



# Chapter X

## Diagnosing Misfits, Inducing Requirements, and Delineating Transformations within Computer Network Operations Organizations

**Nikolaos Bekatoros HN**

*Naval Postgraduate School, USA*

**Jack L. Koons III**

*Naval Postgraduate School, USA*

**Mark E. Nissen**

*Naval Postgraduate School, USA*

### **ABSTRACT**

*The US Government is moving apace to develop doctrines and capabilities that will allow the Department of Defense (DoD) to exploit Cyberspace for military advantage, and the role of computer networked operations (CNO) has taken on greater importance with the rise of network-centric warfare. Unfortunately, extant CNO organizations are slow to anticipate and react, and as such do not operate well within their highly dynamic environments. Contingency Theory research provides considerable knowledge to guide designing organizational structures that fit well with various mission-environmental contexts, and as such it offers excellent potential to inform leaders and policy makers regarding how to bring their CNO organizations and approaches into better fit, and hence to improve performance. In this chapter, we identify a candidate set of organizational structures that offer potential to fit DoD better as it strives, and struggles, to address the technological advances and risks associated with CNO. Using*

*the Organizational Consultant (OrgCon) expert system to model and diagnose key problems and misfits associated with extant CNO organizations in the DoD, we propose a superior organizational structure for CNO that can also be applied to organizations in the international environment. Results elucidate important insights into CNO organization and management, suitable for immediate policy and operational implementation, and expand the growing empirical basis to guide continued research.*

## INTRODUCTION

The Internet has become the new frontier where nation states and stateless actors can communicate on a global scale and with a rate of speed and security as never seen before. The Internet has been operational since 1969 in one form or fashion, and over one billion people are said to use the Internet today (*estimated at 1,407,724,920 as of March 2008*, Internet Usage Statistics, 2008). Nation states in particular are becoming increasingly reliant on the Internet and Cyberspace for infrastructure to support economic and security interests.

In addition to nation states, the rise of terrorist groups such as Al Qaeda, and other nefarious groups such as mafia crime families, would have been unable to reach current epic proportions without such modern means of global communications. To counter threats from both nation states and nefarious groups, the US maintains numerous organizations (e.g., National Security Agency, military service network commands) charged with the protection and defense of the communications and network infrastructure enabled by the Internet. Indeed, one can argue that a plethora of different, often non-cooperating organizations (e.g., Federal Bureau of Investigation, Central Intelligence Agency) seek simultaneously and with minimal coordination to accomplish efficiently and effectively computer network operations. This confusion and uncoordination between them serves to slow responses to network attacks and intrusions, particularly where more than one organization strives simultaneously to provide critical infrastructure, expertise and technology.

To reverse this trend in part, the US Government is moving apace to develop doctrines and capabilities that will allow the Department of Defense (DoD) to exploit Cyberspace for military advantage. Within the broad rubric of Information Operations (IO), there is increasing effort devoted to shaping the organizational structures of Computer Network Operations (CNO) at the joint, combatant command, and service levels, and the role of CNO has taken on greater importance with the rise of network-centric warfare. Comprised primarily of defense, attack and exploitation, the technological capabilities are growing exponentially, as is the rate of data exchange, yet the organizational structures supporting CNO are slow to anticipate and react. This presents a serious issue in terms of mission-environmental fit, as such organizations do not operate well within their highly dynamic environments, nor are they suited well to the missions and expectations placed upon them.

A half century of Contingency Theory research (e.g., Burns & Stalker, 1961; Harvey, 1968; Galbraith, 1973) provides considerable knowledge to guide designing organizational structures that fit well with various mission-environmental contexts, and as such it offers excellent potential to inform leaders and policy makers regarding how to bring their CNO organizations and approaches into better fit, and hence to improve performance. The key research question is, which organizational configurations provide the best CNO performance within the network-centric environment?

The purpose of this chapter is to identify a candidate set of organizational structures that offer potential to fit DoD like agencies, and international organizations as they strive, and struggle,

to address the technological advances and risks associated with CNO. Using the Organizational Consultant (OrgCon) expert system to model and diagnose key problems and misfits associated with extant CNO organizations in the DoD, we propose a superior organizational structure for CNO, and we outline a three-step transformation plan to guide movement toward such structure.

In the balance of this chapter, we first review key background literature on CNO and the OrgCon expert system. We then describe a grounded CNO organization model specified via OrgCon, and depict such model in two, contrasting, network-centric environments. Results follow to elucidate important insights into CNO organization and management, suitable for immediate policy and operational implementation, and expand the growing empirical basis to guide continued research along these lines. Hence, the potential contribution of this research has both theoretical and real-world implications, and should appeal to both the academic and practitioner communities.

## **BACKGROUND**

In this section we describe a current CNO organization, focusing in particular on Computer Network Defense (CND) to ground our model in current practice for analysis. CND represents a very practical point to begin an investigation such as this: there is little opportunity to conduct computer attacks and exploitations if one's own defenses are weak, and one's own network is vulnerable. We then describe the Organizational Consultant expert system that drives our analysis of such grounded CND organization.

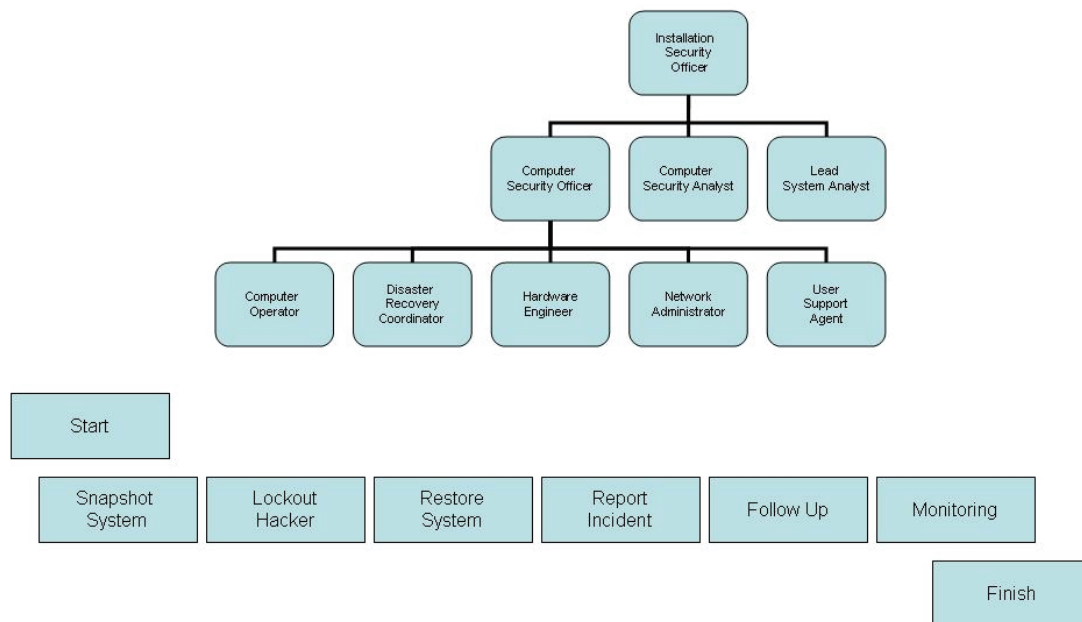
### **Grounded CND Model**

To understand computer network defense as it exists in the field, we survey best practices via published and online references (e.g., see US-CERT, 2008; SANS 2008; University of California

San Francisco Medical Center, 2008; University of Minnesota Office of Information Technology, 2008; The National Strategy to Secure Cyberspace, 2003; DoD IA Strategic Plan Version 1.1, 2004; DoD Net-Centric Data Strategy, 2003 ; CJCSI, 2007; Computer Security Enhancement Act of 2001, 2001; DoD Directive 5200.1-R, 1997), and speak at length with subject matter experts at a major DoD educational institution (to include lecturer and tenured faculty in the Department of Computer Science as well as Network Security Office specialists and administrators). This integrated, online and field research allows us to sample from a wide range of computer network organizational approaches (e.g., educational, governmental, business). We build upon such research to develop a general model, which provides the basis for our OrgCon analysis.

Figure 1 depicts a representative computer network defense approach (e.g., organizational structure, task structure, personnel staffing, technological infrastructure). We ground our depiction of this approach via analysis of the organization structures and workflow processes of a major U. S. West Coast university, and we subject such model to face validation by various DoD CND experts. Our exemplar organization was predicated on the availability of open source material concerning the respective CND effort. In addition, we determined their use of network infrastructure to support research and communication across a large and geographically disperse medical and research facility readily transferable towards any number of international, public, and private network operations. Notice that the CND organization depicted in the figure includes only three levels, and represents a relatively small organization. Clearly, CND comprises only a part of CNO, which in turn comprises only a part of IO, and so forth; hence, we focus on a tangible, front-line organization charged specifically to conduct CND. This provides considerable depth of focus for the study, and enables us to develop a specific, well-understood model for analysis. Nonetheless,

Figure 1. Computer network operations organization diagram & associated workflow



our survey confirms that this organization is quite typical of CND in practice today; hence our results should generalize relatively broadly. To ensure the widest audience, validation of our model was accomplished by tenured faculty and researchers at a major US educational institution as well as relevant subject matter experts. These experts are active in the CNO and CND arena-both in private and public practice.

