3-24-2016

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

Michael D. Quigg II


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

THESIS

Michael D. Quigg II, Captain, USA

AFIT-ENV-MS-16-M-177

**DEPARTMENT OF THE AIR FORCE**
**AIR UNIVERSITY**

**AIR FORCE INSTITUTE OF TECHNOLOGY**

**Wright-Patterson Air Force Base, Ohio**

AFIT-ENV-MS-16-M-177

# CYBERSPACE AND ORGANIZATIONAL STRUCTURE:

# AN ANALYSIS OF THE CRITICAL INFRASTRUCTURE ENVIRONMENT

THESIS

Presented to the Faculty

Department of Systems Engineering and Management

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Engineering Management

Michael D. Quigg II, BBA

Captain, USA

March 2016

AFIT-ENV-MS-16-M-177

# CYBERSPACE AND ORGANIZATIONAL STRUCTURE:

# AN ANALYSIS OF THE CRITICAL INFRASTRUCTURE ENVIRONMENT

Michael D. Quigg II, BBA

Captain, USA

Committee Membership:

LTC Mason Rice, PhD
Chair

Michael R. Grimaila, PhD, CISM, CISSP
Member

Maj Benjamin Ramsey, PhD
Member

## Abstract

Now more than ever, organizations are being created to protect the cyberspace environment. The capability of cyber organizations tasked to defend critical infrastructure has been called into question by numerous cybersecurity experts. Organizational theory states that organizations should be constructed to fit their operating environment properly. Little research in this area links existing 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 analysis to identify opportunities for improvement.

This thesis analyzes the cyber-connected critical infrastructure environment using the dominant organizational structure theories. By using multiple case study and content analysis, 2,856 sampling units are analyzed to ascertain the level of perceived uncertainty in the environment (complexity, dynamism, and munificence). The results indicate that the general external environment of cyber organizations tasked to protect critical infrastructure is highly uncertain thereby meriting implementation of organic structuring principles.

*To my Savior Jesus Christ, the source of everything good in my life; mom and dad; my wife for modeling Christ's love while raising the girls.*

## Acknowledgments

I would like to thank LTC Mason Rice for joyfully accepting me as a research pupil and for guiding me with passion, creativity, and kindness; Juan Lopez for being the personification of mentorship, professionalism, and excellence during my research; Dr. Grimaila for your wisdom throughout and for nurturing an idea into a thesis; Dr. Ramsey for the time, attention, and level of detail you gave to making this a work I can truly take joy in. I am also indebted to the Department of Homeland Security for funding this research.

Finally, thank you to MAJ Derek Young, Stephen Dunlap, and CPT Jungsang Yoon for your incredible selflessness in support of this research.

Michael D. Quigg II

**Table of Contents**

Page

Page

## List of Figures

## List of Tables

CYBERSPACE AND ORGANIZATIONAL STRUCTURE:

AN ANALYSIS OF THE CRITICAL INFRASTRUCTURE ENVIRONMENT

# I. Introduction

## Operational Motivation

In his book *Blink*, Gladwell [27] 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. Experts in cyber security, using techniques described by Gladwell, have declared that governments are not prepared to respond to cyber-attacks [5, 10, 13, 36]. These experts, understanding critical infrastructure cyber security, inherently know that response organizations currently in place are ill-fit to handle a crisis that may be right around the corner.

The organizations that are supposed to defend against these threats (e.g., Department of Homeland Security and U.S. Cyber Command) may not be able to resist or recover from a persistent cyber-attack [36, 59]. This situation is particularly troubling because the National Security Agency's Director stated that several countries, including China and Russia, have the cyber capabilities to disrupt electrical utilities throughout the United States [53]. Without necessarily analyzing the cyber operating environment, experts fully understand the government is modeling current cyber defense organizations after practically every other

government organization (e.g., rigid, slow to change, and hierarchical). Perhaps the issues these organizations face are foundational.

As Colquitt, Lepine and Wesson state, almost everything in organizational behavior starts with structure [16]. If security and resilience in cyberspace are a goal, then an analysis of structure should be an initial primary consideration.

The study of organizational structure is largely a discipline within the social sciences and championed by organizational structure theorists. 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 now rapidly restructuring in uncertain emergent global markets, marked by rapid technological change and tremendous competition.

Personal observations while assigned to the headquarters staff for an Army organization tasked with creating a new cyber unit were enlightening. Numerous leaders worked furiously to find out the best way to accomplish the task. Time was limited. The pressure to be ready to defend the network was great. Attacks on military networks were growing by the day. This situation did not allow for slow and deliberate theoretical analysis. Rather, it created a cyber-organization solution whose future effectiveness was in question.

Situations like this one are happening everywhere there is a need to defend critical cyber assets. The urgency of the circumstance creates the need for

immediate action. The pervasiveness of information technology and societies increasing dependence on cyber is not likely to resolve quickly. Indeed a couple of decades ago Ilinitch, D'Aveni and Lewin claimed about this new environment, "Although numerous organizations are being created, few are examining the organizational research and many are experimenting with disaster" [32]. This thesis seeks to fill the gap in the literature to address this critical issue.

## Research Questions

This thesis analyzes relevant organizational structure theory and its connection to cyber organizations to answer the following research questions:

1. What is organizational structure?
2. What theories contribute to organizational structure?
3. How should organizations structure in cyber environments?

## Methodology

The research approach is qualitative, pragmatic, and exploratory in nature, using multiple case study and content analysis. The environment of cyber-connected critical infrastructure, defined as critical infrastructure that connects to cyberspace (primarily the internet), will be evaluated from the perspective of the academic, governmental and private/practitioner communities. Documents provide the information for analysis. Content analysis categorizes and quantifies the level of uncertainty in the environment.

## Limitations

Limitations ranged from software functionality to method selection. Significant software limitations included the lack of flexibility in software modification, and user licenses requiring each coder to have their copy of the software. The researcher limited the cases to the cyber-connected critical infrastructure environment (though the nature of cyber closely links this research with other cyber environments), and the search engines to eight sources. Documentation, provided by the search engines for the data set, were (in some cases) limited; not all information on the cyber-connected critical infrastructure environment is available and some required subscriptions. The availability of personnel with knowledge of the phenomena, the appropriate reading level, and coding expertise was limited. Human coding suffered natural limitations from the ambiguity of word meaning to fatigue. The multiple case study approach with multiple strata was used to overcome data triangulation (multiple data collection techniques, e.g., surveys, interviews). This research used appropriate techniques to mitigate these limitations and others (e.g., rest, training)

## Implications

Theory dictates that organizations should structure to fit their operating environment. The insights of this analysis should help strategic cyber leaders, particularly those tasked to protect critical infrastructure, understand critical

aspects of the environment. The connections made between structure and environment will aid in structuring more effective cyber response organizations.

## II. Literature Review

### Structuring Organizations

When discussing organizational structure, it is helpful to define the meaning of "organizational structure." Many people, when hearing organizational structure, will conjure up a picture of an organizational chart of some sort. However, organizational structure encompasses far more than a chart. Organizational structure commonly breaks into two dimensions: structural and contextual [17, 50]. These dimensions help explain the forms organizations take and why they take them. The structural dimensions include how organizations attempt to control behavior and complete tasks. Contextual dimensions, often called contingencies, are forces acting within and outside the organization, which affect the structural dimensions. Table 1 displays some of the significant structural and contextual dimensions.

**Table 1. Structural 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. | What size is the organization and its subunits; what choices are being made by leadership; perceived values and beliefs; what is happening in and around the organization which can affect it; the presence and effects of technology. |

This thesis will explore these dimensions to determine their implication for structuring organizations to operate in cyberspace. What follows is a review of the dominant theoretical principles.

## Organizational Structure Theory

The study of the existence of organizations and how to sustain that existence has increased dramatically in the last 75 years [49]. The rise and ubiquitous nature of information technology and its effects on organizational structure theory in the social sciences have led to proportionately rapid theory development [45]. Few could foresee the universality and importance of technological systems. The four

dominant, historical theories on organizational structure are (i) institutional, (ii) resource dependence, (iii) population ecology, and (iv) structural contingency.

