# Cyberspace and Organizational Structure: An Analysis of the Critical Infrastructure Environment

Michael Quigg, Juan Lopez, Mason Rice, Michael Grimaila, Benjamin Ramsey



Chapter 1

# CYBERSPACE AND ORGANIZATIONAL STRUCTURE: AN ANALYSIS OF THE CRITICAL INFRASTRUCTURE ENVIRONMENT

Michael Quigg, Juan Lopez, Mason Rice, Michael Grimaila and Benjamin Ramsey

**Abstract** Now, more than ever, organizations are being created to protect the cyberspace environment. The ability of cyber organizations tasked to defend critical infrastructure assets has been called into question by numerous cyber security experts. Organizational theory states that organizations should be constructed to fit their operating environments properly. Little research in this area links organizational theory to cyber organizational structure. Because of the cyberspace connection to critical infrastructure assets, the factors that influence the structure of cyber organizations designed to protect these assets warrant analyses to identify opportunities for improvement.

This chapter examines the cyber-connected critical infrastructure environment using organizational structure theories. A multiple case study and content analysis involving 2,856 sampling units were employed to ascertain the level of perceived uncertainty in the environment (measured using the dimensions of complexity, dynamism and munificence). The results indicate that the general external environment of cyber organizations tasked to protect the critical infrastructure is highly uncertain and merits the implementation of organic structuring principles.

**Keywords:** Cyber organizations, structure, critical infrastructure, content analysis

## 1. Introduction

In his book *Blink: The Power of Thinking Without Thinking* [28], Gladwell describes the ability to render accurate expert judgment in situations (e.g., detecting fraudulent art or diagnosing a medical condition) quickly without

collecting and analyzing mass amounts of data. Using techniques described by Gladwell, cyber security experts have declared that governments are not prepared to respond to cyber attacks [5, 11, 14, 38]. These experts inherently know that the response organizations currently in place are ill-prepared to handle crises that may be right around the corner.

The organizations that are supposed to defend against cyber threats (e.g., U.S. Department of Homeland Security and U.S. Cyber Command) may not be able to resist or recover from persistent cyber attacks [38, 60]. This situation is particularly troubling because the National Security Agency Director has stated that several countries, including China and Russia, have the cyber capabilities to disrupt electric utilities in the United States [55]. Without necessarily analyzing the cyber operating environments, experts fully understand that the government has been modeling cyber defense organizations after other government organizations that have hierarchical structures, rigidity and slow to change characteristics. Perhaps, the issues these organizations face are foundational.

Colquitt et al. [17] state that almost everything in organizational behavior starts with structure. If security and resilience in cyberspace are goals, then an analysis of structure should be an initial primary consideration.

The study of organizational structure is largely a discipline within the social sciences. Over the last fifty years, this area of research has grown considerably. Recent theory has advanced significantly from the division of labor analyzed by Adam Smith and Max Weber. It appears that once-stable systems are being rapidly restructured in uncertain emergent global markets characterized by rapid technological changes and tremendous competition. Although numerous organizations are being created, few are examining the organizational research and many are experimenting with disaster [34].

This chapter analyzes organizational structure theory and its connection to cyber organizations in order to understand how to structure organizations and to determine if current structuring attempts are optimal. In particular, the level of uncertainty in the general external environment and its connection to structural types are examined. Traditional government organizations function well in more certain environments (e.g., environments with little change and few disconnected outside influences). However, the same organizations tend to struggle in uncertain environments (e.g., environments with considerable change and numerous interconnected outside influences). This research uses a multiple case study and content analysis to measure the levels of uncertainty (e.g., complexity, dynamism and munificence) in the environments of cyber organizations tasked with critical infrastructure protection. Theory dictates that organizations should be structured to fit their operating environments. The insights provided by this analysis can help structure cyber response organizations to attain the desired fit.

*Table 1.* Structural and contextual dimensions of organizations.

| Type | Dimensions | Traits |
|---|---|---|
| Structural | Specialization; centralization; formalization; span of control; chain of command; personal specialty | How many tasks in a job? Who has the authority to make decisions and where? How standardized and explicit are the rules, policies and procedures? How many people are supervised in a particular group? Who reports to whom up the hierarchy? What is everyone required to know? |
| Contextual | Size; strategy; culture; external and internal environment (competition, hostility, geography); technology | How large are the organization and its sub-units? What choices are being made by leadership? What are the perceived values and beliefs? What is happening in and around the organization that can affect it? What effect does the presence of technology have? |

## 2. Structuring Organizations

When discussing organizational structure, it is helpful to first clarify the meaning of the term. Many people think it is an organizational chart of some sort. However, organizational structure encompasses much more than a mere chart. Theorists commonly describe organizational structure in two dimensions: structural and contextual [18, 52]. These dimensions help explain the forms that organizations take and why they take them. Table 1 presents details about the significant structural and contextual dimensions of organizations.

The structural dimensions include how organizations attempt to control behavior and complete tasks. Contextual dimensions, often called contingencies, are forces that act within and around organizations and affect the structural dimensions. This chapter explores these dimensions to determine their implications with regard to structuring organizations to operate effectively in cyberspace. The following sections review the dominant theoretical principles.

### 2.1 Organizational Structure Theory

The study of the existence of organizations and sustaining their existence has increased dramatically over the last 75 years [51]. The rise and ubiquitous nature of information technology and its effects on organizational structure theory in the social sciences have led to proportionately rapid theoretical developments [47]. Few individuals could foresee how pervasive and influential technological systems would become. The four dominant historical theories

of organizational structure are: (i) institutional; (ii) population ecology; (iii) resource dependence; and (iv) structural contingency.

**Institutional Theory.** Dimaggio and Powell [21] introduced institutional theory (or institutional isomorphism) in 1983. The crux of the theory is that organizations tend to mimic each other in three main ways: (i) coercive; (ii) mimetic; and (iii) normative. In coercive mimicry, organizations have similar structures because they are subjected to similar external environmental pressures (e.g., government oversight). In mimesis, organizations in established fields tend to mimic each other as a bulwark against uncertainty. In normative mimicry, isomorphic processes result from the professionalization of a field accompanied by common training and standards and practices, all of which create homogeneity [21]. It is important to note that institutional isomorphism may not be helpful in the cyber-connected critical infrastructure environment. Observations of cyber structuring in the U.S. Department of Defense indicate the presence of isomorphism. For example, the newly-created cyber forces closely resemble traditional military forces although there are critical differences between the two environments.