To focus our modeling and analysis further, we concentrate on a single yet critical and common work process: responding to hacker attacks. This emerges from our survey and fieldwork summarized above as a perennial CND activity, and serves to facilitate the generalizability of this research further. Our model reflects the steps a CERT element (Computer Emergency Response Team) deals with the threat described below (US CERT 2008 & UCSF 2008):

*...There are two methods for dealing with an active hacker/cracker incident. The first method is to immediately lock the person out of the system and restore the system to a safe state. The second*

*method is to allow the hacker/cracker to continue his probe/attack and attempt to gather information that will lead to an identification and possible criminal conviction. The method used to handle a hacker/cracker incident will be determined by the level of understanding of the risks involved. In the case of an active hacker/cracker incident, a decision must be made whether to allow the activity to continue while evidence is gathered or to get the hacker/cracker off the system and then lock the person out. The Director of Infrastructure and Security Officer or the Network Architecture and Security manager must make this decision. The decision will be based on the availability of qualified personnel to monitor and observe the hacker/cracker and the risk involved.*

Indeed, responses to hacker attacks typically center on one of three main profiles: 1) unauthorized activity on the host system; 2) unauthorized attempt to gain access to the host system; and 3) anomalies on the host system discovered after the fact (UCSF Medical Center, 2008). The model depicted in the figure also reflects six CND work

Table 1. *CND work tasks and activities*

Work Task	Activities
Snapshot the System	Make copies of all audit trail information such as system log files, the root history files, and like tasks, and get a listing of all active network connections.
Lockout the Hacker	Kill all active processes for the hacker/cracker, and remove any files or programs that may have been left on the system. Change passwords for any accounts that were accessed by the hacker/cracker.
Restore the System	Restore the system to a normal stage. Restore any data or files that the hacker/cracker may have modified. Install patches or fixes to close any security vulnerabilities that the hacker/cracker may have exploited. Log all actions taken to restore the system to a normal state in a logbook.
Report the Incident	The incident should be reported following the security incident reporting procedures.
Follow Up	After the investigation, a short report describing the incident and actions that were taken should be documented and distributed to the appropriate personnel.
Monitoring	There are no set procedures for monitoring the activity of a hacker. However, monitored information should be reported in a written log. Each incident will be dealt with on a case-by-case basis. The person authorizing the monitoring activity should provide direction to those doing the monitoring. Once the decision has been made to cease monitoring the hacker's activities and have him removed from the system, the steps outlined previously (i.e., Removal of Hacker/Cracker) are followed.

tasks: 1) snapshot the system, 2) lockout hacker, 3) restore system, 4) report incident, 5) follow up, and 6) monitoring. Table 1 summarizes the key activities comprising these six tasks.

### **Organizational Consultant**

In this section, we describe the Organization Consultant, and indicate its potential for organizational design in the CND domain. DoD in general and the U.S. Air Force specifically, are in the early stages of identifying the basic infrastructure requirements and command and control (C2) mechanisms of CNO (Baddelay, 2008). In particular, the requirement for a CND operator to gain and maintain situational awareness while positioning for proactive response to asymmetrical network threats points to a need for clear C2 lines and organizational structure which supports the dynamic operational environment. Organizational Consultant allows us the ability to use computational modeling to identify those structures best suited for a particular operating environment.

As noted above, the Organization Consultant is a scholarship-based expert system that employs automated inference. A huge formalization and

integration of the Contingency Theory literature supports this scholarship-based expert system's knowledgebase. Most such formalization is made in terms of research propositions, expressed via If-Then rules, which are easily intelligible to people as well as machines.

For instance, one proposition reads (Burton and Obel, 2004, p. 19): "If environmental complexity is *simple*, and environmental change is *static*, then the organizational structure should be *functional*." Here the symbols "simple" and "static" represent inputs to the system, and the symbol "functional" represents the output. This formalizes one chunk of organization theory as articulated from above (Duncan, 1979). Other, similar chunks from Duncan's theoretical articulation are formalized similarly in terms of rules. Then theoretical chunks from other authors (e.g., Mintzberg, 1979; Perrow, 1967; Thompson, 1967) are formalized into additional rules, and so forth, until a substantial segment of the Contingency Theory literature is captured in the knowledgebase. For the interested reader this knowledgebase building process is described in Baligh et al (1993). The validation and refinement process used for the Organizational Consultant's knowledgebase relied on information obtained from twenty two case studies, consul-

tation with executives in telecommunications, pharmaceutical, manufacturing, retailing firms and others, dialogue with experts, and finally approximately 150 executive MBA (Master's program in Business Administration) students' assignments in an organizational design course, where the students were asked to apply Organizational Consultant to their organization (Carley and Prietula 1994).

Clearly not all authors from the organization studies literature agree with one another. Hence, many theoretical chunks are mutually inconsistent. The expert system uses the approach *certainty factors* to integrate such diverse and possibly conflicting theoretical chunks. This approach assigns confidence values to various propositions in the knowledgebase, values that are combined algorithmically to determine a composite level of confidence in a particular chunk. For instance, if two authors with propositions in the system agree with one another but a third one disagrees, one might expect to see a certainty factor of 0.67 (i.e., two-thirds) associated with the proposition. The second use of the certainty factors is to refer to the relative strength of the various contingency factors based on the examined organization. For example if the modeler believes that the decentralized structure of the examined organization is more important than its strategic type, different certainty factors can be used to reflect their relative strength. This represents a long-standing and effective approach to knowledge integration in expert systems (Carley and Prietula 1994). In our research, we kept the certainty factors constant (1.00) in order to avoid unnecessary complexity and eliminate any future concerns that the values of the certainty factors have in fact great influence on the output of the expert system. Therefore, the use of a fixed value for the certainty factors eliminates any bias and subjectivity unintentionally introduced by the researcher and any future disagreement among experts about the relative value of specific certainty factors.

Operationally, the Organizational Consultant takes as input description of an organization in terms of six dimensions (i.e., management and leadership style, organizational climate, size, environment, technology, strategy). The expert system asks a number of questions to gather inputs in each area. In the area concerning management style, questions pertain to organizational characteristics such as: top management involvement in data gathering and interpretation; top management control over decision-making; top management preferences in terms of pro-activity, risk-aversion and control; middle management control over budgets, rewards, hiring and unit evaluation; and others. In the area concerning organization climate, questions pertain to characteristics such as: interpersonal trust, sharing and openness; intra-organizational conflict, disagreement and friction; employee morale, confidence and enthusiasm; resistance to change; leader credibility; and others. Inputs such as these involve judgment and interpretation on the part of the person answering the Organizational Consultant's questions.

Size and ownership questions are more objective than those above are. For instance, size is measured principally by the number of employees; the age of the organization is selected from among multiple descriptive categories (e.g., new, mature); and the organization's establishment as a public or private enterprise is input. These represent factual questions. Questions pertaining to technology are similar but require some additional judgment. For instance, the user must determine whether the primary outputs are products or services; whether the technology involves mass production, automation, specialized customization, or some other; how routine (e.g., analyzable, with few exceptions) the technology is; how divisible (e.g., involving decomposable tasks) the work is; the extent of information systems use; and others.

Arguably, questions pertaining to the organizational environment and strategy fall somewhere in between those above in terms of judgment required to answer them. In the area concerning

environment, questions pertain to characteristics such as: environmental complexity, uncertainty, equivocally, hostility, and others. In the area concerning strategy, questions pertain to characteristics such as: capital requirements; product and process innovation; concern for quality; relative price level; and others.

The Organizational Consultant uses inputs gathered through such questions and answers to drive a matching process with its myriad propositional rules and confidence factors. Through the analytical lens of Contingency Theory, it uses evaluation criteria (e.g., *effectiveness*, *efficiency*, *viability*) to assess the organization's fit in terms of these inputs as well as an overall assessment of appropriateness in terms of its mission and environment. In a natural language format, it associates user inputs with theory through a series of classifications. For instance, it may characterize an organization as "small" or "large" based on the number of employees and the nature of their professionalism. Such classifications are rooted in organization theory. As another instance, it may characterize an organization as having an "internal process climate" or "developmental climate" based on answers to the user's answers provided to questions about organizational climate. As above, such classifications are rooted in organization theory. Theory rooted classifications in the other areas are provided as well in similar fashion.

Where potential misfits are diagnosed, the Organizational Consultant also provides relatively fine-grain, contextualized recommendations for improving fit through different organizational design alternatives. For instance, it may classify the organization as pursuing a "Defender" strategy, but recommend that an alternate strategy such as "Analyzer" appears to be more appropriate. As another instance, it may recommend restructuring a "Machine Bureaucracy" along the lines of an alternate organizational form such as "Functional Configuration," and it may suggest other structural changes such as decreasing the degree

of horizontal differentiation, formalization and centralization. Where multiple recommendations are suggested by the expert system rules and automated inference, it will list each recommendation separately, along with the corresponding certainty factor as an estimate of relative confidence, and explain the characteristics and implications of each. This section on diagnosed misfits and recommendations can be empty or very long, depending upon how well the organizational design appears to be appropriate for its mission and environment. This approach is quite novel in the domain of CNO research.

As with any computer-based system, the Organizational Consultant can be run multiple times for sensitivity analysis. This helps the user to gauge the degree to which one or more particular inputs may be driving the system's classifications, diagnoses and recommendations. To a large extent, this system is relatively robust to small changes in inputs. The inclusion of multiple conclusions and certainty factors augments such robustness. However, as with any computer-based system—particularly one that utilizes automated inference—problematic or erroneous inputs will guarantee problematic or erroneous outputs. Prudent modeling procedure calls for users to validate the accuracy and fidelity of their inputs.

## **ORGCN CND MODEL**

Building upon our discussion above, along with prior research (e.g. see Nissen, 2005), we use the OrgCon expert system environment to represent the structure and behavior of the grounded CND model from above. This analysis takes two steps. We analyze first the current organization in terms of a mission-environment scenario labeled "Simple Environment." This is used to characterize the environment where largely amateur hacker attacks target known network vulnerabilities, and which can be countered principally via the use of Standard Operating Procedures (SOPs) that exist

within the organization. This represents the nature of CND organizations' routine work, and provides an understandable baseline for comparison.