***Institutional Theory.***

Dimaggio and Powell introduced institutional theory (or institutional isomorphism) in 1983. The crux of this theory can be summed up rather simply – organizations tend to mimic each other [20]. Dimaggio and Powell point to three main types of isomorphism, which are coercive, mimetic and normative. Coercion explains how organizations often result in similar structures because of similar external environmental pressures (e.g., government oversight). Mimetic explains how organizations in established fields tend to mimic each other as a bulwark against uncertainty. Normative isomorphic processes result from the professionalization of a field accompanied by common training, standards and practices, which create homogeneity [20]. It is important to note, that in the cyber-connected critical infrastructure environment, institutional isomorphism may not be helpful. Observation of government cyber structuring in the U.S. Department of Defense indicates the presence of isomorphism. For example, newly created cyber forces closely resemble traditional military forces, even though there are critical differences in the environments of each.

***Resource Dependence Theory.***

Resource dependence theory argues organizational survival be about acquiring and maintaining resources [49]. There is considerable overlap between

resource dependence and population ecology. However, there are several deviations; some examples are in the roles of information processing and strategic choice. Population ecology argues that, given certain conditions, strategic choice is possible. However, most organizations are often powerless to choose because of inter-organizational dependencies and information processing issues [1]. Resource dependence counters by offering that information systems determine organizational choice and provide critical information [49]. Understanding what constitutes a resource in cyber is difficult. However, some general examples include money and people.

***Population Ecology Theory.***

Population ecology offers explanations based on the natural selection model. Aldrich and Pfeffer argue in the *Environment of Organizations* that organizations change because of the distribution of resources in the organization's environment [3]. The environment selects the organizational form, which demands a constant sense of adaptation. The list of once successful organizations that did not adapt to the environment and quickly found themselves obsolete is long. Government cyber organizations can ill afford to be a part of this group. A consistent theme is developing in the alignment of the environment and the organization. Structural adaptation and flexible structuring in high information technology industries are now prominent.

### *Structural Contingency Theory.*

This theory offers a potential synthesis of ideas represented in the theories above. Structural contingency theory declares the most effective organizational structure is the one which best "fits" the contingencies [22]. Inherent in this definition is that structure should be tailored. Donaldson [23] states that certain factors influence structure. These factors (known as contingency factors) include technology, size, strategy and the environment [23, 47]. Most contingencies involve the internal boundary of the organization, but some of the most critical are outside of that boundary (e.g., the external environment). Contingency theory offers several empirically verified results that show organizations that fit the contingencies present in the environment outperform those who do not [23]. It is important to note that rarely does an organization have to address one contingency and not others, making radical organizational overhauls preferable to prolonged incremental steps [51]. Heuristically, it is also desirable to make these changes earlier in the life of an organization than later, which bodes well for cyber organizations, as they are in their infancy.

## Contingencies

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

***Technology.***

Technology and the change surrounding it increase perceived uncertainty for organizations [55]. 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 [55]. The focus is not whether organizations will use information technology to accomplish something, but how they will 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.***

Size considerably affects the type and classification of an organization [47]. Organizational size has been found to affect nearly everything that defines organizational structure. 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 allow other organizations to increase in size without decreasing efficiency and innovativeness [19]. It is important to note that efficiency has not been shown to improve as organizational size increases [28]. Collyer [15] states that as the size of the project increases so does the chance of failure. The likelihood of that failure is compounded by increased speed and quantity of change in the environment. The consensus

appears to be forming wherein larger organizations form right-sized subunits that perform well when based on the relevant factors.

***Strategy and Strategic Choice.***

The type of strategy an organization pursues significantly affects the structure of organizations [1, 12, 23, 47]. Perhaps most importantly, when organizations choose a strategy to match structure to the relevant contingencies, performance increases [21]. This is a strategy cyber organizations should pursue.

***Environment.***

In line with the population ecology and resource dependence perspectives, organizations that cannot adapt to their environment cannot survive [33]. Environmental contingencies are fundamentally important to organizations. They are of particular importance to cyber organizations, which have a principal security function. It is helpful to separate the internal environment of organizations from the external environment of organizations. This research will exclusively focus on the general external environment, here defined as the relevant physical and social factors outside the boundaries of an organization [24] which generally effect all within the cyber-connected critical infrastructure area. Limited research connecting organizational structure to the cyberspace environment is available. However, research is beginning to emerge on organizational operations in a cyber-environment. For example, Liu et al., [41] have addressed command and control in cyber-physical-social systems (CPSS). However, Liu's research focuses far more on

the potential capabilities of CPSS and far less on optimal structural dimensions for those operating in cyberspace.

The presence of competition and hostility in the environment can significantly affect organizations. For example, if an organization perceives their environment to be hostile or competitive, it will move toward centralization and formalization [34, 48]. 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 light of newly created government cyber organizations. It appears 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 [11]. In assessing environmental considerations, uncertainty emerges as a focal point [11, 24, 39].

**Environmental Uncertainty**

Dynamism, complexity and munificence remain the primary dimensions used to conceptualize the central properties of organization environments [7, 18, 25] and act as significant measures of perceived uncertainty in the external environment [1, 24, 25]. These three dimensions relate to forces in the environment that can influence the organization. Force is operationally defined as an entity external to

cyber-connected critical infrastructure organizations that can effect change in their environment. These forces can be competitors, customers, economic, technological, political, ethical, demographic, cultural and social [17, 24, 57]. 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 [31].

***Complexity.***

Complexity relates to the total amount of forces in the environment, whether they are connecting with each other, and the degree by which they can influence other organizations. For example, a weak force in isolation lowers uncertainty, whereas many interconnecting strong forces increase uncertainty [2, 18, 24].

***Dynamism (Turbulence).***

Dynamism refers to change measured in speed and quantity. Organizations that face a significant amount 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, 18, 24].

***Munificence (Resource).***

Munificence deals with capacity, or more generally, the amount of resources available to sustain or support that environment. This category represents a considerable portion of the focus of structural theory. As it pertains to uncertainty,

the scarcer the resources, the greater the uncertainty [2, 18, 47]. Figure 1 conceptually depicts munificence, complexity and dynamism as sources of uncertainty in the external environment.

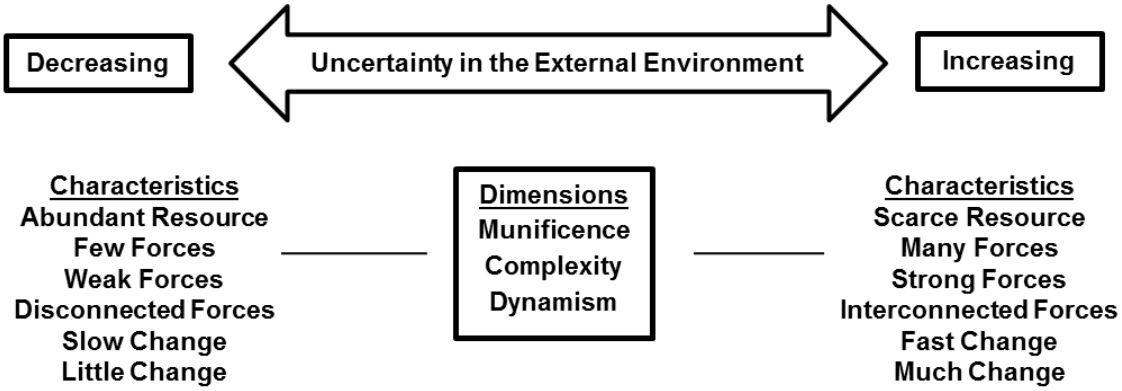



**Figure 1. The External Environment and Uncertainty**

## Structures

The mechanistic and organic structural continuum represents the type of forms organizations can take[11]. This continuum offers two extremes for management systems based on the level of perceived uncertainty in the environment. Empirical results strongly indicate that perceived environmental uncertainty significantly correlates with organic and mechanistic structural types. Table 2 lists characteristics of the two 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, policies and procedures | Decreased formalization |
| Standardized vertical communication | All-encompassing communication |
| Directives and orders | Advice and information sharing |
| Fixed functional departments | Fluid (mixed) functional departments |
| Status increases up hierarchy | Status increases with brilliance |
| Narrow span of control | Wide span of control |

## Mechanistic and Organic in Practice

Two organizations are used as examples to demonstrate mechanistic and organic structures. The U.S. Army is used to typify mechanistic structures; Apache Indians, Anonymous and Al Qaeda display examples of organic structures.