**Population Ecology Theory.** The natural selection model is the basis of population ecology. Aldrich and Pfeffer [3] argue that an organization changes as a result of the distribution of resources in its environment. The environment selects the organizational form, which demands a constant sense of adaptation. The list of once-successful organizations that did not adapt to their environments and quickly became obsolete is long. Government cyber organizations can ill afford to be a part of this group. A consistent theme is to develop within the alignment of the environment and the organization. Structural adaptation and flexible structuring are now prominent themes in information technology industries.

**Resource Dependence Theory.** Resource dependence theory argues that organizational survival is determined by acquiring and maintaining resources [51]. Considerable overlap exists between resource dependence and population ecology. However, there are several deviations, for example, in the roles of information processing and strategic choice. Population ecology maintains that strategic choice is possible under certain conditions. However, most organizations are often powerless to make choices due to interorganizational dependencies and information processing challenges [1]. Resource dependence offers that information systems help determine organizational choices and provide critical information [51]. Understanding what constitutes a resource in cyberspace is difficult; however, some general examples are money and people.

**Structural Contingency Theory.** Structural contingency synthesizes the ideas represented in the theories discussed above. The theory declares that the most effective organizational structure is the one that best "fits" the con-

tingencies [24]. Inherent in this definition is that structure should be tailored. Donaldson [23] states that certain factors impact structure. These factors – known as contingency factors – include technology, size, strategy and the environment [23, 49]. Most contingencies are within the internal boundary of an organization, but some are outside the boundary (e.g., in the external environment). Central to contingency theory are numerous empirically-verified results that suggest that organizations that fit the contingencies present in their environments outperform organizations that do not [23]. It is important to note that an organization rarely has to address one contingency and not others, making radical organizational overhauls preferable to prolonged incremental steps [53]. Heuristically, it is also desirable to make changes earlier in the life of an organization than later; this bodes well for cyber organizations because they are in their infancy.

## 2.2 Contingencies

Building on contingency theory, what follows is a brief review of the central contingencies in the research literature and their relevance to cyber environments.

**Technology.** Technology and the change surrounding it increase the perceived uncertainty for organizations [57]. As uncertainty increases so does the pressure to learn and increase knowledge. This pressure for knowledge creates new work roles, workflows and even changes the language used to describe work [57]. The present focus is not on whether organizations will use information technology to accomplish something, but how they accomplish things within and around it. Cyber organizations should keep these principles in mind and be careful not to design structures that are comfortable but inappropriate.

**Size.** The size of an organization considerably affects its type and classification, and nearly everything that defines its structure [49]. For instance, larger organizations are often more complex, have more formalization and survive longer than smaller organizations [7]. Information-technology-rich environments have been shown to reduce organization size as information systems replace middle management and information technology enables other organizations to increase in size without reducing efficiency and innovation [20]. It is important to note that efficiency often does not improve as organizations increase in size [29]. Collyer [16] states that, as project size increases, so does the chance of failure. The likelihood of failure is compounded by increased speed and environmental change. Indeed, consensus appears to be forming that larger organizations should create right-sized sub-units that perform well based on the relevant factors.

**Strategy and Strategic Choice.** The types of strategy that organizations pursue significantly affect their structure [1, 13, 23, 49]. Perhaps most importantly, performance increases when an organization chooses a strategy

that matches its structure to the relevant contingencies [22]. Clearly, cyber organizations should pursue such a strategy.

**Environment.** In line with the population ecology and resource dependence perspectives, organizations that cannot adapt to their environments will not survive [35]. Environmental contingencies are fundamentally important to cyber organizations, especially those that have important security functions. It is helpful to separate the internal environment of an organization from the external environment. This research focuses on the general external environment, which is defined as the relevant physical and social factors outside the organizational boundaries [25]; this external environment affects most organizations in the cyber-connected critical infrastructure domain. Limited research connecting the organizational structure to the cyberspace environment is available. However, research is beginning to emerge on organizational operations in cyber environments. For example, Liu et al. [43] have studied command and control in cyber-physical-social systems. However, their research focuses more on the potential capabilities of cyber-physical-social systems and less on the optimal structural dimensions of systems that operate in cyberspace.

The presence of competition and hostility in an environment can significantly impact an organization. For example, if an organization perceives its environment to be competitive or hostile, it moves toward centralization and formalization [36, 50]. This reaction may be instinctive. However, it can lead to a structure that is ill-suited to meet the challenging characteristics of the environment. This phenomenon is insightful in the light of newly-created government cyber organizations. It appears that centralization and formalization are increasing in these organizations, conceivably to their peril.

Each organizational environment has unique extrinsic factors. These factors influence organizational shape, means and actions within the environment [12]. Uncertainty emerges as a focal point when assessing environmental considerations [12, 25, 41].

## 2.3 Environmental Uncertainty

Complexity, dynamism and munificence are the primary dimensions for conceptualizing the central properties of environments [7, 19, 26] and they act as significant measures of perceived uncertainty in external environments [1, 25, 26]. The three dimensions relate to forces in an environment that can influence and effect organizational change. These forces may be competitors, customers and/or economic, technological, political, ethical, demographic, cultural and social conditions [18, 25, 58]. Note that while complexity, dynamism and munificence are capable of providing an extensive view of the environment, they are not the only determinants of environmental effects on structure [32].