Then we analyze this same, grounded organization in a different scenario labeled "Complex Environment." This is used to characterize an environment where largely professional hacker attacks target unknown network vulnerabilities, which are much less likely to be countered effectively via solely SOPs as above. Although less common than the kinds of amateur attacks corresponding to the simple environment, defending the network effectively in this latter case is critical, as professional hackers can cause crippling damage if left unthwarted.

There is no doubt that there is middle ground between the two extreme cases that have been chosen for our research. There are two main reasons why this approach was followed. The first reason is that by examining the extremes the similarities and the differences are maximized, therefore can be identified and analyzed by the researcher with greater confidence. The second reason is that in order to examine a case that is in fact a hybrid of extreme cases one must first understand and analyze these extremes before examining the middle ground between them.

### **Simple Environment: Amateur Hacker Attack Scenarios**

This scenario conceives of the current CND organization that operates in a simple environment with relatively low levels of uncertainty and hostility. Following our discussion of OrgCon inputs above, six key aspects of the CND organization are addressed to instantiate a model: 1) organization size, 2) climate, 3) management style, 4) strategy, 5) organizational characteristics, and 6) technology. A detailed summary of OrgCon inputs and outputs is included in Appendix A.

Regarding size, the CND organization is modeled via OrgCon as "medium size," reflecting the 25 employees in our grounded model. Also, the

level of professionalism is very high in the CND team. This reflects not only ubiquitous college degrees among organization members but also the considerable formal training received by everyone inside the organization, and is consistent with the highly specialized jobs of people that work within the CND arena.

In terms of climate, the CND team is classified by OrgCon as having "internal process climate." This is consistent with the considerable work formalization, structure, procedure, formality, and policy guidance employed in the CND organization. The employees' morale and the high leader credibility suggest aspects of a "group" climate also, but several attributes of a "group" climate do not appear to match well with our grounded CND organization. The "group" climate is "a friendly place to work where people share a lot of themselves; success is defined in terms of sensitivity to customers and concern for people; and the organization places a premium on teamwork, participation, and consensus." which does not portray the climate of a CND organization.

The management style is classified as one of medium preference for "micro-involvement," because management has both a short-time and long-term horizon when making decisions when countering hacker attacks. The management of CND prefers taking actions on some decisions and being reactive toward others. The fact that management is risk averse and prefers using control to coordinate activities leads it toward a moderate preference for micro-involvement.

The strategy categories derive from Miles and Snow (1978), and include colorful terms such as *Prospector*, *Defender*, *Analyzer* and *Reactor* and are summarized in Table 2. An analyzer with innovation strategy appears to fit the CND organization well, and is a combination of the "Defender" and the "Prospector" strategies. A concern for high quality, moderate preference for micro-involvement and influence, and control over current operations all point to the analyzer with innovation strategy.



Table 2. The miles and snow strategy categories (adapted by Burton and Obel 1998)

Strategy Categories	Description
Prospector	An organization that almost continually searches for market opportunities and regularly experiments with potential responses to emerging environmental trends. Thus, the organization often is the creator of change and uncertainty to which its competitors must respond. However, because of its strong concern for product and market innovation, it usually is not completely efficient.
Defender	An organization that has a narrow product market domain. Top managers in this type of organization are highly expert in their organization's limited area of operation but do not tend to search outside their domains for new opportunities. As a result of this narrow focus, these organizations seldom need to make major adjustments in their technology, structure, or methods of operation. Instead, they devote primary attention to improving the efficiency of their existing operations.
Analyzer with innovation	An organization that combines the strategy of the defender and the prospector. It moves into the production of a new product or enters a new market after viability has been shown. But contrary to an analyzer without innovation, it does have innovations that run concurrently with the regular production. It has a dual technology core.
Analyzer without innovation	An organization whose goal is to move into new products or new markets only after their viability has been shown yet maintains an emphasis on its ongoing products. It has limited innovation related to the production process and generally not the product.
Reactor	An organization in which top management frequently perceives change and uncertainty occurring in their organizational environments but are unable to respond effectively. Because this type of organization lacks a consistent strategy or structure relationship, it seldom makes adjustment of any sort until forced to do so by environmental procedures.

Current organizational characteristics are driven by organizational differentiation, centralization and formalization. Differentiation has three components: horizontal, vertical and spatial. These three components of differentiation reflect, respectively: 1) breadth of organizational tasks and jobs, 2) number of hierarchical levels, and 3) geographical distribution of operations. Centralization pertains to information flows and decision rights being concentrated in the leadership at the organization's center. Formalization pertains to the level of standardization of work processes and written procedures to specify and govern work behavior and performance. These descriptors appear to fit the CND organization well.

Finally, technology refers to how the organization transforms inputs into outputs. The CND organization is characterized first as a *service* (i.e., not a product organization). CND does not produce products as manufacturing firms do. Rather it performs valuable services by defending the networks from hacker attacks. The current CND organization technology is characterized also as *standard, high-volume*. This reflects the high

degree of standardization in terms of computers, procedures, organizations, training, personnel and other aspects of CND, along with the high volume of attacks experienced by the organization. The CND technology is characterized further as *semi-routine*, reflecting the analyzability of work and predictability of associated outcomes, and is characterized also as *semi-divisible*, which pertains to the decomposability of work tasks into discrete and independent components. CND technology is characterized further as *strong dominant*, which refers to the sophisticated, capital-intensive networks and systems used for CND.

### **Complex Environment: Professional Hacker Attack Scenarios**

This scenario projects the grounded CND organization forward into a highly unstable and unpredictable environment where the organization has to counter professional hackers. As above, a detailed summary of OrgCon inputs and outputs is included in Appendix B.

With this Complex Environment scenario, all inputs to characterize the CND organization are the same as those above in the Simple Environment scenario except for those that refer specifically to the environment. As in a laboratory experiment, we hold constant the grounded CND organization, but vary systematically the nature of its environment. In other words, the same CND organization as described and analyzed above is assessed in a different environmental context.

The inputs *that differ* from above are the four for the environmental category. In the previous scenario: 1) simple environment, 2) with low level of uncertainty 3) and equivocality, 4) within a low hostility environment. In the current scenario: 1) complex environment, 2) with high levels of uncertainty 3) and equivocality, 4) within an extremely hostile environment.

## RESULTS

In this section, we present and discuss results of the OrgCon analysis. We begin by summarizing results for the simple and complex environments modeled above, and then proceed to induce a set of organizational design requirements for CND in both environments. We conclude by mapping a preliminary transformation plan for the grounded CND organization to follow.

*Table 3. OrgCon diagnosis of CND organization in simple environment*

Diagnosis	Misfit	Recommendation
Perceived Misfits	Analyzer with innovation Strategy	Defender or Analyzer without innovation strategy
Configuration	Machine Bureaucracy configuration	Functional configuration
Formalization	High formalization	Medium formalization

## Simple Environment

Based upon the model instantiated above, OrgCon draws upon its codified organizational design expertise to diagnose the misfits and recommend transformations to our grounded CND organization. The three such misfits and recommendations are summarized in Table 3.

First, OrgCon summarizes *perceived situation misfits*: aspects of the CND organization that do not appear to fit well with its environment. The analyzer with innovation strategy is questioned first as a possible misfit, because of the few different factors in the environment that affect the CND organization, the low equivocality of CND’s environment, and the internal process climate. An analyzer without innovation or a defender strategy is suggested as an alternate approach.

Second, OrgCon recommends that the most likely structure to fit the situation best is a functional configuration. A functional organization reflects unit grouping by functional specialization (e.g., computer operations, network administration, user support). The proposed configuration is functional because the equivocality of CND’s environment is not high, the environmental complexity is low, the environment is not highly uncertain, and the organization has an internal process climate. This configuration is feasible for a CND team since units based on functional specialization can counter hacker attacks (i.e. Block Hacker Team, Restore System Team, and Monitoring Team).

Third, OrgCon recommends that organizational formalization should be medium instead of high. It makes this recommendation, because there should be some formalization between the organizational units, but less formalization within the units due to the high professionalization. Medium size organizations and organizations with medium-routine technology should have medium formalization. Medium formalization is consistent with the leadership style when top

management’s preference for micro-involvement is medium also.

Based upon the diagnosis, we rerun the OrgCon CND Organization – Simple Environment model to reflect the three recommendations summarized in Table 3. This is essentially a test to see whether OrgCon’s recommendations are stable; that is, whether OrgCon will diagnose additional misfits even after making its recommended changes. In this situation, the recommendations are stable indeed, and OrgCon diagnoses no additional organizational misfits. For the interested reader, precise variable manipulations are mentioned in Appendix C. Hence, after altering the OrgCon model to reflect its recommendations—and thus obviate its prior misfits—we establish a CND organization reflecting good fit with its simple environment, and the organizational leader or manager has an operationalized set of steps that can be taken to improve the CND organization.

**Complex Environment**

As for the simple environment, based upon the model instantiated above, OrgCon draws upon its codified organizational design expertise to diagnose the misfits and recommend transformations to our grounded CND organization. The seven such misfits and recommendations are summarized in Table 4.

First, recall from above that we hold constant everything except our four environmental settings. Hence, the same *perceived situation misfits* suggested above (i.e., the analyzer with innovation strategy) obtains in this complex environment also. As above, an analyzer without innovation or a defender strategy is suggested as an alternative solution.