### *Mechanistic Organization: U.S. Army.*

An Army infantry division represents an organization that displays mechanistic characteristics. While not all of the Army trends toward mechanistic, most of the Army easily fits this structure. A typical division is largely mechanistic when analyzing its dimensional traits.

This particular type of structure is common throughout the Army regardless of the environment and context in which it conducts business. Recent combat operations in Iraq are an example. During the initial campaign, 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 Army found its divisional structure ill-suited for nation building, and struggled to find the flexibility to adjust amidst the growing dynamics and complexities (e.g., environmental uncertainty) of a counterinsurgency [4]. This experience serves to highlight the need for flexible organizational modification processes. Table 3 depicts the structural dimensions of a typical infantry division.

**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 subunits. | 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 | The amount of personnel supervised is 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 Army. | Mixed-Organic |
| Status | Increases up the hierarchy. | Mechanistic |
| Communication | More vertical than all encompassing; directive and orders based. | Mechanistic |

The means of creating an Army organization offers some explanation as to why they are mechanistic.

***Creating Mechanistic Organizations.***

The Army creates organizations through the Force Development Process which "consists of defining military capabilities, designing force structures to provide these capabilities, and translating organizational concepts based on doctrine, technologies, materiel, manpower requirements, and limited resources into a trained and ready Army" [56].

There are five phases in the Force Development Process, and they are:

(1) Develop capabilities.

(2) Design organizations.

(3) Develop organizational models.

(4) Determine organizational authorizations.

(5) Document organizational authorizations.

Army organizations follow this process, to include Army cyber organizations. This five-step process results in the creation of an organizational structure. Figure 3 shows the model of the system of systems process with the inputs and outputs.

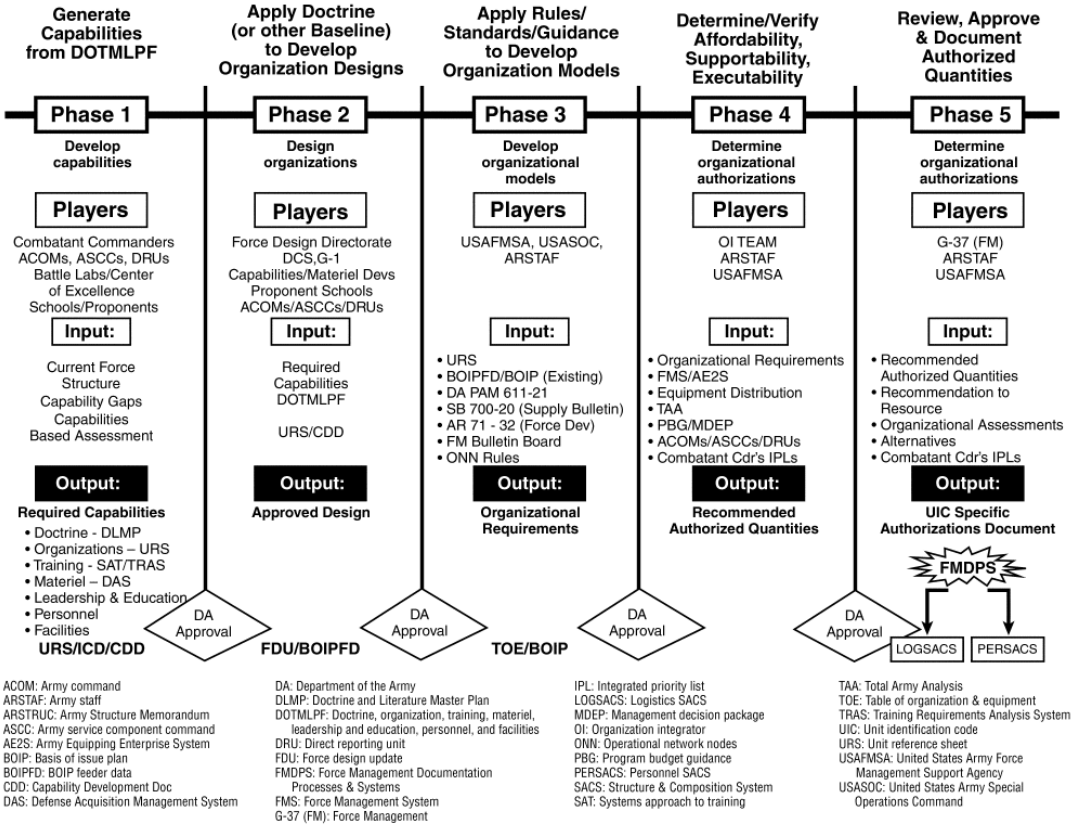



**Figure 2. Army Force Development Process (AR 71-32) [56]**

Once the Army identifies the requirement for a new organization, the planning, programming, budgeting, and execution (PPBE) process begins to develop the organization. The process map in Figure 4 highlights the key steps.

