other four. A detail of this dynamic appears in Figure 3.

Figure 3.0
Detail of Inter-relational Dynamics Among Diverse Challenges in Intelligence Reform

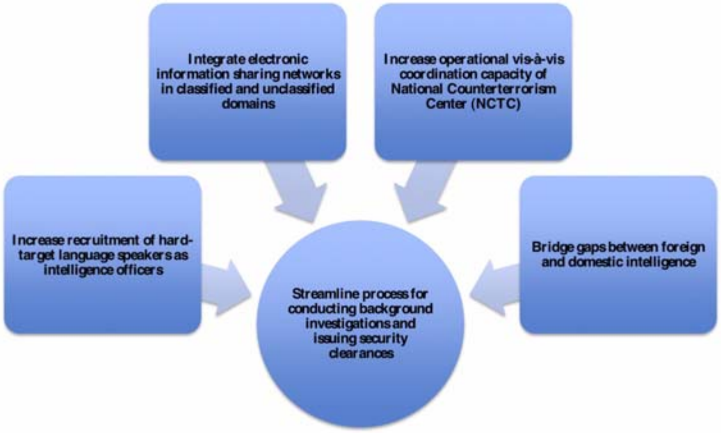

Integrate electronic information sharing networks in classified and unclassified domains
Increase operational vis-à-vis coordination capacity of National Counterterrorism Center (NCTC)
Increase recruitment of hard-target language speakers as intelligence officers
Bridge gaps between foreign and domestic intelligence
Streamline process for conducting background investigations and issuing security clearances

Figure 3 illustrates a detail of the dynamics involved among these issues in one direction—that is, a given reform challenge directly affecting the process of streamlining background investigations for security clearances. The need for additional hard-target language speakers drives enhancements to the background investigation screening process. A faster process will help filter viable candidates more efficiently. Integration of electronic information sharing networks, too, will increase the need for a streamlined security clearance system to enhance overall access for IC employees.

An elevated operational posture for the NCTC, in which the center directs intelligence operations in a more robust fashion, will theoretically impact the background investigation process by increasing demand for uniformity in clearance standards and furthering coordination and collaboration among IC members. The need to bridge the foreign-domestic intelligence divide, as well, necessitates refinements to the background investigation process for security clearances.

At present, certain security clearances (for instance, for the FBI) do not necessarily equate to other IC clearances (say, for the Defense Intelligence Agency). This effectively means that, in theory, a DIA employee may not automatically be granted access to information classified by the FBI, despite a "need to know." The reverse also holds true: an FBI analyst may not be given access to information classified by the DIA. This systemic deficiency can inhibit information sharing among intelligence and law enforcement agencies.

In reviewing the dynamic relationships among these five intelligence reform factors, the IC's systems architecture is underscored, and the need for concomitant systems-based approaches to reform is thrown into sharp relief. The interdependent nature of these issues is apparent, in that people, processes, technologies, and organizations must work in tandem to achieve synergies greater than the sum of their components.

Accordingly, systemic reform requires a systems-based approach that considers the totality of functions performed by the IC. Absent this holistic view, the potential for unintended consequences in the reform process increases, as decisions to modify one variable—information sharing networks or the security clearance process, for instance—inevitably have cascading effects upon others. The following section addresses the potential policy implications of utilizing systems engineering in intelligence reform, and speculates on this new approach's possible outcomes.

Potential Policy Implications

While transitioning to a systems-based approach doubtless would prove a long-term effort, a practical first step would involve the DNI assembling a focused working group of IC representatives, tasked with examining planned agency changes during the next five years. Given a basic primer on the principles and concepts of systems engineering, this working group could serve as a "brain trust," reporting directly to the DNI on the ramifications of anticipated changes and making recommendations to ensure their effectiveness.

The use of systems engineering stands to affect the intelligence reform process in organizational and technological respects. For example, divergent practices in granting security clearances can, in theory, be aligned. Through development of a single, IC-wide clearance adjudication standard, agency investigative offices stand to benefit from enhanced efficiency in operations, budgetary savings, simplification of administrative processes, and reduced confusion regarding interagency clearance compatibility.

The consolidation of electronic information sharing networks under a single, IC-wide portal could aid in providing analysts simpler options to search for critical pieces of raw intelligence, ultimately resulting in more useful intelligence products. With recent drastic increases in the volume of intelligence collected each day by the USG, the need for enhanced efficiency among analysts is greater than ever.

The case of Umar Farouk Abdulmutallab, the young Nigerian who attempted to detonate an improvised explosive device (IED) aboard a Detroit-bound airplane on December 25, 2009, underscores this observation. A White House incident review concluded that intelligence analysts had access to a sufficient amount of data to conclude that Abdulmutallab presented a threat, yet the inability to "connect the dots" about him resulted in part from the aggregate volume of intelligence and inadequate electronic search tools.[42] Strengthening these areas, then, remains a priority for the IC. While development of a single IC portal for electronic databases will not be a panacea, it may reduce duplication of effort, enhance visibility of discrete pieces of intelligence information, and facilitate more fluid information sharing.