Second, OrgCon recommends that the fittest organizational configuration for this scenario is a simple organization that has a flat hierarchy with a singular head for control and decision making. The primary reason for recommending a simple configuration is that the organization faces extreme environmental hostility, which requires rapid responses to unforeseen challenges. As in the simple environment above, the machine bureaucracy cannot react quickly when unexpected events occur, and is not recommended. Interestingly, *most CND organizations in DoD are Machine Bureaucracies.*

Third, OrgCon recommends also that employees should be loosely supervised with the allowance to deviate from standards; therefore, the organizational formalization should be low. Moreover, the organizational complexity should be low since it is recommended that the number of job titles should be reduced from very many to very few. OrgCon recommends that the managers should get involved more in the data collection

*Table 4. OrgCon diagnosis of CND organization in complex environment*

<b>Diagnosis</b>	<b>Misfit</b>	<b>Recommendation</b>
Perceived Misfits	Analyzer with innovation Strategy	Defender or Analyzer without innovation strategy
Configuration	Machine Bureaucracy configuration	Simple structure configuration
Formalization	High formalization	Low formalization
Complexity	Many job titles	Few job titles
Centralization	Medium centralization	High centralization
Technology	Routine, high-volume technology	Flexible, adaptable technology
Climate	Internal process climate	Rational goal or development climate

and interpretation; therefore, the centralization should become high. This appears to be in direct conflict with current practice in many DOD like and international organizations and offers further research opportunities in terms of current private and public practice.

Further, CND is in a highly equivocal environment here, and may not be able to react responsively to changes in the environment due to the routine, high-volume nature of its technology. This is a vulnerable situation. A highly equivocal environment requires rapid adjustment to unpredictable environmental shifts, and calls for more flexible and adaptable technology.

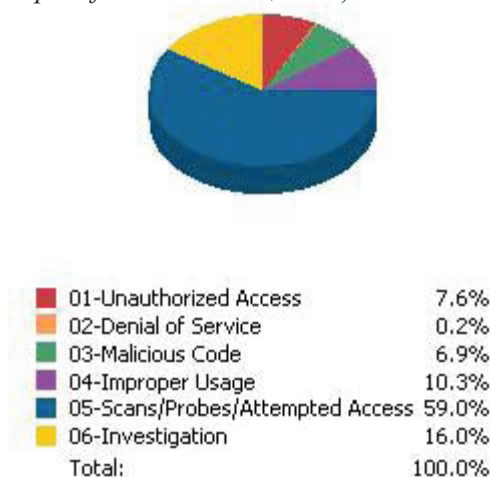
In addition, CND's internal process climate is questioned as a misfit, because it may cause problems in a high or moderately high equivocal environment. An internal process climate focuses more on the inside of the organization than on the outside. In an equivocal environment, which is likely to require change and adaptation, the internal process climate may not perceive the shifts or understand the need for change, and may not support adaptation to such needed change. An equivocal environment requires an external orientation, which is found in the rational goal and development climates.

Clearly, OrgCon diagnoses more misfits with the CND organization in the complex environment than in its simple counterpart, and produces correspondingly more recommendations for organizational transformation. As above, the diagnoses are stable, as no additional diagnoses result from rerunning OrgCon after making the recommended changes, and as above, the organizational leader or manager has an operationalized set of steps that can be taken to improve the CND organization.

## Design Requirements

In this section, using the OrgCon recommendations from above for guidance, we induce a set of design requirements for a CND organization to

Figure 2. Distribution of incidents and responses (adapted from US-CERT, 2007)



perform effectively in both simple and complex environmental contexts. The rationale is that our grounded CND organization faces *both simple and complex* environments simultaneously; that is, much of its time and energy are devoted to routine work such as locking out amateur hackers, but considerable time and energy are devoted to thwarting professional attacks as well.

Indeed, we draw from the fourth quarter United States Computer Emergency Response Team (US-CERT *Quarterly Trend Analysis: Cyber Security Trends, Metrics, and Security Indicators*, 2007) data summarized in Figure 2 to estimate that only 16% of hacker/cracker attempts conform to attacks by amateur hackers; the remaining 84% require more extensive organizational responses. Thus, we need to specify requirements for a CND organization that can respond simultaneously to both simple and complex environments. We draw from Tables 3 and 4 above, and integrate the corresponding OrgCon diagnoses and recommendations, to induce such organization design requirements. Clearly, because CND organizations are conservative by default, the integrated organization will tend to reflect the complex-environment recommendations summarized in Table 4 for the most part, but the organization

must be efficient as well, and be able to handle routine hacker attempts as such.

In particular, in a complex environment the flat hierarchy with a singular head for control and decision making is suggested, because the organization operates—most of the time—in an extremely hostile environment, one which requires consistently rapid responses to unforeseen challenges. Alternatively, in a simple environment a functional configuration is proposed, because the equivocality of CND’s environment is not high—at many times—the environmental complexity is low, not highly uncertain, and the organization needs to operate efficiently in these simple hacking cases. Combining these two results, an integrated approach could include a functional configuration but with a singular head for control and decision making. Where threats are deemed low, the CND organization can rely upon its functional groups and procedures to address amateur attacks, but where threats are high, the leader can still seize control, and take quick actions. The remaining requirements stem directly from recommendations summarized for the complex environment in Table 4.

### **Preliminary Transformation Plan**

Based upon the integrated recommendations above, our CND organization needs to address its strategy (i.e., analyzer with innovation), configuration (i.e., Machine Bureaucracy), formalization (i.e., high), technology (i.e., routine, high-volume), climate (i.e., internal process), complexity (i.e., many job titles) and centralization (i.e., medium). This represents organizational change of considerable scope, and it will be difficult to effect all aspects of such change either quickly or simultaneously. This is the case in particular for the conservative, highly proceduralized, DoD Machine Bureaucracy. Additionally, because all of the various organizational design elements need to fit together—at the same time—it is highly likely that some changing elements will have to *move*

*out of fit* as others wait for their times to change. This will leave the CND organization in multiple stages of misfit as the leaders and managers work to maneuver it into better overall fit through time. Therefore we are not describing an easy transformation by any means. Nonetheless, the alternative is to accept the status quo: considerable misfit and hence vulnerability. We outline the transformation plan in three, discrete steps.

**Step 1: Management Changes.** The easiest organizational design changes for management to effect pertain to management itself. Addressing the strategy is something that management can do directly, and adopting a Defender strategy would represent a natural progression for a conservative organization seeking to respond to an increasingly complex environment.

Additionally, management has considerable discretion to re-organize into a functional configuration, simply by revising the organization chart, and shifting people’s roles, responsibilities and reporting relationships. Since our grounded CND organization has a relatively small number of people, this should not impact its operations or performance greatly. New, fewer job titles will be required—for jobs that reflect less formalization—and current jobs can be combined to effect this change. This can all take place via written documentation.

Further, along with such re-organization, management can impose stricter policy regarding centralization of information flows and decision making. This will enable the organization to address the complex environment depicted in part by the professional hacker attacks. Where the simple environment depicted in part by the amateur hacker attacks obtains, management can delegate the organizational response via SOPs. These changes will prepare the organization to pursue the next steps.

**Step 2: Training and practice.** Myriad organizational changes fail to meet objectives, because people are not given adequate training and practice to perform well in different organizational conditions. It is one thing to tell people that they will be organized differently, that they will have new and fewer, less-formalized job titles, and that they will need to adhere to stricter centralization requirements than before; it is another for the people in an organization to adjust to such changes. They need to be trained, and they need to practice. Clearly trial-and-error, on-the-job “training” will provide much of the training and practice necessary, but this approach is both time-consuming and error-prone. Management should seek out professional help with training and practice, and institute fallback procedures for responding to attacks that exceed the CND organization’s capabilities while in transition.

**Step 3: Climate.** The third step involves the most difficult changes: moving to flexible and adaptable technology, and changing to a rational goal or developmental climate. Technological change can be expensive and time-consuming, and each new technology introduced into an organization tends to both disrupt its current operations and require modifications to jobs. Hence technological change will impart feedback on the steps above, and the organization will need to iterate repeatedly through these steps. Such repeated, impacted iteration is challenging.

Moreover, climate change involves culture: long and widely understood to be one of the most difficult aspects of an organization to alter. New managers and/or new employees may be required to accomplish this well, and any cultural change will need to be endorsed by the organizations

superior to our grounded CND unit, but training and practice can help here too. As above, management will need a fallback plan to address the likely cases of slow or stalled climate change, in addition to the repeated disruptions caused by new technology introductions.

In the end, management will have to assess whether the problems associated with its current CND organizational misfits outweigh the problems stemming from organizational change of the magnitude outlined in the three steps above. Perhaps a devastating, professional hacker attack will suffice to convince even the least change-oriented managers, but this would represent an expensive and hazardous way to learn. Counseling on how to convince reluctant managers is beyond the scope of this article, but outlining the three-step path to CND organizational transformation provides such managers with a plan to consider, and with a path to follow. This provides new knowledge to the CND organization manager, and can be used to generate new research questions for other CND researchers to investigate.

## **DISCUSSION & CONCLUSION**

The US Government is moving apace to develop doctrines and capabilities that will allow the DoD to exploit Cyberspace for military advantage, and the role of CNO has taken on greater importance with the rise of network-centric warfare. Comprised primarily of defense, attack and exploitation, the technological capabilities are growing exponentially, as is the rate of data exchange. Unfortunately, many extant CNO organizations are slow to anticipate and react, and as such do not operate well within their highly dynamic environments, nor are they suited well to the missions and expectations placed upon them today.

A half century of Contingency Theory research provides considerable knowledge to guide designing organizational structures that fit well with various mission-environmental contexts, and as

such it offers excellent potential to inform leaders and policy makers regarding how to bring their CNO organizations and approaches into better fit, and hence to improve performance. The key research question is, which organizational configurations provide the best CNO performance within the network-centric environment?