**Complexity.** Complexity relates to the total amount of forces in the environment, whether they connect with each other and the degree to which they can influence other organizations. For example, a weak force in isola-

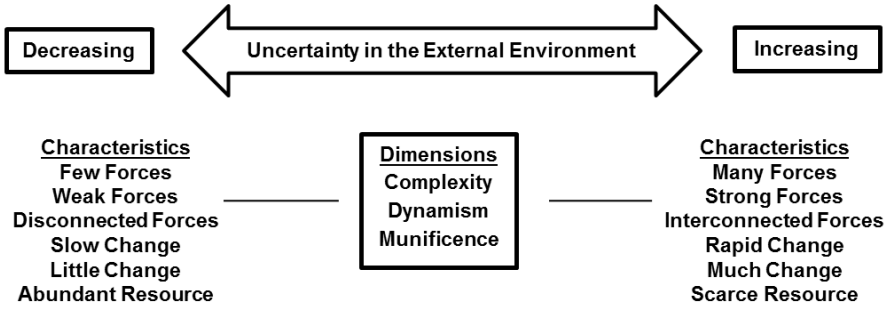


*Figure 1.* External environment and uncertainty.

tion lowers uncertainty, whereas many interconnecting strong forces increase uncertainty [2, 19, 25].

**Dynamism (Turbulence).** Dynamism refers to change measured in speed or quantity. Organizations that face significant amounts of change operate in environments that are more uncertain. Organizations that experience small amounts of change have less uncertainty. An increased rate or speed of change only adds to the uncertainty [2, 19, 25].

**Munificence (Resource).** Munificence deals with capacity, or more generally, the amount of resources available to sustain or support an environment. This category represents a considerable portion of the focus of structural theory. In general, the scarcer the resources, the greater the uncertainty [2, 19, 49].

Figure 1 conceptually depicts complexity, dynamism and munificience as sources of uncertainty in an external environment.

## 2.4 Structures

The mechanistic and organic structural continuum covers the forms that organizations can take [12]. The continuum offers two extremes for management systems based on the level of perceived uncertainty in the environment. Empirical results indicate that perceived environmental uncertainties significantly correlate with mechanistic and organic structural types. Table 2 lists the characteristics of mechanistic and organic structures.

# 3. Mechanistic and Organic Structures

This section discusses mechanistic and organic structures. The U.S. Army characterizes a mechanistic structure. The Apache Indians, Anonymous and Al Qaeda are examples of organic structures.

*Table 2.* Characteristics of mechanistic and organic structures.

| **Mechanistic** | **Organic** |
|---|---|
| Specialized individual tasks | Adjustable team tasks |
| Vertical hierarchy | Flexible (flatter) structure |
| Individual responsibility | Team responsibility |
| Centralized authority | Decentralized authority |
| Increased rules and policies | Decreased formalization |
| Vertical communication | Encircling communication |
| Directives and orders | Advice/information sharing |
| Fixed functional departments | Fluid functional departments |
| Status increases up the hierarchy | Brilliance increases status |
| Narrow span of control | Wide span of control |

*Table 3.* U.S. Army infantry division structure.

| **Dimension** | **Trait** | **Structure** |
|---|---|---|
| Specialization | Highly specialized down to the individual through task lists; highly functional and compartmentalized into sub-units | Mechanistic |
| Centralization | Authority to make decisions is often kept at multiple levels above the worker | Mechanistic |
| Formalization | Highly formalized tasks driven by doctrine, codified and checked frequently; dozens of policies and procedures dictate actions | Mechanistic |
| Span of Control | Doctrinally driven and rigid; often a narrow and vertical hierarchy; difficult to change | Mechanistic |
| Chain of Command | Doctrinally driven and considerably vertical; often with a dozen leaders with authority to change what the lowest individual will do | Mechanistic |
| Professionalism | Varied with deliberate intentions of being high throughout the U.S. Army | Mixed-Organic |
| Status | Increases up the hierarchy | Mechanistic |
| Communication | More vertical than all encompassing; directive and orders based | Mechanistic |

## 3.1 U.S. Army

A U.S. Army infantry division is an organization that displays mechanistic characteristics (Table 3). This particular type of structure is common through-

out the U.S. Army regardless of the environment and context in which it conducts business. Recent combat operations in Iraq are an example. During the initial campaign, U.S. Army divisions were deployed to dominate the environment with mass resources against a singular, weaker and mechanistic adversary. As the war matured and kinetic operations diminished, the U.S. Army found its divisional structure ill-suited to nation building and struggled to find the flexibility to adjust amidst the growing dynamics and complexities (e.g., environmental uncertainty) of the counterinsurgency [4]. This experience highlights the need for flexible organizational modification processes.

## 3.2 Apache Indians, Anonymous and Al Qaeda

The 16th century Apache Indians, the Anonymous hacker group and Al Qaeda are examples of organic structures in a nearly pure form. The three organizations exhibited or exhibit an unusual ability to succeed against vastly larger adversaries. These organizations operated or operate in highly uncertain environments characterized by sudden and vast amounts of change, considerable forces that shift at a moment's notice and limited availability of resources.

The Apache occupied what are now northern Mexico and the southwestern United States for hundreds of years. They increased in fame and notoriety during their conflict with the Spanish Conquistadors in the 16th century. The Spanish appeared to be unstoppable and acquired considerable territory in Central America until they ventured north and encountered the Apache. The Spanish met their match in an undersized and under-resourced adversary [10].

The Anonymous hacker group is similar. It has clashed with Fortune 500 companies, computer security firms and major religious organizations, and brought them great difficulty (at least temporarily) [46].

Al Qaeda has kept powerful militaries busy for nearly fifteen years. They have done this using simple technologies and sneaky tactics to make up for their lack of air support, advanced communications and weaponry.

There is a commonality in the Apache, Anonymous and Al Qaeda organizations as well as in their adversaries. All their adversaries exhibited tendencies to structure and operate in a mechanistic fashion despite external environmental conditions that suggested the opposite. Table 4 presents the structural dimensions of these organic organizations.