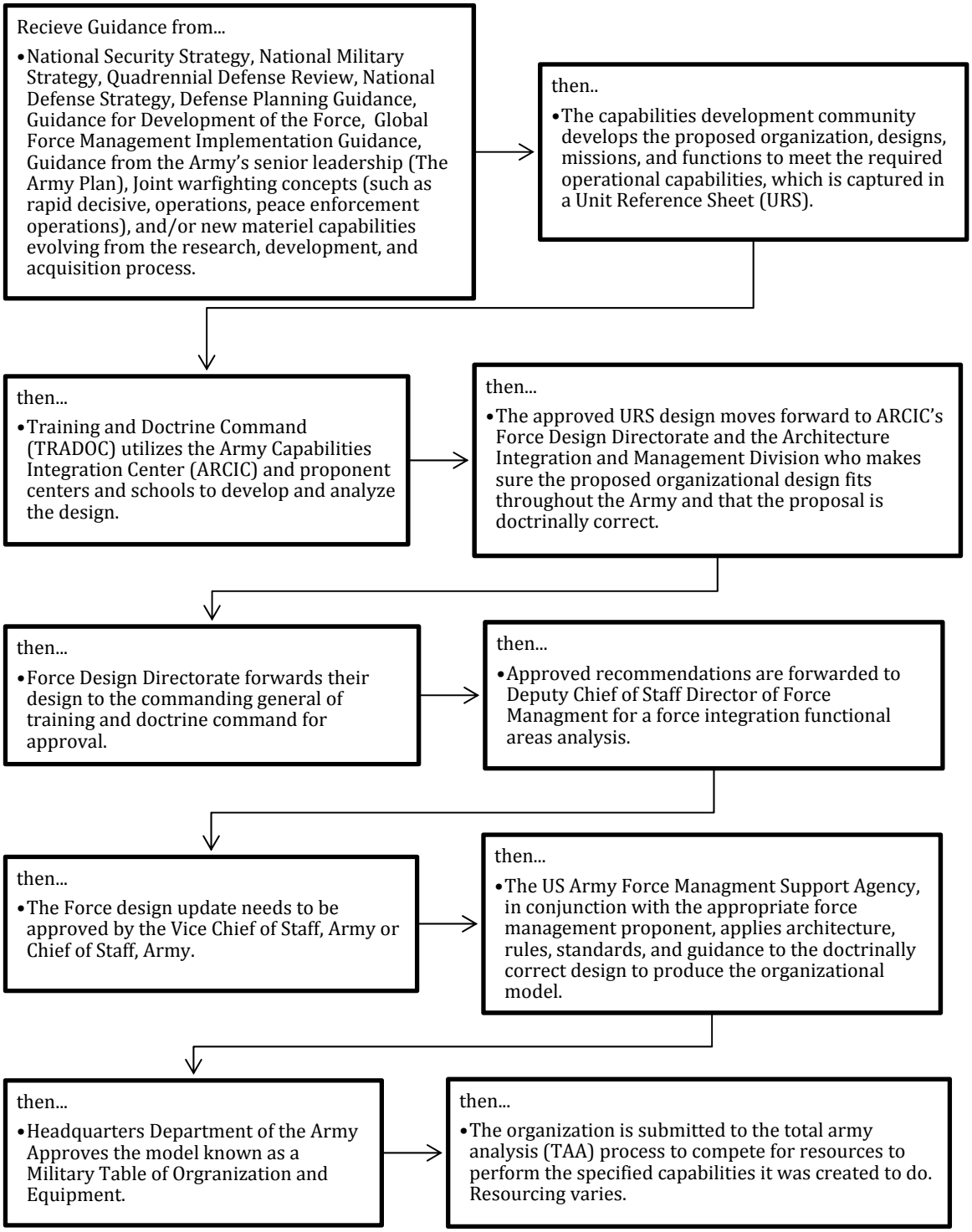



**Figure 3. Process Map for Creating Army Organizations**

The process map does not show all of the process. For instance, the Army will still need to purchase equipment, requisition personnel, prep sites, and publish doctrine. All of this happens within the confines of what has occurred previously. This process does not happen quickly. Senior leader approval can cause bottlenecks (there are many in this example), transitions from one organization to another, rework, or additions/modifications from approving officials. Leaders often change, which creates stagnation in the process. Several other factors and variables cause delay to include embedded subprocesses. All of this adds up to an organizational creation process facilitating mechanistic entities. Perhaps the most significant point is that the Army evaluates structural context to determine needed capabilities, not to determine structural strategy.

***Organic Organizations: Apache Indians, Anonymous and Al Qaeda.***

The Apache Indians, Anonymous Cyber Network, and Al Qaeda offer examples of organic structuring in a nearly pure form. These three organizations exhibited an unusual ability to succeed against vastly larger adversaries; they operate in highly uncertain environments, characterized by sudden and vast amounts of change, considerable forces that are prone to shift at a moment's notice, and limited availability of resources. Table 4 depicts the structural dimensions of these organizations.

**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 subunits; near flat organizational hierarchy with common themes allowing 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 |

The Apache Indians have occupied what are now northern Mexico and the southwestern United States for hundreds of years. They increased in fame and notoriety during the era of Spanish Conquistadors in the Americas in the 16th century. The Spanish appeared to be unstoppable as they gained considerable ground throughout Central America until they ventured north and encountered the Apache. The Spanish met their match in an undersized and under-resourced adversary [9].

The anonymous hacker group is similar. They clashed with Fortune 500 companies, computer security firms, major religious organizations and brought them, at least temporarily, great difficulty [44].

Al Qaeda has very noticeably kept powerful militaries busy for over a decade. They have done so using simple technology and sneaky tactics to make up for their lack of air support, advanced communications and weaponry. There is a commonality in these three organizations and their adversaries. All of their adversaries exhibited tendencies to structure and operate in a mechanistic fashion despite external environmental conditions that suggest the opposite.

***Creating Organic Organizations.***

Describing the creation of these and other organic organizations is difficult; they are, almost by definition, unstructured. However, Burns and Stalker highlight the presence of three factors in the creation of organic structures: shared beliefs and goals, commitment to a common concern, and personnel with expertise who emerge as leaders [11]. Table 5 shows the presence of these factors.

**Table 5. Structural Factors Present in Creating Organic Organizations**

| Organization | Shared beliefs/goals | Common concern | Emergent leaders |
|---|---|---|---|
| 16th Century Apache Indians | Yes | Repelling the Spanish invasion | Nant'ans |
| Anonymous Hacker Group | Yes | Varies on emergent "operations" of interest | Ops champion; skilled hackers |
| Al Qaeda | Yes | Repel the west; establish a caliphate | Commanders/emirs |

The strength of the factors appears to increase the strength of the organization. When beliefs and goals begin to compete with one another, this can create opposing factions, effectively reducing the collective power of the entity. A common concern acts to focus the horizontal structure, which creates the impetus for more skilled leaders to champion it. Weakening the common concern likewise weakens the integration of existing groups. Followers choose leadership based on proven effectiveness in the area of interest. The absence of skilled leaders hinders the ability of the organization to accomplish goals. In the case of the Apache, leaders are known as Nant'ans, spiritual and cultural front-runners people liked following [9]. There were many Nant'ans, and they would at times align with each other when needed. When one died, another would emerge. Figure 5 is a depiction of horizontal and network-based nature of the Apache Indians in the 16th century:

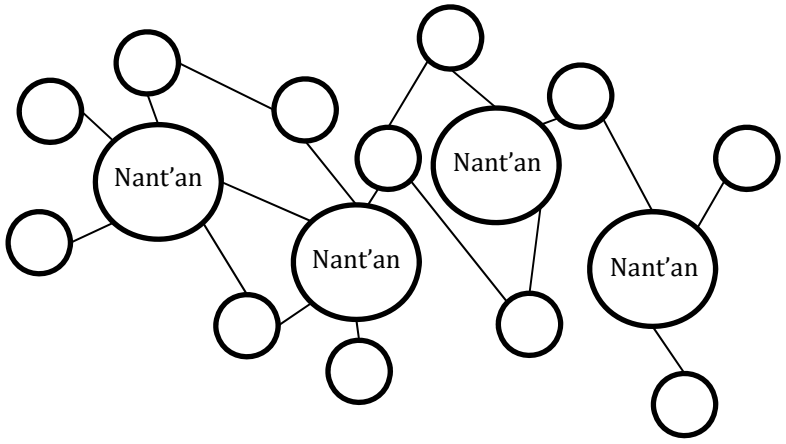



**Figure 4. Apache Structural Depiction**

**Structure and Environmental Uncertainty Synthesis**

As it relates to performance, the greater the perceived uncertainty in the environment, the more the organization should take an organic form, and with less uncertainty, they undertake a mechanistic form [11, 29, 39]. When an organization takes an organic form in an environment that is highly uncertain, this is considered a structural fit, which is shown to increase performance [21]. This alignment seems intuitive, as organic structures are more fluid and adaptable. Following the same logic, organic structures are not as helpful in stable environments. It is worth noting that no single contingency or structure applies to all. Organic or mechanistic structural types are only "better" if they fit the contingencies. Organizational structures and their relationship to environmental uncertainty and structural contingency can be synthesized as shown in Figure 2.

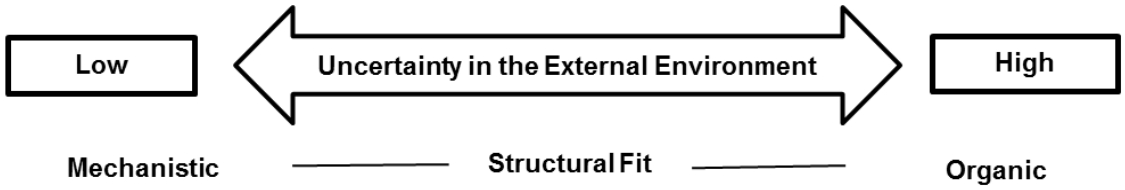



**Figure 5: Organizational Structure, Uncertainty and the External Environment**

This research seeks to find out the level of uncertainty in the general external environment of cyber connected critical infrastructure to determine structural guidance for cyber organizations tasked with protecting these critical assets.

# III. Methodology

## Research Design and Methodology

The research method is a multiple case study. The approach is structured as an exploratory study with a retrospective lens for organizational patterns. The case study method allows investigators to retain the holistic and meaningful characteristics of real-life events such as individual life cycles, small group behavior, organizational and managerial processes and the maturation of industries [60].