In this chapter, we review key background literature on CNO, and describe a current CNO organization. Focusing in particular on Computer Network Defense to ground our model in current practice, we discover how CND represents a very practical point to begin an investigation with the following premise: there is little opportunity for an organization with a specific network infrastructure to conduct computer attacks over time if its own defenses are weak.

We also describe the Organizational Consultant expert system that drives our analysis of such grounded CND organization, and note how this scholarship-based expert system's knowledge-base is supported by a huge formalization and integration of the Contingency Theory literature. Most such formalization is made in terms of research propositions, expressed via If-Then rules, which are easily intelligible to people as well as machines, and we learn how OrgCon diagnoses misfits between organizational structures and mission-environmental contexts.

Further, we use the OrgCon expert system environment to represent the structure and behavior of the grounded CND model from above, and depict such model in two, contrasting, network-centric environments:

1. A relatively simple environment — used to characterize one in which largely amateur hacker attacks target known network vulnerabilities, and which can be countered principally via the use of SOPs that exist within the organization
2. A relatively complex environment — used to characterize one in which largely professional hacker attacks target unknown

network vulnerabilities, and which are much less likely to be countered effectively via solely SOPs as above.

Results follow to diagnose three misfits for the grounded CND organization in a simple environment: 1) the analyzer with innovation strategy, 2) the Machine Bureaucracy configuration, and 3) high formalization. OrgCon diagnoses these same three misfits in a complex environment, in addition to four additional ones: 4) routine, high-volume technology, 5) internal process climate, 6) many job titles, and 7) medium centralization. Such diagnoses enable us to induce a set of design requirements for a CND organization to perform effectively in both simple and complex environmental contexts, understanding that such organization must respond to both. Of course, the most costly in terms of time and energy are those devoted to thwarting professional attacks.

This supports our development of a three-step transformation plan: 1) management changes, 2) training and practice, and 3) climate. Such plan constitutes organizational change of considerable magnitude—and that presents substantial challenge—and time to effect well. In the end, management will have to assess whether the problems associated with its current CND organizational misfits outweigh the problems stemming from organizational change of the magnitude outlined via this three-step plan.

Because of our grounded CND model and broadly applicable OrgCon expert system, results also elucidate important insights into CNO organization and management more generally. For instance, most bureaucratically driven CNO organizations (e.g., those organized within the DoD) are likely to suffer from misfit conditions similar to those diagnosed above for our grounded CND organization, and hence to benefit from similar transformational steps as outlined in response.

Further, such results are suitable for immediate policy and operational implementation. For instance, DoD policy makers can and should

call to assess all current CNO organizations for signs of misfits like those diagnosed through this study, and consider the relative advantages and disadvantages of undertaking change along the lines of our three-step plan versus leaving such organizations exposed to the risks inherent within misfit organizational structures.

Additionally, our results serve to expand the growing empirical basis of Contingency Theory, and appear to represent the first such results applicable specifically to DoD CNO. Such results can serve well to guide continued research along these lines. For instance, applying OrgCon to assess other, grounded, CND organizations would represent a logical next step, and assessing other aspects of CNO organizations (e.g., exploitation and attack) would follow logically as well. Indeed, this research highlights the promise inherent in the use of OrgCon to assess myriad DoD organizations—that is, well beyond the CNO domain—and calls for a wealth of applied research along these lines to begin. Hence the potential contribution of this research has both theoretical application and real-world implications, and should appeal therefore to both the academic and practitioner/policy maker communities.

Further, fieldwork is required to validate the model specifications and behaviors described above, as well as to apply and evaluate the kinds of insights and recommendations generated through this research. Such fieldwork can drive additional theoretical insight through induction as well, which can drive in turn further model development, and the subsequent expansion of organizational forms, missions and environments that can be analyzed and emulated. Laboratory research is similar. Indeed, these multiple types of research—theoretical, developmental, computational, field and laboratory—complement one another richly. When integrated into a coherent research stream, they enable the kind of progressive and cumulative accretion of new knowledge that represents a hallmark of science. This represents a relatively novel approach to generating

new knowledge in the CND domain, particularly as it pertains to the hacker attack response team at the group level.

Indeed, the present study provides useful insights regarding organization configuration and the attributes of a CND organization, but as with all studies, it has limitations that should be taken into account. The Organization Consultant is a scholarship-based expert system, which draws from the contingency theory literature to diagnose organizational misfits and to recommend transformations. One important limitation to this approach is that an organization may have some unique attributes that are not reflected well in the OrgCon contingency theory knowledgebase. This does not appear to be the case in the present study, but such limitation is endemic to expert systems, and should be considered by future researchers addressing research questions along the lines of this investigation.

Additionally, the level of analysis in our study is the *group*. Hence, our results apply most directly to group-level CND, and call for caution when making any generalizations the organizational or the inter-organizational levels of analysis. This calls for future research to address different levels of analysis explicitly. Also, the CND organization examined in our research reflects a medium-size organization operating within a DoD environment, and hence our results may not generalize well to either very large or very small organizations outside such environment. Additional research along the lines of this investigation are called for in this regard as well. Moreover, there is clearly substantial room for interpretation of OrgCon results, particularly where composing a set of organizational design requirements and outlining a transformation plan are concerned. The requirements and plan described in this chapter represent one of many approaches and paths that leaders, managers and policy makers can take. Nonetheless, they call for action, and serve to fill a current void in terms of guidance based upon grounded and systematic research.



## REFERENCES

- Baddelay, A. (2008, April). Systems for Cyber Control. *Military Information Technology*, 12(3). Retrieved May 15, 2008 from <http://www.military-information-technology.com/article.cfm?DocID=2398>
- Baligh, H., Burton, R. M., & Obel, B. (1993). *Creating the Theory for a Usable Organization Designing Expert System*. Working Paper, Fuqua School of Business, Duke University, Durham, NC.
- Burns, T., & Stalker, G. M. (1961). *The Management of Innovation*. London: Havistock.
- Burton, R. M., & Obel, B. (2004). *Strategic Organizational Diagnosis and Design: Developing Theory for Application*. Third Edition, Boston, MA: Kluwer.
- Carley, K. M., & Prietula, M. J. (1994). *Computational Organization Theory*. Hillsdale, NJ: Lawrence Erlbaum Associates, Inc.
- Chairman of the Joint Chiefs of Staff Instruction (CJCSI) (2007, Aug 14). *Information Assurance (IA) and Computer Network Defense (CND)*. Retrieved May 14, 2008 from [http://www.dtic.mil/cjcs\\_directives/cdata/unlimit/6510\\_01.pdf](http://www.dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf)
- Computer Security Enhancement Act of 2001*. (2001, Nov 28). Retrieved May 14, 2008 from <http://thomas.loc.gov/cgi-bin/query/D?c107:1:./temp/~c107VdS4Gr:>
- Department of Defense, (2003). *Information Operations Roadmap (classified)*. National Security Archive Electronic Briefing Book No. 177. Unclassified summary retrieved May 14, 2008 from <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/>
- DoD Directive 3020.26 (2007, Jan 1). *Defense Continuity Program (DCP)*. Retrieved May 14, 2008 from <http://www.dtic.mil/whs/directives/corres/html/302026.htm>
- DoD Directive 5200.1-R. (Jan 17 1997). *Information Security Program*. Retrieved May 14, 2008 from <http://www.dtic.mil/whs/directives/corres/pdf/520001r.pdf>
- DoD. (2004, Jan). *IA Strategic Plan Version 1.1*. Retrieved May 14, 2008 from [http://www.defenselink.mil/cio-nii/docs/DoD\\_IA\\_Strategic\\_Plan.pdf](http://www.defenselink.mil/cio-nii/docs/DoD_IA_Strategic_Plan.pdf)
- DoD Chief Information Officer (CIO) (2003, May 9). *DoD Net-Centric Data Strategy*. Retrieved May 14, 2008 from <http://www.defenselink.mil/cio-nii/docs/Net-Centric-Data-Strategy-2003-05-092.pdf>
- Duncan, R.B. (1979). What is the Right Organization Structure?. *Organizational Dynamics*, 7(3), 59-79.
- Galbraith, J. R. (1973). *Designing Complex Organizations*. Boston, MA: Addison-Wesley Longman Publishing Co., Inc.
- Harvey, E. (1968, April). Technology and the Structure of Organizations. *American Sociology Review*, 33, 247- 259.
- Internet Usage Statistics: The Internet Big Picture*. (2008, March). Last Retrieved 5/19/2008 from <http://www.internetworldstats.com/stats.htm>
- Miles, R. E., & Snow, C. C. (1978). *Organizational Strategy, Structure, and Process*. New York, NY: McGraw-Hill.
- Mintzberg, H. (1979). *The Structuring of Organizations*. Englewood Cliffs, NJ: Prentice-Hall.
- Mintzberg, H. (1980). Structure in 5's. A Synthesis of the Research on Organization Design. *Management Science*, 26(3), 322-341.
- North American Computational Social and Organization Sciences (NAACSOS)*. (2007). Retrieved March 13, 2008 from <http://www.casos.cs.cmu.edu/naacos/>

Nissen, M. E. (2005, June). A Computational Approach to Diagnosing Misfits, Inducing Requirements, and Delineating Transformations for Edge Organizations. *Proceedings International Command and Control Research and Technology Symposium*, McLean, VA.

Perrow, C. (1967). A Framework for Comparative Analysis of Organizations. *American Sociological Review*, 32, 194-208.