## 3.3 Synthesis

As it relates to performance, the greater the perceived uncertainty in the environment, the more an organization should take an organic form; in the presence of less uncertainty, the organization may take a more mechanistic form [12, 30, 41]. When an organization takes an organic form in an environment that is highly uncertain, the resulting structural fit has been shown to increase performance [22]. This alignment is intuitive because an organic structure is both fluid and adaptable. Following the same logic, an organic structure is not as effective in a stable environment. High reliability organizations and

*Table 4.* Apache Indians, Anonymous Hacker Group and Al Qaeda structures.

| Dimension | Trait | Structure |
|---|---|---|
| Specialization | Low level of specialization with operators performing a broad range of random tasks with little standardization; fluid team and network-based task units | Organic |
| Centralization | Personnel follow emergent leaders and often act with autonomy | Organic |
| Formalization | Frequently no formalization is present in the performance of tasks | Organic |
| Span of Control | Emergent and varied; at times extraordinarily wide | Organic |
| Chain of Command | Emergent and flexible based on contingencies facing sub-units; near flat organizational hierarchy with common themes that allow various actors to plug into the organization when needed or desired | Organic |
| Professionalism | Varied | Mixed |
| Status | Increases with displayed brilliance | Organic |
| Communication | Ranges from horizontal to all encompassing; advice and information sharing | Organic |

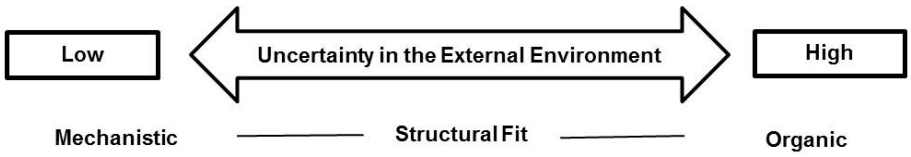


*Figure 2.* Organizational structure, uncertainty and the external environment.

resilience engineering management practices primarily support this view, especially with regard to the critical infrastructure environment [8, 33]. It is worth noting that no single contingency or structure applies to all. Mechanistic and organic structural types are only "better" if they fit the contingencies. Organizational structures and their relationships to environmental uncertainty and structural contingency can be synthesized as shown in Figure 2.

# 4. Research Method

This section describes the research design and methodology chosen to explore uncertainty in the general external environment of a cyber-connected critical infrastructure.

## 4.1 Research Design and Methodology

The research method involved a multiple case study. The approach was structured as an exploratory study with a retrospective lens for organizational patterns. A case study method enables investigators to retain the holistic and meaningful characteristics of real-world events such as individual life cycles and the maturation of industries [61].

The data analysis technique used was content analysis. Content analysis is suitable for condensing many words in a document into a small set of content categories based on explicit coding rules for the purpose of examination [6, 31, 39, 56]. The content categories were established *a priori* based the organizational structure theories of population ecology, resource dependence and structural contingency. The categories were defined iteratively to maximize mutual exclusivity and exhaustiveness [59]. This research highlights external environmental uncertainty for its significance in shaping organizational structure across three measured dimensions: (i) complexity; (ii) dynamism (turbulence); and (iii) munificence (resource) [19].

## 4.2 Data Collection

A stratified purposive sample of published artifacts (documents) provided the context for analysis. The strata (cases) were divided into academia, government and private/practitioner [45, 48]. Each stratum represents stakeholders of publicly-available information related to cyber and critical infrastructure in the United States. Information about cyber linkages to the critical infrastructure is a specific topic of interest where relevant information is known mostly by a particular subset of professionals in the three strata [39]. Search engines (including Google, RAND/CSIS/MITRE and `.gov` sources) identified the artifacts using algorithms that sort documents retrieved from large databases. This process helped identify artifacts with the most references and information about cyber and the critical infrastructure. The U.S. Government Accountability Office definition of artifacts as physically-separable, minimally-sized and self-contained textual information was adopted [31].

**Artifact Discrimination.** Artifacts were retrieved using the terms, "industrial control system," "SCADA" and "critical infrastructure cyber," based on their close linkages to the cyber-connected critical infrastructure [9]. The initial search harvested a large number of artifacts. To further filter the results, additional criteria were applied to obtain a relevant and representative sample for each stratum. Table 5 lists the criteria. The content analyst converted the

*Table 5.* Artifact criteria.

| Category | Criteria |
|---|---|
| Content | Discuss the cyber and critical infrastructure general external environment |
| Geography | U.S. related |
| Timeliness | Published within the last seven years (since July 2008) |
| Availability | Publicly available |
| Size | No more than 20 codeable pages per document |

selected artifacts to the portable document format (PDF) to minimize the file size, standardize the format of all coders and ease the importing of the data into the Maxqda content analysis software.

*Table 6.* Artifact retrieval results.

| Stratum | Initial Sample | Met Criteria | Final |
|---|---|---|---|
| Academia | 91 | 34 | 10 (50%) |
| Government | 65 | 17 | 5 (25%) |
| Private/Practitioner | 73 | 17 | 5 (25%) |
| **Total** | **229** | **68** | **20 (n = 60)** |

Table 6 presents the artifact retrieval results. More academia artifacts were reviewed because of their perceived reliability, validity and trust. A slightly higher amount of private/practitioner artifacts were reviewed than government artifacts due to search engine limitations unique to RAND, CSIS and MITRE. Google's platform dominated because of its ability to return timely results in the focus area (usually within one year of publication). Government artifact selection also suffered from search engine limitations and syntactic issues (e.g., results included only the minutes of congressional meetings), which increased the amount of artifacts that had to be viewed.

Artifacts were randomized using Microsoft Excel to generate the final sample. All 68 artifacts meeting the selection criterion were coded with an A, G or P (academia, government or private/practitioner). The final random sample contained 20 documents per coder (distributed 10-A/5-G/5-P), corresponding to a total of 60 documents. It is important to note that, in content analysis, unlike quantitative statistical analysis, an accurate representation of all the documents in the area of cyber-connected critical infrastructures was not the goal. Instead, the goal was to retrieve a useful set of artifacts to answer the research question fairly [39].

**Parent Organizations.** The documents analyzed by the coders represented a diverse amount of information from all three strata. Parent organizations that published content included in the final sample were the Association

*Table 7.* Code categories.

| **Category** | **Sub-Category** |
|---|---|
| Complexity | Forces interconnecting |
| Complexity | Forces not connecting |
| Complexity | Many forces |
| Complexity | Few forces |
| Complexity | Forces are strong |
| Complexity | Forces are weak |
| Dynamism | Forces change a lot |
| Dynamism | Forces change infrequently |
| Dynamism | Forces change rapidly |
| Dynamism | Forces change slowly |
| Munificence | Resources are scarce |
| Munificence | Resources are abundant |
| Not Applicable | Not Applicable |

for Computing Machinery, Institute of Electrical and Electronics Engineers, International Federation for Information Processing, Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, International Journal of Critical Infrastructure Protection, Forbes, Dow Jones and Company, The Economist, Tripwire, Army Research Laboratory, Government Accountability Office, The White House and the U.S. Department of Homeland Security.