The need to recruit and retain skilled hard-target linguists remains a challenge for the IC. This holds true in at least two respects: first, there is a quantifiable shortage of able personnel to provide translation services in hard-target languages; second, there is a clear lack of sufficient educational programs in secondary schools to allow for widespread early hard-target language acquisition. It may be that enhancing funding to secondary institutions to develop programs in Arabic, Persian, Mandarin-Chinese, and other hard-target languages could serve to expand the pool of potential intelligence officers to a number suitable for the future threat environment.

While the wall between intelligence agencies and law enforcement organizations is being dismantled, numerous challenges in intelligence sharing persist.[43] Through the development of a universal clearance standard, consolidation of access to electronic intelligence-sharing networks, and closer ties between intelligence operators and analysts in the NCTC, greater progress toward effective information sharing could be made.

Conclusions

This article argued that recent challenges in intelligence reform may be better understood by viewing the IC as a system, and therefore systems engineering can provide a more effective means for achieving organizational transformation within the IC.

Though approaches to intelligence reform have varied since the National Security Act of 1947, some might argue that the status quo—while imperfect, as with any process—provides sufficient advancement toward IC transformational goals. Yet recent history demonstrates that changes in one area (increased emphasis on information sharing, for example) can carry unexpected consequences in others (for instance, difficulty searching for intelligence information in databases). By contrast, a systems-based approach to reform takes into account myriad variables impacting reform, reducing the risk of missteps and errors during organizational changes. This, in turn, leads to increased efficiency.

The field of intelligence studies needs further research related to the connections between network theory and intelligence reform. Within the IC, the value of the network, broadly defined, is being applied in modes as diverse as Intellipedia and remotely controlled flights of unmanned aerial vehicles (UAVs). Connectedness—both virtual and real-world—adds value to intelligence operations. Understanding the effects of networks on intelligence organizational structure, particularly as "flatter" models of agencies and firms proliferate, would be beneficial to scholars and practitioners. Additionally, the potential ramifications of consolidating historically separate IC functions, like agency-specific security clearance adjudication and collaboration among operators and analysts, carry consequences for current IC projects. The possible implications of organizational changes that move toward streamlined IC operations should be investigated to assess their impact on service continuity, as well as budgetary consequences.

Recognizing the IC's character as that of a vast system, rather than a series of loosely knit components, acknowledges its rich complexity and interrelational dynamics. The IC is more than simply personnel, agencies, departments, and technologies: the relationships among these elements offer the greatest value to policymakers. Systems engineering solves problems in a holistic manner, and offers an approach to intelligence reform that better reflects the sophistication of this critical area of national security.

About the Author

Austen Givens teaches graduate courses on terrorism and emergency management at Utica College in Utica, NY. He previously served as director of emergency management at Christopher Newport University (CNU) in Virginia. Givens is a fellow with Virginia Commonwealth University's (VCU) National Homeland Security Project. He holds a master's degree in

DOI: <p>http://dx.doi.org/10.5038/1944-0472.5.1.5</p>

homeland security and emergency preparedness from VCU, and studied international relations in the Woodrow Wilson Department of Politics at the University of Virginia. He has worked with the Department of Homeland Security, the Office of the Secretary of Defense at the Pentagon, and the Virginia Fusion Center.

Thanks to Nathan E. Busch, Joe Giordano, Andrew Todd, Greg Walsh, and an anonymous reviewer for their helpful comments and suggestions on earlier versions of this article.

References

1 National Security Preparedness Group, *Tenth Anniversary Report Card: The Status of the 9/11 Commission Recommendations* (Washington, D.C.: Bipartisan Policy Center, September 2011), 17.

2 Richard A. Best, Jr., "The National Counterterrorism Center (NCTC)—Responsibilities and Potential Congressional Concerns," *Congressional Research Service*, February 1, 2011, available at: *http://opencrs.com/document/R41022/*.

3 See generally Central Intelligence Agency, "Intellipedia Celebrates Third Anniversary with a Successful Challenge," available at: *http://tinyurl.com/yjww33f (www.cia.gov/news-information/featured-story-archive/intellipedia-celebrates-third-anniversary.html)*; Richard A. Best, Jr., "Intelligence Information: Need to Know vs. Need to Share," *Congressional Research Service*, June 6, 2011, available at: *http://www.fas.org/sgp/crs/intel/R41848.pdf*; Department of Homeland Security Office of the Inspector General, *Information Sharing with Fusion Centers Has Improved, but Information Systems Challenges Remain*, October 2010, OIG-11-04, available at: *http://www.oig.dhs.gov/assets/Mgmt/OIG_11-04_Oct10.pdf*; Department of Homeland Security Press Release, *DHS Announces New Information Sharing Tool to Help Fusion Centers Combat Terrorism*, September 14, 2009, available at: *http://www.dhs.gov/ynews/releases/pr_1252955298184.shtm*.