SANS Institute - about SANS. (2008). Retrieved May 14, 2008 from <http://www.sans.org/about/sans.php>

*The National Strategy to Secure Cyberspace Strategy to secure Cyberspace* (2003, February). Retrieved May 14, 2008 from <http://www.whitehouse.gov/pcipb/>

Thompson, J. D. (1967). *Organizations in Action*. New York, McGraw-Hill.

*UCSFIT Network Architecture & Security: About us*. (2008). Retrieved May 14, 2008 from [http://it-nas.ucsfmedicalcenter.org/about\\_us/](http://it-nas.ucsfmedicalcenter.org/about_us/)

*University of Minnesota Office of Information Technology Home Page*. (2008). Retrieved May 14, 2008 from [http://www1.umn.edu/oit/security/incident/OIT\\_\\_12654\\_REGION1.html](http://www1.umn.edu/oit/security/incident/OIT__12654_REGION1.html)

*US-CERT: United States Computer Emergency Readiness Team*. (2008). Retrieved May 14, 2008 from <http://www.us-cert.gov/>

*US-CERT Quarterly Trend Analysis: Cyber Security Trends, Metrics, and Security Indicators*. (2007, December). Retrieved May 14, 2008 from [http://www.us-cert.gov/press\\_room/trendsanalysisQ407.pdf](http://www.us-cert.gov/press_room/trendsanalysisQ407.pdf)

## **APPENDIX A: ORGCON ANALYSIS AND RECOMMENDATIONS FOR SIMPLE ENVIRONMENTS**

### **Report summary — CND**

#### **Input Data Summary**

The description below summarizes and interprets your answers to the questions about your organization and its situation. It states your answers concerning the organization's current configuration, complexity, formalization, and centralization. Your responses to the various questions on the contingencies of age, size, technology, environment, management style, cultural climate and strategy factors are also given. The writeup below summarizes the input data for the analysis.

- CND has a machine bureaucracy configuration (cf 100).
- CND has a large number of different jobs (cf 100).
- Of the employees at CND 76 to 100 % have an advanced degree or many years of special training (cf 100).
- CND has 3 to 5 vertical levels separating top management from the bottom level of the organization (cf 100).
- The mean number of vertical levels is 3 to 5 (cf 100).
- CND has 1 or 2 separate geographic locations (cf 100).
- CND's average distance of these separate units from the organization's headquarters is less than 10 miles (cf 100).
- 61 to 90 % of CND's total workforce is located at these separate units (cf 100).
- Job descriptions are available for all employees, including senior management (cf 100).
- Where written job descriptions exist, the employees are supervised closely to ensure compliance with standards set in the job description (cf 100).
- The employees are allowed to deviate very little from the standards (cf 100).
- 81 to 100 % non-managerial employees are given written operating instructions or procedures for their job (cf 100).
- The written instructions or procedures given are followed to a very great extent (cf 100).
- Supervisors and middle managers are to a little extent free from rules, procedures, and policies when they make decisions (cf 100).
- More than 80 % of all the rules and procedures that exist within the organization are in writing (cf 100).
- Top Management is not involved in gathering the information they will use in making decisions (cf 100).
- Top management participates in the interpretation of more than 80 % of the information input (cf 100).
- Top management directly controls 0 to 20 % of the decisions executed (cf 100).
- The typical middle manager has no discretion over establishing his or her budget (cf 100).
- The typical middle manager has some discretion over how his/her unit will be evaluated (cf 100).

### ***Diagnosing Misfits, Inducing Requirements, and Delineating Transformations***

- The typical middle manager has great discretion over the hiring and firing of personnel (cf 100).
- The typical middle manager has no discretion over personnel rewards - (ie, salary increases and promotions) (cf 100).
- The typical middle manager has little discretion over purchasing equipment and supplies (cf 100).
- The typical middle manager has some discretion over establishing a new project or program (cf 100).
- The typical middle manager has little discretion over how work exceptions are to be handled (cf 100).
- CND has 25 employees (cf 100).
- CND's age is mature (cf 100).
- CND's ownership status is public (cf 100).
- CND has an undetermined number of different products (cf 100).
- CND has an undetermined number of different markets (cf 100).
- CND only operates in one country (cf 100).
- CND has an undetermined number of different products in the foreign markets (cf 100).
- CND's major activity is categorized as service (cf 100).
- CND has a standard high-volume service technology (cf 100).
- CND has a medium routine technology (cf 100).
- CND's technology is somewhat divisible (cf 100).
- CND's technology dominance is strong (cf 100).
- CND has either planned or already has an advanced information system (cf 100).
- CND's environment is simple (cf 100).
- The uncertainty of CND's environment is low (cf 100).
- The equivocality of the organization's environment is low (cf 100).
- CND's environment has a low hostility (cf 100).
- Top management prefers to make policy and general resource allocation decisions (cf 100).
- Top management primarily prefers to make both long-term and short-time decisions (cf 100).
- Top management has a preference for medium detailed information when making decisions (cf 100).
- Top management has a preference for some proactive actions and some reactive actions (cf 100).
- Top management is risk averse (cf 100).
- Top management has a preference for high control (cf 100).
- CND operates in an industry with an undetermined level of capital requirement (cf 100).
- CND has an undetermined level of product innovation (cf 100).
- CND has a high process innovation (cf 100).
- CND has a high concern for quality (cf 100).
- CND's price level is undetermined relative to its competitors (cf 100).
- The level of trust is medium (cf 100).
- The level of conflict is medium (cf 100).
- The employee morale is medium (cf 100).
- Rewards are given in an inequitably fashion (cf 100).
- The resistance to change is high (cf 100).
- The leader credibility is high (cf 100).
- The level of scapegoating is medium (cf 100).

## The Size

The size of the organization - large, medium, or small - is based upon the number of employees, adjusted for their level of education or technical skills.

Based on the answers you provided, it is most likely that your organization's size is medium (cf 50).

More than 75 % of the people employed by CND have a high level of education. Adjustments are made to this effect. The adjusted number of employees is lower than 500 but greater than 100 and CND is categorized as medium. However, for this adjusted number this size does not have a major effect on the organizational structure.

## The Climate

The organizational climate effect is the summary measure of people and behavior.

Based on the answers you provided, it is most likely that the organizational climate is a internal process climate (cf 79).

It could also be the that climate is a group (cf 69).

The internal process climate is a formalized and structured place to work. Procedures govern what people do. The leaders pride themselves on being good coordinators and organizers. Maintaining a smooth running organization is important. The long-term concerns are stability, predictability, and efficiency. Formal rules and policies hold the organization together.

Employees with a medium to low morale is frequently one element of an internal process climate. Inequitable rewards in the organization drives the climate towards an internal process climate. High resistance to change is normally present in a internal process climate.

The group climate is characterized as a friendly place to work where people share a lot of themselves. It is like an extended family. The leaders, or head of the organization, are considered to be mentors and, perhaps even parent figures. The organization is held together by loyalty or tradition. Commitment is high. The organization emphasizes the long-term benefit of human resource development with high cohesion and morale being important. Success is defined in terms of sensitivity to customers and concern for people. The organization places a premium on teamwork, participation, and consensus.

Employees with a medium morale can be one element of group climate. High leader credibility characterizes an organization with a group climate.

## The Management Style

The level of management's microinvolvement in decision making is the summary measure of management style. Leaders have a low preference for microinvolvement; managers have a high preference for microinvolvement.

Based on the answers you provided, it is most likely that your management profile has a medium preference for microinvolvement (cf 78).

It could also be that your management profile has a high preference (cf 69).

Management has both a short-time and long-term horizon when making decisions, which characterizes a preference for a medium microinvolvement. Since the management has a preference for medium detailed information when making decisions a medium preference for microinvolvement characteriza-

tion is appropriate. The management of CND has a preference for taking actions on some decisions and being reactive toward others. This will lead toward a medium preference for microinvolvement.

Management is risk averse. This is one of the characteristics of a manager with a high preference for microinvolvement. Management has a preference for using control to coordinate activities, which leads toward a high preference for microinvolvement.

## The Strategy

The organization's strategy is categorized as one of either prospector, analyzer with innovation, analyzer without innovation, defender, or reactor. These categories follow Miles and Snow's typology. Based on your answers, the organization has been assigned to a strategy category. This is a statement of the current strategy; it is not an analysis of what is the best or preferred strategy for the organization.

Based on the answers you provided, it is most likely that your organization's strategy is an analyzer with innovation strategy (cf 68).

An organization with an analyzer with innovation strategy is an organization that combines the strategy of the defender and the prospector. It moves into the production of a new product or enters a new market after viability has been shown. But in contrast to an analyzer without innovation, it has innovations that run concurrently with the regular production. It has a dual technology core.

For a medium routine technology, CND has some flexibility. It is consistent with an analyzer with innovation strategy. With a concern for high quality an analyzer with innovation strategy is a likely strategy for CND. With top management preferring a medium level of microinvolvement top management wants some influence. This can be obtained via control over current operations. Product innovation should be less controlled. The strategy is therefore likely to be analyzer with innovation.

## The Current Organizational Characteristics

Based on your answers, the organization's complexity, formalization, and centralization have been calculated. This is the current organization. Later in this report, there will be recommendations for the organization.

The current organizational complexity is medium (cf 100).

The current horizontal differentiation is high (cf 100).

The current vertical differentiation is low (cf 100).

The current spatial differentiation is medium (cf 100).

The current centralization is medium (cf 100).

The current formalization is high (cf 100).

The current organization has been categorized with respect to formalization, centralization, and complexity. The categorization is based on the input you gave and does not take missing information into account.

## Situation Misfits

A situation misfit is an unbalanced situation among the contingency factors of management style, size, environment, technology, climate, and strategy.