The data analysis technique is content analysis. Content analysis is suitable for condensing many words within a document into a small set of content categories based on explicit coding rules for the purpose of examining them [6, 30, 37, 54]. 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 [58]. This research highlights external environmental uncertainty for its significant influence in shaping organizational structure across the following three measured dimensional categories: (i) complexity; (ii) dynamism (turbulence); and, (iii) munificence (resource) [18].

## Data Collection

Once external environmental uncertainty was chosen as the focus of this research, the content analyst was able to draw a stratified purposive sample of

artifacts (documents) from the published material. The strata (cases) divided into academia, government and private/practitioner [43, 46]. Each represents stakeholders of publicly available information related to critical infrastructure and cyber in the United States. Information about the cyber linkage to critical infrastructure is a specific topic of interest where relevant information is known mostly to a specific subset of professionals within these three strata [37]. Search engines (including Google, RAND/CSIS/MITRE and .gov sources) identified the artifacts using algorithms that sort document retrieval from large databases. This process helps to identify artifacts with the most references and information related to critical infrastructure and cyber. The U.S. Government Accountability Office's (GAO) definition of artifacts as physically separable, minimally sized, and self-contained textual information was adopted [30].

***Artifact Discrimination.***

Artifacts were retrieved using the search terms industrial control system, SCADA, and critical infrastructure cyber, based on their close linkage to cyber-connected critical infrastructure [8]. The initial search harvested a large number of artifacts. In filtering the results, additional criteria were applied to achieve a relevant and representative sample for each stratum. Table 6 lists the criteria. The content analyst converted the final selection of artifacts (Appendix A) into individual portable document format (PDF) to minimize the file size, standardize the format for all coders, and make importing into coding software (e.g., Maxqda) easy.

**Table 6. Artifact Criteria**

| Category | Criteria |
|---|---|
| Content | Discuss cyber and the 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 |

Table 7 contains the search results. More artifacts that are academic were reviewed because of their perceived reliability, validity and trust. A slightly higher amount of private/practitioner artifacts were reviewed than government because of search engine limitations unique to RAND, CSIS and MITRE. Google's platform dominated by its ability to return results concentrated on the focus area, which was very timely (usually within one year of publication). Government artifact selection also suffered from search engine limitations and syntactic issues (e.g., included only minutes from congressional meetings) that increased the amount of artifacts needed to be viewed.

**Table 7. Artifact Retrieval Results**

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

Artifacts were randomized using Microsoft Excel to generate the final sample. All 68 artifacts (Appendix B) meeting the selection criterion were coded with an A,

P, G (academic, private/practitioner, and government). The final random sample contained 20 documents per coder (distributed 10-A/5-P/5-G) for a total of n=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 infrastructure is not the goal. The goal is to retrieve a useful set of artifacts to answer the research question fairly [37].

***Organizational Diversity.***

The documents analyzed by the coders represented a diverse amount of information from all three strata. Parent organizations that have published content included in the final sample are: Association for Computing Machinery, IEEE, Forbes, Army Research Lab, International Journal of Critical Infrastructure Protection, Economist, Tripwire, Department of Homeland Security, Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, White House, Government Accountability Office, Dow Jones and Co., and International Federation for Information Processing.

## Coding

Krippendorf defines coding as the step of classifying the sampling or recording units in terms of the categories of the analytical constructs chosen [37]. The sampling unit elected to categorize the information present in the artifact is "the sentence" [54], because of its ability to obtain meaning in relation to text [37],

and due to the use of human coders [30]. Each sentence was read and coded against the code categories using the recording unit classification diagram listed in Appendix C. 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 meaningful and feasible for an artifact that contains less than eight pages of codeable material [37]. An example of a coded artifact is in Appendix D.

***Content Categories.***

The Maxqda graphical user interface provides a visual display of code categories and coded material to check operational definitions against sampling units, as displayed in Figure 6.

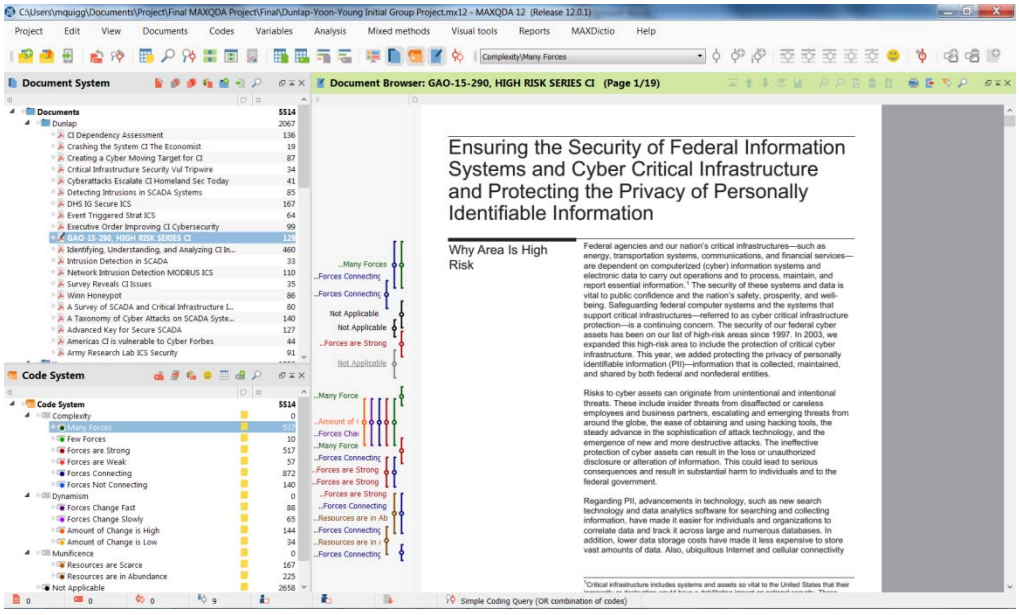



**Figure 6: Maxqda Graphical User Interface**

The "Not Applicable" code category was included in addition to the existing a priori categories of complexity, dynamism and munificence to ensure exhaustiveness [30, 54]. All forces discussed relate to the general external environment. Table 8 lists the code categories.

**Table 8. Code Category Definitions**

| Code Category | Sub Category | Definitions |
|---|---|---|
| Complexity | Forces interconnecting | Are the forces interconnecting? (CONNECTEDNESS) |
| Complexity | Forces not connecting | Are the forces disconnected? (CONNECTEDNESS) |
| Complexity | Many forces | Are the forces many? (AMOUNT) |
| Complexity | Few forces | Are the forces few? (AMOUNT) |
| Complexity | Forces are strong | Are the forces strong? (STRENGTH) |
| Complexity | Forces are weak | Are the forces weak? (STRENGTH) |
| Dynamism | Forces change a lot | Is there a high amount of change? (AMOUNT) |
| Dynamism | Forces change infrequently | Are forces changing very little? (AMOUNT) |
| Dynamism | Forces change fast | Is change happening quickly? (SPEED) |
| Dynamism | Forces change slowly | Is change happening slowly? (SPEED) |
| Munificence | Resources are scarce | Are the amount of resources available scarce? (AMOUNT) |
| Munificence | Resources are in abundance | Are the amount of resources available abundant? (AMOUNT) |
| Not Applicable | Not Applicable | All other sentences (N/A) |

***Coder Training.***

Qualitative data analysis software (Maxqda) was selected for the ability to manage large volumes of text, display information with ease and for working with multiple coders [52]. The content analyst familiarized the coders with Maxqda, operational definitions and code categories (see Appendix E). Also, well-defined explicit coding instructions were written into Maxqda to improve coding consistency [54]. Only the content analyst trained and evaluated each coder [37]. They participated in a beta coding session to improve coding consistency and to minimize idiosyncratic judgments in the coding process [37]. The training process produced favorable reliability results. The coders trained on documents not included in the final sample. No collaboration amongst the coders was allowed during the coding process.

Three graduate students with a strong background in cyber coded the documents. The importance of coders being familiar with the phenomena under consideration was a critical factor in coder selection [37]. The reading level of the documents demanded coders with a higher education level.