4 U.S. Government Accountability Office, *Information Sharing Environment: Better Roadmap Needed to Guide Implementation and Investments*, July 2011, available at: *http://www.gao.gov/new.items/d08492.pdf*.

5 U.S. Congress, Senate Select Committee on Intelligence, *Intelligence Authorization Act for 2010*, Report 111–55, 111th Congress, 1st Session, July 22, 2009, available at: *http://intelligence.senate.gov/090722/11155.pdf*, 53–54.

6 Central Intelligence Agency, "History of the CIA," n.d., available at: *https://www.cia.gov/about-cia/history-of-the-cia/index.html*.

7 U.S. Department of State, "Foreign Relations of the United States 1945–1950: Emergence of the Intelligence Establishment," available at: *http://www.state.gov/www/about_state/history/intel/intro6.html*.

8 The National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (New York: W.W. Norton and Company, 2004), 411.

9 *Ibid.*, 403, 415, 416.

10 See Tennessee Bureau of Investigation, *Tennessee Fusion Center–Frequently Asked Questions*, n.d., available at: *http://www.tbi.state.tn.us/fusion_center/fusion_faq.shtml*; U.S. Government Accountability Office, *DOD Personnel Security Clearance Program*, n.d., available at: *http://www.gao.gov/highrisk/risks/recently_removed/security_clearance.php*.

11 NSPG, *Tenth Anniversary Report Card*, 17.

12 Best, Jr., *The National Counterterrorism Center*, 10.

13 U.S. Congress, Senate Select Committee on Intelligence, *Intelligence Authorization Act for 2010*, 53–54.

14 U.S. Government Accountability Office, *Personnel Clearances: Key Factors for Reforming the Security Clearance Process*, Testimony of Brenda S. Farrell before the U.S. Senate Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, Committee on Homeland Security and Governmental Affairs, GAO 08-776-T, May 22, 2008, available at: *http://www.gao.gov/cgi-bin/getrpt?GAO-08-776T*.

15 For example, see American Civil Liberties Union, "More About Fusion Centers," May 25, 2010, available at: *http://www.aclu.org/spy-files/more-about-fusion-centers*.

16 Rechtin, Eberhardt, *Systems Architecting of Organizations: Why Eagles Can't Swim* (New York: CRC Press, 2000), 4, cited in International Council on Systems Engineering, "A Consensus of the INCOSE Fellows," available at: *http://www.incose.org/practice/fellowsconsensus.aspx*.

17 Ibid.

18 See A. Terry Bahill and Bruce Gissing, "Re-Evaluating Systems Engineering Concepts Using Systems Thinking," *IEEE Transactions on Systems, Man, and Cybernetics - Part C: Applications and Reviews* 28:4 (November 1998); A. Terry Bahill and Frank F. Dean, "What is Systems Engineering? A Consensus of Senior Systems Engineers," available at: *http://www.sie.arizona.edu/sysengr/whatis/whatis.html*; International Council on Systems Engineering website, *http://www.incose.org*; Sage, Andrew P., *Methodology for Large-Scale Systems* (New York: McGraw Hill College, 1977), 5.

19 Bahill and Dean; International Council on Systems Engineering website, *http://www.incose.org*.

20 Information in Figure 1.0 derived from INCOSE.

DOI: <p>http://dx.doi.org/10.5038/1944-0472.5.1.5</p>

21 See Kuo-Ming Chang, Chieh-Li Chen, and Tzong-Lin Wu, "Real-Time Scheduling For Elevator Group Systems," *Systems Analysis Modeling Simulation* 43:12 (December 2003): 1675–1696; Sameer Kumar, Nidhi Ghildayal, and Cheryl Ostor, "A systems approach in examining optimization opportunities and dynamics of the global steel industry," *Information Knowledge Systems Management* 7 (2008): 401–427; Ricardo Valerdi, Deborah Nightingale, and Craig Blackburn, "Leveraging measurement systems to drive enterprise transformation: Two case studies from the U.S. aerospace industry," *Information Knowledge Systems Management* 9 (2010): 77–97.

22 Bahill and Dean.

23 Wendy L. Currie and Leslie Willcocks, "The New Branch Columbus project at Royal Bank of Scotland: the implementation of large-scale business process re-engineering," *Journal of Strategic Information Systems* 5 (1996): 213–236.