## 4.3 Coding

Krippendorf [39] defines coding as classifying sampling or recording units in terms of the categories of the chosen analytical constructs. The sampling unit selected to categorize the information present in the artifact was "the sentence" [56] because of its ability to obtain meaning in relation to text [39] and due to the availability of human coders [31]. Each sentence was read and coded against the code categories. Coders were trained to look for repetitive material so as not to code the same information twice. The coders were instructed to interpret the sampling unit (e.g., sentence) in the context of an entire artifact (e.g., context unit). This interpretation is both meaningful and feasible for an artifact that contains less than eight pages of codeable material [39].

**Content Categories.** The Maxqda qualitative data analysis software was selected for its ability to manage large volumes of text, display information with ease and work with multiple coders [54]. The Maxqda graphical user interface provided a visual display of code categories and coded material to check operational definitions against sampling units. The Not Applicable code category was included in addition to the existing *a priori* categories of complexity, dynamism and munificence to ensure exhaustiveness [31, 56]. Table 7

lists the code categories. Note that all the forces relate to the general external environment.

**Coder Training.** The content analyst familiarized the coders with Maxqda, operational definitions and code categories. Also, well-defined explicit coding instructions were added to Maxqda to improve coding consistency [56]. Only the content analyst trained and evaluated each coder [39]. The coders participated in a beta coding session to improve coding consistency, tighten definitions and minimize idiosyncratic judgments during the coding process [39]. The training process produced favorable reliability results. The coders trained on qualified documents that were not included in the final sample. Collaboration among coders was not permitted during the coding process. Three graduate students with strong backgrounds in cyber security and cyber operations coded the documents. Note that the familiarity of coders with the phenomena under consideration was a critical factor in coder selection [39]. The reading levels of the documents demanded highly-educated coders.

## 4.4 Validity

Every step of the research process was conducted to ensure high-quality results. The guidelines set forth by Krippendorff [39] for validity in content analysis were followed and reviewed periodically throughout the research process.

## 4.5 Reliability

To ensure valid inferences from the text, word meaning and category definitions were tightened, multiple coders were used and inter-coder agreement was calculated. Cohen's kappa coefficient [15] was used as a measure of reliability. The coefficient is considered to be a strict measure of agreement between coders based on the selection of a particular code for the recording unit [44].

# 5. Results

This section discusses the results and analyzes the linkages between the structural types and environmental dimensions.

## 5.1 Descriptive Statistics

Table 8 shows that the coding units range from 1,594 to 2,067 (mean = 1,838). The primary reason for this variance is the manner in which the coders interpreted the coding units. The ambiguity of the language in the published material may have caused one coder to perceive the presence of a coding unit whereas another coder did not.

Table 9 shows that each coder read 156 pages averaging 7.8 pages per artifact. Although there were more academia artifacts than government artifacts, the government artifacts averaged more pages (13.8). Also, the difficulty of in-

*Table 8.* Total codes by coder.

| | Coder | | |
|---|---|---|---|
| | **1** | **2** | **3** |
| Pages | 156 | 156 | 156 |
| Documents | 20 | 20 | 20 |
| Coding Units | 2,067 | 1,853 | 1,594 |

*Table 9.* Pages coded by stratum.

| | **Academia** | **Govt.** | **Private/ Practitioner** | **Aggregate** |
|---|---|---|---|---|
| Pages Read | 74 | 69 | 13 | 156 |
| Pages per Artifact | 7.4 | 13.8 | 2.6 | 7.8 |

terpreting the sampling unit (sentence) in relation to the context unit (artifact) increased for the coders [39].

*Table 10.* Flesch-Kincaid reading scores.

| **Stratum** | **Reading Level** | **Reading Ease** |
|---|---|---|
| Academia | 16 | 24 |
| Government | 17 | 15 |
| Private/Practitioner | 16 | 27 |
| **Total Average** | **16** | **23** |

Flesch-Kincaid reading level and Flesch reading ease measures were computed for each artifact. Table 10 presents the results. The Flesch-Kincaid formulas account for the number of words per sentence and syllables per word to generate a grade-level guide of comprehension and ease of reading [27, 37]. A reading ease below 30 is associated with college graduates. A total of 156 pages were coded, with an average of 1,838 recordable units at a graduate reading level and ease (Flesch-Kincaid Grade 16/Ease 23). The government documents emerged as the most difficult to comprehend based on these indices and they suffered from the highest amount of disagreement.

## 5.2 Inter-Coder Agreement

The coder agreement scale used in Table 11, which is based on the work of Landis and Koch [40], ranges from fair (21%-40%) to substantial (61%-80%). This results in moderate overall agreement with the kappa coefficient that ranges from 51% to 60% in Table 11. Since the research was exploratory, lower levels of agreement are acceptable [44]. Coders were allowed considerable

*Table 11.* Cohen's kappa coefficients.

| | Coders | | | |
|---|---|---|---|---|
| | **1 and 2** | **1 and 3** | **2 and 3** | **Mean** |
| Academia | 0.66 | 0.71 | 0.71 | 0.69 |
| Government | 0.39 | 0.47 | 0.29 | 0.38 |
| Private/Practitioner | 0.36 | 0.51 | 0.31 | 0.40 |
| **Kappa** | **0.52** | **0.60** | **0.51** | **0.54** |

latitude in content interpretation based on their expertise and training. Despite the challenges, the results indicate agreement between coders.