**Data Reduction**

Once the coders finished, the completed thumb drives were given to the content analyst to aggregate. The combined data sets generated numerous descriptive statistics, charts, and tables. The content analyst scrutinized the data for

outliers, incomplete artifacts, and other anomalies. All of the artifacts were deemed complete and properly coded. The data were imported into Microsoft Excel to look for analysis of patterns and trends within and across the set. Numerous graphs and tables were collapsed into a tight set which best articulated the findings.

**Validity**

Every step of the research process was conducted to ensure the quality of the results led to an acceptance of truth. The guidelines set forth by Klaus Krippendorff [37] for validity in content analysis were followed and reviewed periodically throughout the research process.

**Reliability**

To ensure valid inferences from the text, word meaning and category definitions were tightened, multiple coders were used and intercoder agreement was calculated. Cohens Kappa [14] was calculated as a measure of reliability. It is considered a strict measure of agreement between coders based on the selection of a particular code for the recording unit [42].

# IV. Analysis and Results

## Descriptive Statistics

Table 9 shows the coding units range from 1,594 to 2,067 (mean=1,838). The primary reason for this variance lies in how each coder interpreted the coding unit. The ambiguity of the language in the published material might cause one coder to perceive the presence of a coding unit while another did not.

**Table 9. Total Codes by Coder**

| | Coder | | |
|---|---|---|---|
| | 1 | 2 | 3 |
| Pages | 156 | 156 | 156 |
| Documents | 20 | 20 | 20 |
| Coding units | 2067 | 1853 | 1594 |

Table 10 shows that each coder read 156 pages, which averaged 7.8 pages per artifact. Although there were more academic artifacts than government, the government artifacts averaged more pages (13.8). Subsequently, the difficulty of interpreting the sampling unit (sentence) in relation to the context unit (artifact) increased [37].

**Table 10. Pages Coded by Strata**

| | Academic | Government | Private/Practitioner | Aggregate |
|---|---|---|---|---|
| Pages Read | 74 | 69 | 13 | 156 |
| Pages Per Artifact | 7.4 | 13.8 | 2.6 | 7.8 |

Flesch-Kincaid Reading Level and Flesch Reading Ease measures were calculated for each artifact. Table 11 shows the results. The Flesch-Kincaid formulas are mathematical derivations accounting for the amount of words in a sentence and syllables per word to generate a grade level guide for comprehension and ease of reading [26, 35]. The total pages coded were 156, with an average 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 suffered the highest amount of disagreement.

**Table 11. Flesch-Kincaid Reading Scores**

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

## Intercoder Agreement

Based on Landis and Koch [38], the coder agreement in Table 12 ranges from fair (21%-40%) to substantial (61%-80%) which results in moderate overall agreement with Kappa ranging from 51%-60%. Several factors can affect Kappa (e.g., amount of categories (13), specificity of definition); since the research is exploratory, lower levels of agreement are considered acceptable [42]. Coders were allowed considerable latitude in content interpretation based on their expertise and training. Despite challenges, the results indicate agreement between coders.

**Table 12. Cohens Kappa**

| | Coders | | | |
|---|---|---|---|---|
| | 1 and 2 | 1 and 3 | 2 and 3 | Mean |
| Academic | 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** |

## Code Distribution

Table 13 lists the frequency distribution of codes across the sample (n=60). The coders assigned a dimensional code to 51.8% of the content (2,856 sentences). The category "not applicable" was removed from the frequency analysis in Table 13 to remove bias. The frequency analysis indicates that complexity has a strong presence (more than 91%) in each stratum. Complexity (e.g., forces connecting, many forces, forces are strong) accounts for 67.43% of uncertainty in the content coded. Dynamism (e.g., amount of change is high, forces change fast) accounts for 8.12% of uncertainty in the content coded. Munificence (e.g., resources are scarce) accounts for 5.85% of uncertainty in the content coded. Based on coder interpretation, as Figure 7 indicates, there is a strong presence (81.4%) of uncertainty in the general external environment present across the three strata sampled.

**Table 13. Frequency Analysis of Codes**

| Parent code | Code | Frequency | Percent | Documents |
|---|---|---|---|---|
| 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 in Abundance | 225 | 7.88 | 36 |
| Munificence | Resources are Scarce | 167 | 5.85 | 44 |
| Dynamism | Amount of Change is High | 144 | 5.04 | 44 |
| Complexity | Forces Not Connecting | 140 | 4.90 | 32 |
| Dynamism | Forces Change Fast | 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 | - |

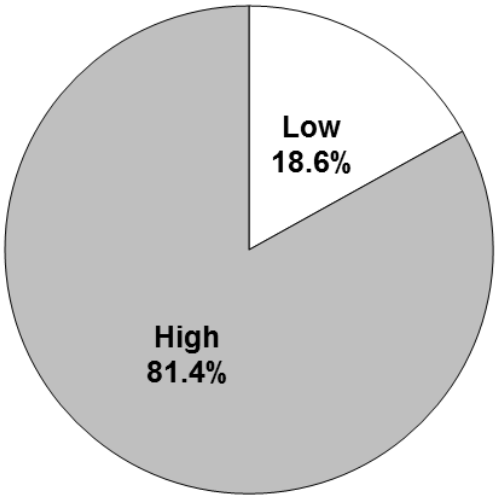



**Figure 7. Uncertainty in the General External Environment**

## Strata Analysis

The following sections will provide an analysis of the presence of uncertainty in the general external environment, within and across strata, displayed in Figure 8.

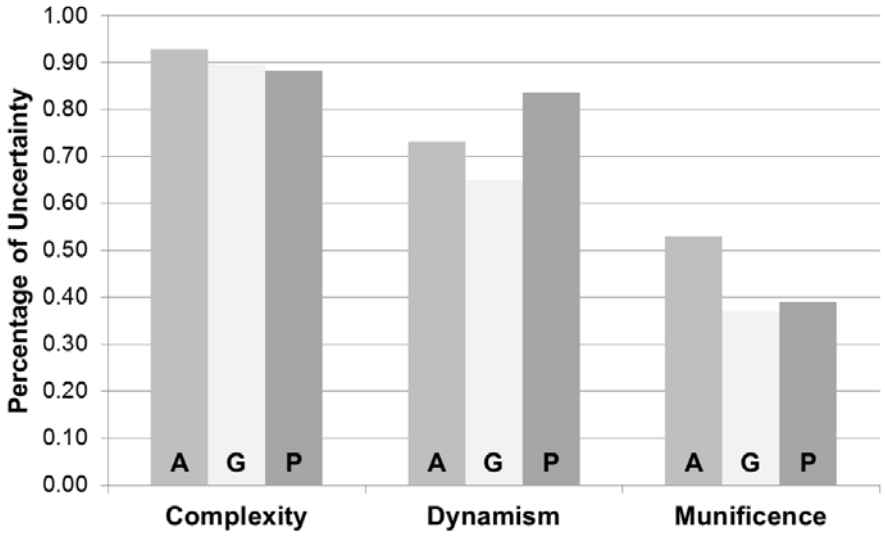



**Figure 8. Percentage of Uncertainty by Dimension and Strata**

### *Complexity.*

Figure 8 illustrates there is strong evidence to support that complexity is extremely high. All three strata showed 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. Private/practitioner displays significantly higher uncertainty than government and academic strata. This level of

uncertainty appears to be reasonable because of the increased competition and desire for revenue present in the private/practitioner environment. This environment requires the ability to dissolve or create organizations rapidly, modify processes, and innovate in response to market stimuli.

The government strata exhibit a lower presence of uncertainty. Unlike private/practitioner, government functions are slow to change. Despite this, coders agree there is 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 13).

***Munificence.***

It is clear from the results there is explanatory power and a measurable degree of resource scarcity (munificence) in the environment. The presence of uncertainty is lower overall across all three environmental resource measures. However, the academic strata exhibit significantly more perceived resource scarcity in the general external environment. A reasonable explanation for the difference is the breadth and depth of research the academic sector dedicates to this complex area.