24 Rechtin, 76–77.

25 Renata Kopach-Konrad, Mark Lawley, Mike Criswell, Imran Hasan, Santanu Chakraborty, Joseph Pekny, and Bradley N. Doebbeling, "Applying Systems Engineering Principles in Improving Health Care Delivery," *Journal of General Internal Medicine* 22, Suppl. 3 (2007): 431–437.

26 Xiao Yan and Rollin J. Fairbanks, "Speaking Systems Engineering: Bilingualism in Health Care Delivery Organizations," *Mayo Clinic Proceedings* 86:8 (August 2011): 719–720.

27 Valerdi et al.

28 Armed Forces Communications and Electronics Association, "Lessons Learned: Building a New National Intelligence Partnership," *A White Paper Prepared by the AFCEA Intelligence Committee*, April 2006, available at: *http://www.afcea.org/mission/intel/documents/WhitePaperSpring06.pdf*.

29 Jeffrey Cooper, *Curing Analytic Pathologies: Pathways to Improved Intelligence Analysis* (Washington, DC: Central Intelligence Agency, Center for the Study of Intelligence, 2005), available at: *http://tinyurl.com/73l95c3 (www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/curing-analytic-pathologies-pathways-to-improved-intelligence-analysis-1/analytic_pathologies_report.pdf)*, 9.

30 Congressional Research Service, *Need-to-Know*, 10.

31 U.S. Government Accountability Office, *Numerous Federal Networks Used to Support Homeland Security Need to Be Better Coordinated with Key State and Local Information-Sharing Initiatives*, Report to the Chairman, Committee on Homeland Security, House of Representatives, Information Technology, GAO-07-455, April 2007, available at: *http://www.gao.gov/products/GAO-07-455*, 2; Department of Homeland Security Office of the Inspector General, *DHS' Efforts to Improve the Homeland Security Information Network*, OIG-09-07, October 2008, available at: *http://www.oig.dhs.gov/assets/Mgmt/OIG_09-07_Oct08.pdf*.

32 Richard A. Best, Jr., *The National Counterterrorism Center (NCTC)—Responsibilities and Potential Congressional Concerns*.

33 Congressional Research Service, *Intelligence Issues*, 13.

34 For example, see U.S. Government Accountability Office, *Homeland Security: Federal Efforts Are Helping to Alleviate Some Challenges Encountered By State and Local Information Fusion Centers*, GAO-08-35, October 2007, available at: http://www.gao.gov/products/GAO-08-35, 14, 18; GAO, 2008, *Personnel Clearances*; Department of Homeland Security Office of the Inspector General, *Information Sharing at the National Operations Center (Redacted)*, OIG-10-15, November 2009, available at: http://www.dhs.gov/xoig/assets/mgmtrpts/OIGr_10-15_Nov09.pdf, 24, 25, 27, 51.

35 GAO, 2008, *Personnel Clearances*.

36 Congressional Research Service, *NCTC*, 7.

37 For information on the benefits of second language learners interacting with native speakers of foreign languages, see Fred Genesee, "Integrating Language and Content: Lessons from Immersion," National Center for Research on Cultural Diversity and Second Language Learning, Education Practice Report 11, 1994, available at: http://escholarship.org/uc/item/61c8k7kh.

38 For example, see Federal Bureau of Investigation Careers, "Background Investigation," n.d., available at: http://www.fbijobs.gov/54.asp. Job applicants across the federal government who require a security clearance are responsible for completing the Standard Form 86.

39 Intelligence.gov, "We Have A Very Good Reason Why We Are So Careful About Whom We Select," n.d., available at: http://tinyurl.com/6sc4rql *(www.intelligence.gov/careers-in-intelligence/background-clearance-process/).*

40 Security clearances are adjudicated pursuant to predefined agency criteria, and take into account the totality of an individual's background. For select summaries of clearance adjudication hearings, see Department of Defense, "Industrial Security Clearance Decisions," n.d., available at: http://www.dod.mil/dodgc/doha/industrial/.

41 Congressional Research Service, *NCTC*, 7.

42 The White House, *Summary of the White House Review of the December 25, 2009 Attempted Terrorist Attack*, n.d., available at: http://tinyurl.com/yh97qdh *(www.whitehouse.gov/sites/default/files/summary_of_wh_review_12-25-09.pdf)*, 6.

43 U.S. Government Accountability Office, *Information Sharing: Progress Made and Challenges Remaining in Sharing Terrorism-Related Information*, Statement of Eileen R. Larence for the record to the Committee on Homeland Security and Government Affairs, U.S. Senate, GAO-12-144T, October 12, 2011, available at: http://www.gao.gov/new.items/d12144t.pdf.

DOI: <p>http://dx.doi.org/10.5038/1944-0472.5.1.5</p>