*Table 12.* Frequency analysis of codes.

| **Category** | **Code** | **Freq.** | **%** | **Docs.** |
|---|---|---|---|---|
| Complexity | Forces connecting | 872 | 30.53 | 56 |
| Complexity | Many forces | 537 | 18.80 | 55 |
| Complexity | Forces are strong | 517 | 18.10 | 58 |
| Munificence | Resources are abundant | 225 | 7.88 | 36 |
| Munificence | Resources are scarce | 167 | 5.85 | 44 |
| Dynamism | Amount of change is high | 144 | 5.04 | 44 |
| Complexity | Forces are not connecting | 140 | 4.90 | 32 |
| Dynamism | Forces change rapidly | 88 | 3.08 | 25 |
| Dynamism | Forces change slowly | 65 | 2.28 | 20 |
| Complexity | Forces are weak | 57 | 2.00 | 29 |
| Dynamism | Amount of change is low | 34 | 1.19 | 11 |
| Complexity | Few forces | 10 | 0.35 | 8 |
| | **Total** | **2,856** | **100.00** | – |

## 5.3 Code Distribution

Table 12 presents the frequency distributions of codes across the entire sample (n = 60). The coders recognized and assigned a code to 51.8% of the content. The Not Applicable category was eliminated to remove bias. Frequency analysis indicates that complexity has a strong presence (more than 91%) in each stratum. Complexity (e.g., forces connecting, many forces and forces are strong) accounts for 67.43% of the uncertainty in the content coded. Dynamism (e.g., amount of change is high and forces change rapidly) accounts for 8.12% of the uncertainty in the content coded. Munificence (e.g., resources are scarce) accounts for 5.85% of the uncertainty in the content coded. Based on coder interpretation, as Figure 3 indicates, there is a strong presence of uncertainty (81.4%) in the general external environment across the three sampled strata.

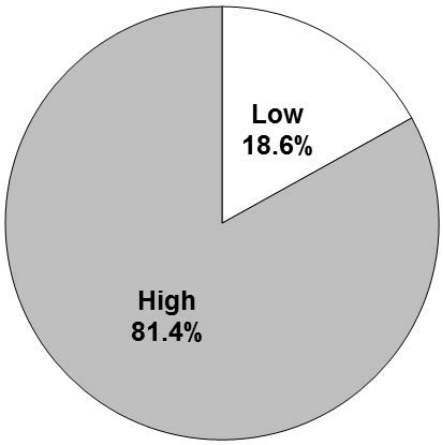


*Figure 3.* Uncertainty in the general external environment.

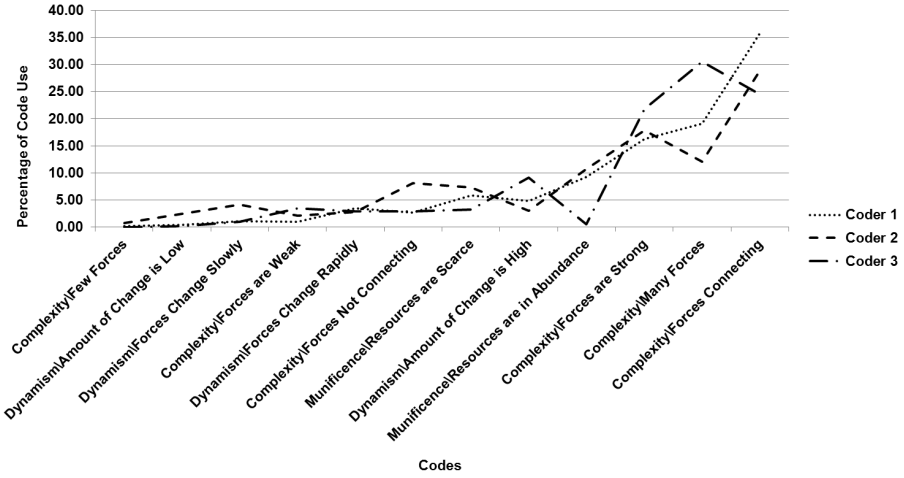


*Figure 4.* Coder overlap.

## 5.4 Coder Analysis

Figure 4 clearly demonstrates that the coders were consistent in their coding across all three dimensions of uncertainty. While there is slight disagreement in complexity (amount/connectedness of forces) and munificence (resource), there is general agreement overall.

## 5.5 Strata Analysis

This section provides an analysis of the presence of uncertainty in the general external environment within and across strata.

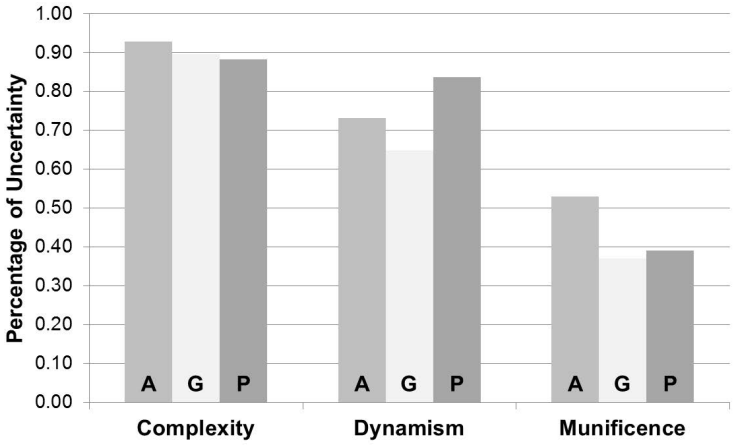


*Figure 5.* Percentage of uncertainty by dimension and stratum.

**Complexity.** Figure 5 compares the percentage of uncertainty by dimension and stratum. The figure demonstrates that there is strong evidence to support that the complexity is extremely high. All three strata show a strong presence of complexity in the general external environment. In fact, the data appears to be a statistical dead heat at about 90%.

**Dynamism.** Dynamism presents a different picture. The private/practitioner stratum displays significantly higher uncertainty than the academia and government strata. This level of uncertainty appears to be reasonable because of the increased competition and desire for revenue present in the private/practitioner environment. The environment requires the ability to dissolve or create organizations rapidly, modify processes and innovate in response to market stimuli.

The government stratum exhibits a lower presence of uncertainty. Unlike private/practitioner functions, government functions are slow to change. Despite this, the coders agreed that there was vastly more change (dynamism) in the general external environment across all three strata. In fact, the amount of change was detected at four times the frequency (see Table 12).