The following misfits are present: (cf 100).

## ***Diagnosing Misfits, Inducing Requirements, and Delineating Transformations***

When only few factors in the environment affect CND, the analyzer with innovation strategy may not be a suitable one! With only a few environmental factors, there may be limited need for innovation and adaptation. There are probably limited opportunities to which to adapt. An analyzer without innovation, or a defender strategy that focuses directly on the few environmental factors and meets market needs efficiently will usually yield better results.

When the equivocality of CND's environment is low, the analyzer with innovation strategy may not be a suitable one! With low equivocality, the environment is well known and understood. An innovative strategy works best when the environment offers new opportunities for products and services. Here such opportunities are limited. However, process innovation, which reduces costs, is appropriate.

CND has an internal process climate. This is a mismatch with analyzer with innovation strategy! An internal process climate is internally oriented with a focus on control. Innovation is difficult to achieve with this orientation. More flexibility and a more external orientation are desirable for innovation. An internal process climate supports better an analyzer without innovation and defender strategy.

### **Orgcon Recommendations**

Based on your answers about the organization, its situation, and the conclusions with the greatest certainty factor from the analyses above OrgCon has derived recommendations for the organization's configuration, complexity, formalization, and centralization. There are also recommendations for coordination and control, the appropriate media richness for communications, and incentives. More detailed recommendations for possible changes in the current organization are also provided.

### **Organizational Configurations**

The most likely configuration that best fits the situation has been estimated to be a functional configuration (cf 44).

A functional organization is an organization with unit grouping by functional specialization (production, marketing, etc.).

When the equivocality of CND's environment is not high, the environmental complexity is low, and the environment is not highly uncertain, the configuration should be functional. An organization with an internal process climate could have a functional configuration.

### **Organizational Characteristics**

The recommended degree of organizational complexity is medium (cf 63).

Medium size organizations should have medium organizational complexity. CND has a technology that is somewhat routine, which implies that the organizational complexity should be medium. When the uncertainty of CND's environment is low, the organizational complexity should neither be very low nor very high so that CND will be able to react quickly when the environment changes. Top management of CND has a preference for a medium level of microinvolvement, which drives the organizational complexity towards medium. Because CND has an advanced information system, organizational complexity can be greater than it could otherwise.

The recommended degree of horizontal differentiation is medium (cf 28).

The recommended degree of vertical differentiation is medium (cf 64).

The recommended degree of formalization is medium (cf 55).

There should be some formalization between the organizational units but less formalization within the units due to the high professionalization. Medium size organizations should have medium formalization. Organizations with medium-routine technology should have a medium formalization. Medium formalization is consistent with the leadership style when top management's preference for microinvolvement is neither very great nor very low.

The recommended degree of centralization is medium (cf 55).

CND has an analyzer with innovation strategy. Centralization should be medium. There should be tight control over current activities and looser control over new ventures. CND is of medium size. Such organizations should have medium to high centralization. Medium centralization is recommended when top management has neither a great desire nor very little desire for microinvolvement. Because CND has an advanced information system, centralization can be greater than it could otherwise. An internal process climate in the organization requires a medium to high level of centralization.

CND's span of control should be moderate (cf 62).

Since CND has some technology routineness, it should have a moderate span of control.

CND should use media with medium media richness (cf 70).

The information media that CND uses should provide a small amount of information (cf 70).

Incentives should be based on procedures (cf 85).

CND should use planning as means for coordination and control (cf 87).

When the environment of CND has low equivocality, low uncertainty, and low complexity, the information media need not be rich nor provide a large amount of information. Direct supervision with some planning will be appropriate. Incentives can be procedure based and based on implementation of the rules of formalization. It is appropriate to see that the rules are followed and implemented.

## Organizational Misfits

Organizational misfits compares the recommended organization with the current organization.

The following organizational misfits are present: (cf 100).

Current and prescribed configuration do not match.

Current and prescribed formalization do not match.

## More Detailed Recommendations

There are a number of more detailed recommendations (cf 100).

You may consider decreasing the number of positions for which job descriptions are available.

You may consider supervising the employees less closely.

You may consider allowing employees more latitude from standards.

You may consider fewer written job descriptions.

Managerial employees may be asked to pay less attention to written instructions and procedures.

You may give supervisors and middle managers fewer rules and procedures.

You may consider having fewer rules and procedures put in writing.



## **APPENDIX B: ORGCON ANALYSIS AND RECOMMENDATIONS FOR COMPLEX ENVIRONMENTS**

### **Report Summary — CND**

#### Input Data Summary

The description below summarizes and interprets your answers to the questions about your organization and its situation. It states your answers concerning the organization's current configuration, complexity, formalization, and centralization. Your responses to the various questions on the contingencies of age, size, technology, environment, management style, cultural climate and strategy factors are also given. The writeup below summarizes the input data for the analysis.

- CND has a machine bureaucracy configuration (cf 100).
- CND has a large number of different jobs (cf 100).
- Of the employees at CND 76 to 100 % have an advanced degree or many years of special training (cf 100).
- CND has 3 to 5 vertical levels separating top management from the bottom level of the organization (cf 100).
- The mean number of vertical levels is 3 to 5 (cf 100).
- CND has 1 or 2 separate geographic locations (cf 100).
- CND's average distance of these separate units from the organization's headquarters is less than 10 miles (cf 100).
- 61 to 90 % of CND's total workforce is located at these separate units (cf 100).
- Job descriptions are available for all employees, including senior management (cf 100).
- Where written job descriptions exist, the employees are supervised closely to ensure compliance with standards set in the job description (cf 100).
- The employees are allowed to deviate very little from the standards (cf 100).
- 81 to 100 % non-managerial employees are given written operating instructions or procedures for their job (cf 100).
- The written instructions or procedures given are followed to a very great extent (cf 100).
- Supervisors and middle managers are to a little extent free from rules, procedures, and policies when they make decisions (cf 100).
- More than 80 % of all the rules and procedures that exist within the organization are in writing (cf 100).
- Top Management is not involved in gathering the information they will use in making decisions (cf 100).
- Top management participates in the interpretation of less than 20 % of the information input (cf 100).
- Top management directly controls 0 to 20 % of the decisions executed (cf 100).
- The typical middle manager has no discretion over establishing his or her budget (cf 100).
- The typical middle manager has great discretion over how his/her unit will be evaluated (cf 100).

### ***Diagnosing Misfits, Inducing Requirements, and Delineating Transformations***

- The typical middle manager has great discretion over the hiring and firing of personnel (cf 100).
- The typical middle manager has no discretion over personnel rewards - (ie, salary increases and promotions) (cf 100).
- The typical middle manager has little discretion over purchasing equipment and supplies (cf 100).
- The typical middle manager has some discretion over establishing a new project or program (cf 100).
- The typical middle manager has little discretion over how work exceptions are to be handled (cf 100).
- CND has 25 employees (cf 100).
- CND's age is mature (cf 100).
- CND's ownership status is public (cf 100).
- CND has an undetermined number of different products (cf 100).
- CND has an undetermined number of different markets (cf 100).
- CND only operates in one country (cf 100).
- CND has an undetermined number of different products in the foreign markets (cf 100).
- CND's major activity is categorized as service (cf 100).
- CND has a standard high-volume service technology (cf 100).
- CND has a medium routine technology (cf 100).
- CND's technology is somewhat divisible (cf 100).
- CND's technology dominance is strong (cf 100).
- CND has either planned or already has an advanced information system (cf 100).
- CND's environment is complex (cf 100).
- The uncertainty of CND's environment is high (cf 100).
- The equivocality of the organization's environment is high (cf 100).
- CND's environment is extremely hostile (cf 100).
- Top management prefers to make policy and general resource allocation decisions (cf 100).
- Top management primarily prefers to make both long-term and short-time decisions (cf 100).
- Top management has a preference for medium detailed information when making decisions (cf 100).
- Top management has a preference for some proactive actions and some reactive actions (cf 100).
- Top management is risk averse (cf 100).
- Top management has a preference for high control (cf 100).
- CND operates in an industry with an undetermined level of capital requirement (cf 100).
- CND has an undetermined level of product innovation (cf 100).
- CND has a high process innovation (cf 100).
- CND has a high concern for quality (cf 100).
- CND's price level is undetermined relative to its competitors (cf 100).
- The level of trust is medium (cf 100).
- The level of conflict is medium (cf 100).
- The employee morale is medium (cf 100).
- Rewards are given in an inequitably fashion (cf 100).
- The resistance to change is high (cf 100).
- The leader credibility is high (cf 100).
- The level of scapegoating is medium (cf 100).

## The Size

The size of the organization - large, medium, or small - is based upon the number of employees, adjusted for their level of education or technical skills.

Based on the answers you provided, it is most likely that your organization's size is medium (cf 50).

More than 75 % of the people employed by CND have a high level of education. Adjustments are made to this effect. The adjusted number of employees is lower than 500 but greater than 100 and CND is categorized as medium. However, for this adjusted number this size does not have a major effect on the organizational structure.

## The Climate

The organizational climate effect is the summary measure of people and behavior.

Based on the answers you provided, it is most likely that the organizational climate is a internal process climate (cf 79).

It could also be the that climate is a group (cf 69).

The internal process climate is a formalized and structured place to work. Procedures govern what people do. The leaders pride themselves on being good coordinators and organizers. Maintaining a smooth running organization is important. The long-term concerns are stability, predictability, and efficiency. Formal rules and policies hold the organization together.

Employees with a medium to low morale is frequently one element of an internal process climate. Inequitable rewards in the organization drives the climate towards an internal process climate. High resistance to change is normally present in a internal process climate.