## Coder Analysis

Figure 9 clearly demonstrates the coders were consistent in their coding across all three dimensions of uncertainty. While there is slight disagreement in munificence (resource) and complexity (amount/connectedness of forces), there is general agreement overall.

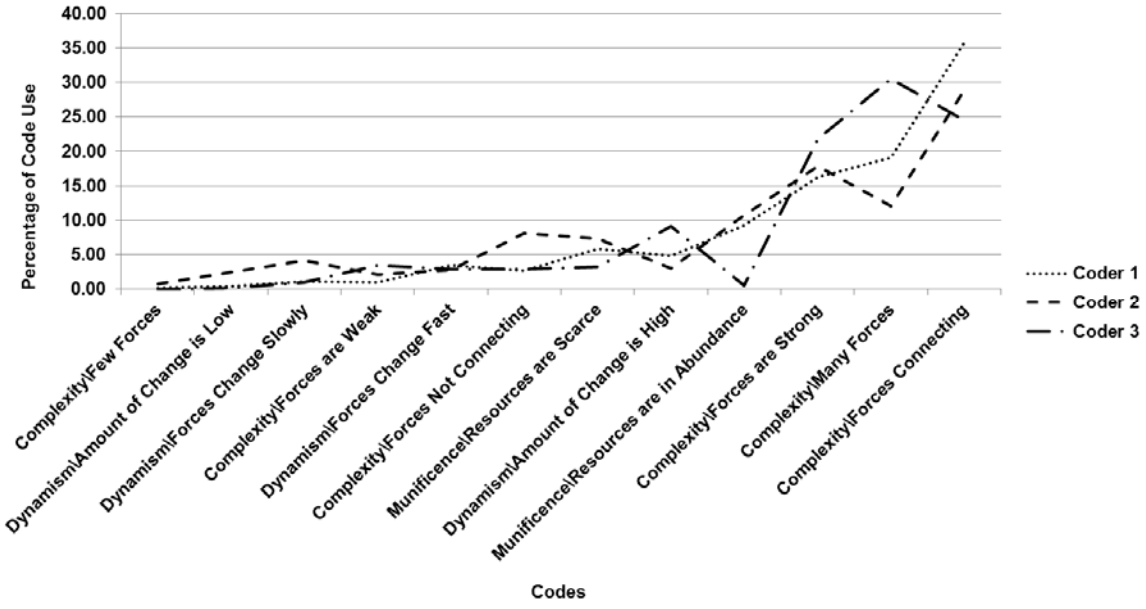



**Figure 9. Coder Overlap**

## Recommendations for Action

Understanding the outcomes presented in this study, it would be logical to structure government cyber organizations operating in the critical infrastructure environment in an organic fashion rather than the current mechanistic structure. The government should generate separate processes in the creation of these

organizations to allow for fast implementation and frequent modification. These cyber organizations should have the following characteristics if they are to succeed:

- People do not perform highly specialized tasks but have a broader view.
- A chain of command exists but is more decentralized because of the need for shifting responsibilities.
- The high level of complexity and change in the environment warrants knowledgeable personnel working in teams and coordinating frequently to make fast decisions when needed.
- Communication often occurs and at many levels.
- Orders and directives diminish as advice and information sharing increase.
- Knowledge and expertise increase individual status.

One of the most appealing aspects of the research is the potential for generalizability to other cyber organizations operating within the United States and similarly developed countries. One could make the argument that the cyber environments of the Department of Homeland Security, the Department of Defense, private utility companies, and high technology firms have significant similarities.

It is worth mentioning that significant barriers exist to implementing these principles in the DoD and other government agencies ranging from culture to strategic direction. Understanding the connections between organizational performance, structure, and the environment should act as an impetus for these difficult changes.

# V. Conclusions

## Conclusions of Research

Few topics within the area of national interest are more important than the understanding of how to organize in cyber and protect national critical infrastructure assets from cyberspace threats. Participation at the United States Army Cyber Talks at the National Defense University in September of 2015 served to strengthen the need for empirical analysis and evidence that could lead to organizational structuring decisions and adjustments. Innovation and knowledge management were direct concerns of attendees, which relate directly to organizational structure [40]. Several structural dimensions were repeatedly discussed as inhibitors to performance further validating the need for this research.

The three research questions answered in this study were:

1. What is organizational structure?

   Answer: The research literature depicts organizational structure in two dimensions: structural and contextual. The contextual dimensions significantly affect the structural dimensions.

2. What theories contribute to organizational structure?

   Answer: Institutional isomorphism, resource dependence, population ecology, and structural contingency are dominant organizational theories that contribute to the explanation of organizational structure. Of these four theories, structural contingency provides a pragmatic explanation of how to structure organizations based on context and contingency. The environment emerges as a prominent point of focus in every dominant theory. The level of uncertainty with regard to the organization's general external environment shows a strong connection to structural type.

3. How should organizations structure in cyber environments to defend critical infrastructure?

   Answer: The perceived level of uncertainty, as measured by the degree of complexity, dynamism, and munificence in the external environment of cyber organizations relates well to the mechanistic and organic structural continuum. Cyber organizations should structure organically in highly uncertain environments and mechanistically in less uncertain environments.

As it pertains to the cyber-connected critical infrastructure environment, forces within and across strata are overwhelmingly numerous, strong and connecting. The amount of change at present is very high. The speed of change is fast and resources are typified by an abundance of information technology with low barriers to entry creating opportunity and availability for adversary and ally alike. These elements create the perception of a highly uncertain situation for organizations operating in the cyber-connected critical infrastructure environment. Organic structuring principles allow for the adaptability and flexibility this environment requires. This research indicates organizations should follow organic structuring principles while operating in the cyber-connected critical infrastructure environment.

## Recommendations for Future Research

### *Measure Government Cyber Organizations.*

This research approached answering the question of how to structure organizations in cyberspace by first analyzing the contextual dimension of external environmental uncertainty. It will now be appropriate and helpful to measure empirically structural dimensions of government cyber organizations (e.g., DHS ICS-CERT, USCYBERCOM), to contribute further to the answer.

### *Replicate the Study.*

This research focused on the U.S. only. However the U.S. is not the only country in need of strategic direction in the creation of cyber organizations tasked to protect critical infrastructure. A replicative study for other allied nations who mutually support cyber alongside the U.S. (Great Britain, Australia, Canada, and New Zealand), would contribute to the overall security of each nation.

### *Identify Dominant Factors for Munificence.*

Munificence (resource) in this research is broadly defined. With the insight gained from this study, it is apparent that resource in cyber would benefit from structural equation modeling (e.g., confirmatory factor analysis). This research will aid in the identification of dominant resource factors in the cyber-connected critical infrastructure environment.

Appendix A. Artifact Final Selection (Front Page Information)

# Event-triggered strategies for industrial control over wireless networks (invited paper)

Maben Rabi
ACCESS Linnaeus Centre
School of Electrical Engineering
Royal Institute of Technology
100 44 Stockholm, Sweden
maben.rabi@ee.kth.se

Karl H. Johansson
ACCESS Linnaeus Centre
School of Electrical Engineering
Royal Institute of Technology
100 44 Stockholm, Sweden
karl.henrik.johansson@ee.kth.se

## ABSTRACT

New event-based sampling strategies can support the efficient use of radio resources in wireless control systems. Motivated by the recent introduction of wireless network nodes in process control industry, we consider the particular demands these closed-loop systems set on the wireless communication and the influence the communication has on the control performance. In the paper, it is pointed out that by letting sensor nodes transmit only when needed, it is possible to minimize the communication bandwidth utilization in these systems. We show how classical control strategies commonly based on periodic sampling, such as proportional-integral-derivative control and minimum variance control, can be cast in an event-based setting in which decentralized communication decisions are taken suitable for commonly used contention-based medium access control protocols. Event-triggered sampling for estimation is also reviewed. Simulated examples illustrate the results.