**Munificence.** The results clearly demonstrate that there is explanatory power and a measurable degree of munificence (resource scarcity). The presence of uncertainty is lower overall across all three environmental resource measures. However, academia exhibits significantly more perceived resource scarcity in the general external environment. A reasonable explanation for the difference is the breadth and depth of research that academia conducts in this complex area.

## 5.6 Recommendations

Based on the outcomes of this study, it would be logical to structure government cyber organizations that operate in the critical infrastructure environment in an organic fashion rather than in the current mechanistic manner. Because of the complexity and dynamism of the environment, the government should generate separate processes when creating these organizations to facilitate rapid implementation and frequent modifications. Specifically, government cyber organizations should have the following characteristics if they are to succeed:

- People should not only perform highly specialized tasks; they should also have broader views.
- A chain of command should exist, but it should be more decentralized to accommodate shifting responsibilities.
- The high level of complexity and change in the environment warrant knowledgeable personnel working in teams and coordinating frequently to make rapid decisions when needed.
- Communications should occur often and at many levels.
- Orders and directives should diminish as advice and information sharing increase.
- Knowledge and expertise should increase individual status.

An appealing aspect of this research is the potential for generalization to other cyber organizations that operate in the United States and in other developed countries. An argument could be made that there are few significant differences in the cyber environments of the U.S. Department of Homeland Security, U.S. Department of Defense, private utilities and high technology firms.

# 6. Conclusions

Few topics have more national security import than understanding how to organize in cyberspace and protect critical infrastructure assets from cyber threats. The United States Army Cyber Talks at the National Defense University in September 2015 recognized the need for empirical analysis and evidence that could enhance organizational structuring decisions and adjustments. Innovation and knowledge management were strong concerns of the attendees that related directly to organizational structure [42]. In fact, the attendees repeatedly discussed several structural dimensions as inhibitors to performance, further validating the need for this research.

As it pertains to the cyber-connected critical infrastructure environment, forces within and across strata are numerous, strong and connecting. The amount of change at present is very high. The speed of change is rapid and resources are typified by an abundance of information technology with low barriers to entry. Cyberspace is ubiquitous, which creates opportunities for malicious

actors. These elements create the perception of highly uncertain situations for organizations operating in the cyber-connected critical infrastructure environment. Organic structuring principles facilitate the adaptability and flexibility needed to operate effectively in this environment. Indeed, the research results demonstrate that the general external environment is decidedly uncertain, indicating that organizations should follow organic structuring principles when operating in the cyber-connected critical infrastructure environment.

Note that the views expressed in this chapter are those of the authors and do not reflect the official policy or position of the U.S. Air Force, U.S. Army, U.S. Department of Defense or U.S. Government.

## References

[1] H. Aldrich, *Organizations and Environments*, Stanford University Press, Stanford, California, 2008.

[2] H. Aldrich and D. Herker, Boundary spanning roles and organization structure, *Academy of Management Review*, vol. 2(2), pp. 217–230, 1977.

[3] H. Aldrich and J. Pfeffer, Environments of organizations, *Annual Review of Sociology*, vol. 2, pp. 79–105, 1976.

[4] T. Barnett, *Blueprint for Action: A Future Worth Creating*, Berkley Publishing Group, New York, 2005.

[5] C. Bennett, U.S. not prepared for cyberattacks, ex-NSA chief warns, *The Hill*, November 14, 2014.

[6] B. Berelson, *Content Analysis in Communication Research*, Free Press, Glencoe, Illinois, 1952.

[7] A. Bluedorn, Pilgrim's progress: Trends and convergence in research on organizational size and environments, *Journal of Management*, vol. 19(2), pp. 163–191, 1993.

[8] A. Boin and M. van Eeten, The resilient organization, *Public Management Review*, vol. 15(3), pp. 429–445, 2013.

[9] S. Boyer, *SCADA: Supervisory Control and Data Acquisition*, Instrumentation, Systems and Automation Society, Research Triangle Park, North Carolina, 2010.

[10] O. Brafman and R. Beckstrom, *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations*, Penguin, New York, 2006.

[11] E. Bumiller and T. Shanker, Panetta warns of dire threat of cyberattack on U.S., *New York Times*, October 11, 2012.

[12] T. Burns and G. Stalker, *The Management of Innovation*, Tavistock, London, United Kingdom, 1961.

[13] J. Child, Organizational structure, environment and performance: The role of strategic choice, *Sociology*, vol. 6(1), pp. 1–22, 1972.

[14] R. Clarke and R. Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, HarperCollins Publishers, New York, 2010.

[15] J. Cohen, A coefficient of agreement for nominal scales, *Educational and Psychological Measurement*, vol. 20(1), pp. 37–46, 1960.

[16] S. Collyer and C. Warren, Project management approaches for dynamic environments, *International Journal of Project Management*, vol. 27(4), pp. 355–364, 2009.

[17] J. Colquitt, J. LePine and M. Wesson, *Organizational Behavior: Improving Performance and Commitment in the Workplace*, McGraw-Hill, New York, 2014.

[18] R. Daft, J. Sormunen and D. Parks, Chief executive scanning, environmental characteristics and company performance: An empirical study, *Strategic Management Journal*, vol. 9(2), pp. 123–139, 1988.

[19] G. Dess and D. Beard, Dimensions of organizational task environments, *Administrative Science Quarterly*, vol. 29(1), pp. 52–73, 1984.

[20] T. Dewett and G. Jones, The role of information technology in the organization: A review, model and assessment, *Journal of Management*, vol. 27(3), pp. 313–346, 2001.

[21] P. DiMaggio and W. Powell, The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields, *American Sociological Review*, vol. 48(2), pp. 147–160, 1983.

[22] L. Donaldson, Strategy and structural adjustment to regain fit and performance: In defense of contingency theory, *Journal of Management Studies*, vol. 24(1), pp. 1–24, 1987.

[23] L. Donaldson, The normal science of structural contingency theory, in *Studying Organizations: Theory and Method*, S. Clegg and C. Hardy (Eds.), Sage Publications, London, United Kingdom, pp. 51–70, 1999.

[24] L. Donaldson, The contingency theory of organizational design: Challenges and opportunities, in *Organization Design*, R. Burton, B. Eriksen, D. Hakonsson and C. Snow (Eds.), Springer, New York, pp. 19–40, 2006.