The group climate is characterized as a friendly place to work where people share a lot of themselves. It is like an extended family. The leaders, or head of the organization, are considered to be mentors and, perhaps even parent figures. The organization is held together by loyalty or tradition. Commitment is high. The organization emphasizes the long-term benefit of human resource development with high cohesion and morale being important. Success is defined in terms of sensitivity to customers and concern for people. The organization places a premium on teamwork, participation, and consensus.

Employees with a medium morale can be one element of group climate. High leader credibility characterizes an organization with a group climate.

## The Management Style

The level of management's microinvolvement in decision making is the summary measure of management style. Leaders have a low preference for microinvolvement; managers have a high preference for microinvolvement.

Based on the answers you provided, it is most likely that your management profile has a medium preference for microinvolvement (cf 78).

It could also be that your management profile has a high preference (cf 69).

Management has both a short-time and long-term horizon when making decisions, which characterizes a preference for a medium microinvolvement. Since the management has a preference for medium detailed information when making decisions a medium preference for microinvolvement characteriza-

tion is appropriate. The management of CND has a preference for taking actions on some decisions and being reactive toward others. This will lead toward a medium preference for microinvolvement.

Management is risk averse. This is one of the characteristics of a manager with a high preference for microinvolvement. Management has a preference for using control to coordinate activities, which leads toward a high preference for microinvolvement.

## The Strategy

The organization's strategy is categorized as one of either prospector, analyzer with innovation, analyzer without innovation, defender, or reactor. These categories follow Miles and Snow's typology. Based on your answers, the organization has been assigned to a strategy category. This is a statement of the current strategy; it is not an analysis of what is the best or preferred strategy for the organization.

Based on the answers you provided, it is most likely that your organization's strategy is an analyzer with innovation strategy (cf 68).

An organization with an analyzer with innovation strategy is an organization that combines the strategy of the defender and the prospector. It moves into the production of a new product or enters a new market after viability has been shown. But in contrast to an analyzer without innovation, it has innovations that run concurrently with the regular production. It has a dual technology core.

For a medium routine technology, CND has some flexibility. It is consistent with an analyzer with innovation strategy. With a concern for high quality an analyzer with innovation strategy is a likely strategy for CND. With top management preferring a medium level of microinvolvement top management wants some influence. This can be obtained via control over current operations. Product innovation should be less controlled. The strategy is therefore likely to be analyzer with innovation.

## The Current Organizational Characteristics

Based on your answers, the organization's complexity, formalization, and centralization have been calculated. This is the current organization. Later in this report, there will be recommendations for the organization.

The current organizational complexity is medium (cf 100).

The current horizontal differentiation is high (cf 100).

The current vertical differentiation is low (cf 100).

The current spatial differentiation is medium (cf 100).

The current centralization is medium (cf 100).

The current formalization is high (cf 100).

The current organization has been categorized with respect to formalization, centralization, and complexity. The categorization is based on the input you gave and does not take missing information into account.

## Situation Misfits

A situation misfit is an unbalanced situation among the contingency factors of management style, size, environment, technology, climate, and strategy.

The following misfits are present: (cf 100).

## ***Diagnosing Misfits, Inducing Requirements, and Delineating Transformations***

ND is in a highly equivocal environment, but has a mass production technology. CND may not be able to react to changes in the environment. This is a vulnerable situation. Most mass production operations are very limited in capacity to adapt and make different products. Mass production optimizes on the economies of specialization and standardization. A highly equivocal environment requires adjustment to the unknown as that environment becomes clearer. The possibility for mismatch of what the existing mass production can do and what will be required in the new environment is very high and further the economic consequences are likely to be great with low return. A highly equivocal environment calls for a more non routine production capability than most mass production operations have.

CND has an internal process climate. This may cause problems in a high or moderately high equivocal environment! An internal process climate focuses more on the inside of the organization than on the outside. In an equivocal environment which is likely to require change and adaptation, the internal process climate may not either see the shift, understand the need for change and does not have an organization which supports adaptation to such needed change. There is high resistance to change. An equivocal environment requires an external orientation which is found in the rational goal and development climates.

CND has an internal process climate. This is a mismatch with analyzer with innovation strategy! An internal process climate is internally oriented with a focus on control. Innovation is difficult to achieve with this orientation. More flexibility and a more external orientation are desirable for innovation. An internal process climate supports better an analyzer without innovation and defender strategy.

### **OrgCon Recommendations**

Based on your answers about the organization, its situation, and the conclusions with the greatest certainty factor from the analyses above OrgCon has derived recommendations for the organization's configuration, complexity, formalization, and centralization. There are also recommendations for coordination and control, the appropriate media richness for communications, and incentives. More detailed recommendations for possible changes in the current organization are also provided.

### **Organizational Configurations**

The most likely configuration that best fits the situation has been estimated to be a simple configuration (cf 70).

It is certainly not: a machine bureaucracy (cf -100).

A simple organization has a flat hierarchy and a singular head for control and decision making.

The primary reason for recommending a simple configuration is that the organization has extreme environmental hostility. Extreme environmental hostility requires that the organization can respond consistently and rapid to unforeseen challenges. Therefore, it must have a simple configuration.

When the organization is confronted with hostility, it cannot be a machine bureaucracy. A machine bureaucracy cannot act appropriately when unexpected events occur.

## **Organizational Characteristics**

The recommended degree of organizational complexity is low (cf 68).

Not much is known about the environment since both the environmental uncertainty and the environmental equivocality of CND are high. In this situation, the organizational complexity should be low. This allows the organization to adapt quickly. When the environmental hostility of CND is high, organizational complexity should be low.

The recommended degree of horizontal differentiation is low (cf 68).

The recommended degree of vertical differentiation is low (cf 84).

The recommended degree of formalization is low (cf 68).

Since the set of variables in the environment that will be important is not known and since it is not possible to predict what will happen, no efficient rules and procedures can be developed, which implies that CND's formalization should be low. When environmental hostility is high formalization should be low.

The recommended degree of centralization is high (cf 77).

There is evidence against it should be: low (cf -17).

CND is of medium size. Such organizations should have medium to high centralization. When the environment is extremely hostile, top management must take prompt action and centralization must be high. Because CND has an advanced information system, centralization can be greater than it could otherwise. An internal process climate in the organization requires a medium to high level of centralization.

CND's span of control should be moderate (cf 62).

Since CND has some technology routineness, it should have a moderate span of control.

CND should use media with high media richness (cf 70).

The information media that CND uses should provide a large amount of information (cf 70).

Incentives should be based on results (cf 70).

CND should use meetings as means for coordination and control (cf 85).

It should also use planning (cf 75).

It should also use rules (cf 75).

When the environment of CND has high equivocality, high uncertainty, and high complexity, coordination and control should be obtained through integrators and group meetings. The richness of the media should be high with a large amount of information. Incentives must be results based. Top management should play the central role in coordinating and controlling the activities of the organization as well as making strategic and operating decisions.

Top management should make many decisions. However, many individuals should be involved in gathering information and implementing those decisions.

## **Organizational Misfits**

Organizational misfits compares the recommended organization with the current organization.

The following organizational misfits are present: (cf 100).

Current and prescribed configuration do not match.

Current and prescribed complexity do not match.

Current and prescribed centralization do not match.

Current and prescribed formalization do not match.

## More Detailed Recommendations

There are a number of more detailed recommendations (cf 100).

You may consider decreasing the number of positions for which job descriptions are available.

You may consider supervising the employees less closely.

You may consider allowing employees more latitude from standards.

You may consider fewer written job descriptions.

Managerial employees may be asked to pay less attention to written instructions and procedures.

You may give supervisors and middle managers fewer rules and procedures.

You may consider having fewer rules and procedures put in writing.

Top management may consider gathering the information needed for decision making themselves.

Top management may interpret and analyze more information itself.

Top management may control the execution of decisions more actively.

The middle managers may be given less discretion over evaluations.

You may give middle managers less discretion on hiring and firing personnel.

## APPENDIX C

### Complex and Simple Case Detailed Variables

*Table 1C.*

Categories	Variables	Current Case	Proposed case- Complex Environment	Proposed case- Simple environment
<b>Organizational Configurations</b>		Machine bureaucracy	Simple configuration	Functional Form
<b>Organizational Complexity</b>	Job Titles	Large Number	Very Few	Large Number
	Vertical Levels	3-5	1-2	1-2
<b>Organizational Formalization</b>	Job descriptions	Opera.employees incl. senior managers	Opera. employees and first line supervisors	Opera. employees excl senior managers
	Employee supervision	Close	Loose	Moderately close
	Latitude from standards	Very Little	Large Amount	A Moderate Amount
	Written instructions	81%-100%	41%-60%	61%-80%
	Written procedures followed	A very great deal	Some	Some
	Free from rules to make a decision	Little	A great deal	A great deal
	Procedures in writing	More than 80%	41%-60%	41%-60%
<b>Current Centralization</b>	Managerial data collection	None	A great deal	None
	Managerial data input interpretation	Less than 20%	More than 80%	Less than 20%
	Control of decision execution	0% to 20%	More than 80%	0% to 20%

*continued on following page*

**Diagnosing Misfits, Inducing Requirements, and Delineating Transformations**

*Table 1C. continued*

	Middle manager budget establishment	None	Little	None
	Discretion in hiring and firing personnel	Great	Some	Great
	Middle Manager exception handling	Great	Some	Great
	New project establishment by Middle Managers	Some	Little	Some
<b>Environment</b>	Environmental Complexity	Complex	Complex	Simple
	Level of Uncertainty	High	High	Low
	Environmental Equivocality	High	High	Low
	Competition	Extreme	Extreme	Low