[25] R. Duncan, Characteristics of organizational environments and perceived environmental uncertainty, *Administrative Science Quarterly*, vol. 17(3), pp. 313–327, 1972.

[26] P. Fiss, Building better causal theories: A fuzzy set approach to typologies in organization research, *Academy of Management Journal*, vol. 54(2), pp. 393–420, 2011.

[27] R. Flesch, *How to Write Plain English: A Book for Lawyers and Consumers*, HarperCollins Publishers, New York, 1979.

[28] M. Gladwell, *Blink: The Power of Thinking Without Thinking*, Back Bay Books, New York, 2007.

[29] R. Gooding and J. Wagner, A meta-analytic review of the relationship between size and performance: The productivity and efficiency of organizations and their sub-units, *Administrative Science Quarterly*, vol. 30(4), pp. 462–481, 1985.

[30] L. Gordon and V. Narayanan, Management accounting systems, perceived environmental uncertainty and organization structure: An empirical investigation, *Accounting, Organizations and Society*, vol. 9(1), pp. 33–47, 1984.

[31] Government Accountability Office, Content Analysis: A Methodology for Structuring and Analyzing Written Material, GAO/PEMD-10.3.1, Washington, DC, 1996.

[32] R. Harris, Organizational task environments: An evaluation of convergent and discriminant validity, *Journal of Management Studies*, vol. 41(5), pp. 857–882, 2004.

[33] E. Hollnagel, D. Woods and N. Leveson, *Resilience Engineering: Concepts and Precepts*, Ashgate Publishing, Burlington, Vermont, 2006.

[34] A. Ilinitch, R. D'Aveni and A. Lewin, New organizational forms and strategies for managing in hypercompetitive environments, *Organization Science*, vol. 7(3), pp. 211–220, 1996.

[35] D. Jacobs, Dependency and vulnerability: An exchange approach to the control of organizations, *Administrative Science Quarterly*, vol. 19(1), pp. 45–59, 1974.

[36] P. Khandwalla, Environment and its impact on the organization, *International Studies of Management and Organization*, vol. 2(3), pp. 297–313, 1972.

[37] J. Kincaid, R. Fishburne, R. Rogers and B. Chissom, Derivation of New Readability Formulas (Automated Readability Index, Fog Count and Flesch Reading Ease Formula) for Navy Enlisted Personnel, Research Branch Report 8-75, Chief of Naval Technical Training Command, Naval Air Station Memphis, Millington, Tennessee, 1975.

[38] T. Koppel, *Lights Out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath*, Crown Publishers, New York, 2015.

[39] K. Krippendorff, *Content Analysis: An Introduction to its Methodology*, Sage Publications, Thousand Oaks, California, 2013.

[40] J. Landis and G. Koch, The measurement of observer agreement for categorical data, *Biometrics*, vol. 33(1), pp. 159–174, 1977.

[41] P. Lawrence and J. Lorsch, Differentiation and integration in complex organizations, *Administrative Science Quarterly*, vol. 12(1), pp. 1–47, 1967.

[42] C. Liao, S. Chuang and P. To, How knowledge management mediates the relationship between environment and organizational structure, *Journal of Business Research*, vol. 64(7), pp. 728–736, 2011.

[43] Z. Liu, D. Yang, D. Wen, W. Zhang and W. Mao, Cyber-physical-social systems for command and control, *IEEE Intelligent Systems*, vol. 26(4), pp. 92–96, 2011.

[44] M. Lombard, J. Snyder-Duch and C. Campanella Bracken, Content analysis in mass communication: Assessment and reporting of inter-coder reliability, *Human Communication Research*, vol. 28(4), pp. 587–604, 2002.

[45] C. Okoli and S. Pawlowski, The Delphi method as a research tool: An example, design considerations and applications, *Information and Management*, vol. 42(1), pp. 15–29, 2004.

[46] P. Olson, *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous and the Global Cyber Insurgency*, Back Bay Books, New York, 2013.

[47] W. Orlikowski, The duality of technology: Rethinking the concept of technology in organizations, *Organization Science*, vol. 3(3), pp. 398–427, 1992.

[48] M. Patten, *Understanding Research Methods: An Overview of the Essentials*, Pyrczak Publishing, Glendale, California, 2009.

[49] J. Pfeffer, *Organizations and Organization Theory*, Pitman, Boston, Massachusetts, 1982.

[50] J. Pfeffer and H. Leblebici, The effect of competition on some dimensions of organizational structure, *Social Forces*, vol. 52(2), pp. 268–279, 1973.

[51] J. Pfeffer and G. Salancik, *The External Control of Organizations: A Resource Dependence Approach*, Stanford University Press, Stanford, California, 2003.

[52] D. Pugh, The measurement of organization structures: Does context determine form? *Organizational Dynamics*, vol. 1(4), pp. 19–34, 1973.

[53] J. Qiu, L. Donaldson and B. Luo, The benefits of persisting with paradigms in organizational research, *Academy of Management Perspectives*, vol. 26(1), pp. 93–104, 2012.

[54] M. Savin-Baden and C. Howell Major, *Qualitative Research: The Essential Guide to Theory and Practice*, Routledge, Abingdon, United Kingdom, 2012.

[55] G. Seffers, Cyber commander expects damaging critical infrastructure attack, *Signal*, December 1, 2014.

[56] S. Stemler, An overview of content analysis, *Practical Assessment, Research and Evaluation*, vol. 7(17), 2001.

[57] M. Tushman and R. Nelson, Introduction: Technology, organizations and innovation, *Administrative Science Quarterly*, vol. 35(1), pp. 1–8, 1990.

[58] A. van de Ven and D. Ferry, *Measuring and Assessing Organizations*, John Wiley and Sons, New York, 1980.

[59] R. Weber, *Basic Content Analysis*, Sage Publications, Newbury Park, California, 1990.

[60] S. Worrall, Is the United States prepared for a massive cyberattack? *National Geographic*, Washington, DC, November 8, 2015.

[61] R. Yin, *Case Study Research Design and Methods*, Sage Publications, Thousand Oaks, California, 2014.