## 1. INTRODUCTION

There is a growing deployment of wireless networks in industrial control and automation. The lower installation cost and easier system reconfiguration for wireless devices can have a major influence on future control systems. Employing several control loops over a common wireless medium raises however new issues on how to allocate radio resources in an efficient way with guarantees on closed-loop system performance for the control applications. In some situations, a deterministic scheduling of the communication medium for control and estimation applications is required. In many cases, however, feedback control can provide good performance also with contention-based access schemes. In this paper, we show precisely that by indicating how event-triggered sensing and control provides a more scalable and efficient trade-off between control performance and communication cost. By making transmissions only when needed and taking the communication decisions locally at the sensor nodes, it is possible to minimize the communication bandwidth utilization.


*WICON'08* November 17-19, 2008, Maui, Hawaii, USA

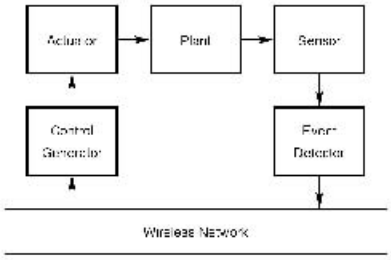




**Figure 1: Control architecture for event-triggered control over a wireless network.**

Proportional-integral-derivative (PID) control is by far the dominating controller in process industry [5]. Design and implementation of PID controllers with periodically sampled sensor readings and control actuations is a well established area [4]. Stochastic optimal control is in its simplest formulation denoted minimum variance control, in which, the variance of the plant output is minimized by suitable zero-order hold control [2]. The traditional implementation of also minimum variance control is through periodic updates of the controller and actuator.

The main contribution of this paper is to propose extensions of these traditional control architectures to event-based implementations. By removing the constraint of periodic communication of sensor and control data, the wireless network resources can be used more efficiently. The proposed event-triggered control architecture is shown in Figure 3. An event detector decides on when to transmit plant information depending on the sensor measurements. The receiver generates a control command that is executed by the actuator. The main inspiration to this scheme comes from the work on event-triggered and time-triggered control in [3]. More recent contributions in the area includes [9, 11, 7, 10]. A deadband-based PID controller was proposed in [1].

The outline of the paper is as follows. Section 2 introduces event-triggered PID control. In particular, a suitable event



**The White House**
Office of the Press Secretary

For Immediate Release February 12, 2013

# Executive Order -- Improving Critical Infrastructure Cybersecurity

EXECUTIVE ORDER

---

# Ensuring the Security of Federal Information Systems and Cyber Critical Infrastructure and Protecting the Privacy of Personally Identifiable Information

## Why Area Is High Risk

Federal agencies and our nation's critical infrastructures—such as energy, transportation systems, communications, and financial services—are dependent on computerized (cyber) information systems and electronic data to carry out operations and to process, maintain, and report essential information.[1] The security of these systems and data is vital to public confidence and the nation's safety, prosperity, and well-being. Safeguarding federal computer systems and the systems that support critical infrastructures—referred to as cyber critical infrastructure protection—is a continuing concern. The security of our federal cyber assets has been on our list of high-risk areas since 1997. In 2003, we expanded this high-risk area to include the protection of critical cyber infrastructure. This year, we added protecting the privacy of personally identifiable information (PII)—information that is collected, maintained, and shared by both federal and nonfederal entities.

Risks to cyber assets can originate from unintentional and intentional threats. These include insider threats from disaffected or careless employees and business partners, escalating and emerging threats from around the globe, the ease of obtaining and using hacking tools, the steady advance in the sophistication of attack technology, and the emergence of new and more destructive attacks. The ineffective protection of cyber assets can result in the loss or unauthorized disclosure or alteration of information. This could lead to serious consequences and result in substantial harm to individuals and to the federal government.

Regarding PII, advancements in technology, such as new search technology and data analytics software for searching and collecting information, have made it easier for individuals and organizations to correlate data and track it across large and numerous databases. In addition, lower data storage costs have made it less expensive to store vast amounts of data. Also, ubiquitous Internet and cellular connectivity

[1]Critical infrastructure includes systems and assets so vital to the United States that their incapacity or destruction would have a debilitating impact on national security. These critical infrastructures are chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; health care and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

FEATURE


## Identifying, Understanding, and Analyzing

# Critical Infrastructure Interdependencies

By Steven M. Rinaldi, James P. Peerenboom, and Terrence K. Kelly

The notion that our nation's critical infrastructures are highly interconnected and mutually dependent in complex ways, both physically and through a host of information and communications technologies (so-called "cyber-based systems"), is more than an abstract, theoretical concept. As shown by the 1998 failure of the *Galaxy 4* telecommunications satellite, the prolonged power crisis in California, and many other recent infrastructure disruptions, what happens to one infrastructure can directly and indirectly affect other infrastructures, impact large geographic regions, and send ripples throughout the national and global economy.

In the case of the *Galaxy 4* failure, the loss of a single telecommunications satellite led to an outage of nearly 90% of all pagers nationwide [1]. From an interdependency perspective, it also disrupted a variety of banking and financial services, such as credit card purchases and automated teller machine transactions, and threatened key segments of the vital human services network by disrupting communications with doctors and emergency workers. In California, electric power disruptions in early 2001 affected oil and natural gas production, refinery operations, pipeline transport of gasoline and jet fuel within California and to its neighboring states, and the movement of water from northern to central and southern regions of the state for crop irrigation [2]-[6]. The disruptions also idled key industries, led to billions of dollars of lost productivity, and stressed the entire Western power grid, causing far-reaching security and reliability concerns [7]-[10].

*Peerenboom (jpeerenboom@anl.gov) is with Argonne National Laboratory, 9700 S. Cass Ave., Bldg. 900, Argonne, IL 60439, U.S.A. Rinaldi is with the Air Force Quadrennial Defense Review, Washington, D.C. 20330-1670, U.S.A. Kelly is with the Executive Office of the President, Washington, D.C. 20502, U.S.A.*

0272-1708/01/$10.00©2001IEEE

# Intrusion Detection in SCADA Networks

Rafael Ramos Regis Barbosa and Aiko Pras

University of Twente
Design and Analysis of Communication Systems (DACS)
Enschede, The Netherlands
{r.barbosa,a.pras}@utwente.nl

**Abstract.** Supervisory Control and Data Acquisition (SCADA) systems are a critical part of large industrial facilities, such as water distribution infrastructures. With the goal of reducing costs and increasing efficiency, these systems are becoming increasingly interconnected. However, this has also exposed them to a wide range of network security problems. Our research focus on the development of a novel flow-based intrusion detection system. Based on the assumption that SCADA networks are *well-behaved*, we believe that it is possible to model the *normal* traffic by establishing relations between network flows. To improve accuracy and provide more information on the *anomalous* traffic, we will also research methods to derive a flow-based model for *anomalous* flows.

## 1 Introduction

Large industrial facilities such as water distribution infrastructures, electricity generation plants and oil refineries need to be continuously monitored and controlled to assure proper functioning. SCADA (Supervisory Control and Data Acquisition) systems are commonly deployed to aid these actions, by automating telemetry and data acquisition. Historically, SCADA systems were believed to be secure because they were isolated networks: an operator station, or human-machine interface (HMI), connected to remote terminal units (RTUs) and programmable logic controlers (PLCs) through a proprietary purpose-specific protocol.

Yielding to market pressure, that demands industries to operate with low costs and high efficiency, these systems are becoming increasingly more interconnected. Many of modern SCADA networks are connected to both the company's corporate network and the Internet[1]. Furthermore, it is common that the HMI is a commodity PC, which is connected to RTUs and PLCs using standard technologies, such as Ethernet and WLAN (see Figure 1). This has exposed these networks to a wide range of security problems. Probably the most well-know attack to a SCADA system happened at Maroochy Water Services in Australia [2]. An attacker was able to successfully interfere with the communications, causing pumps not to work properly and preventing alarms to be sent. Areas were flooded and rivers polluted with sewage. Another example happened in 2003, when the Davis-Besse nuclear power plant in Ohio was infected with

B. Stiller and F. De Turck (Eds.): AIMS 2010, LNCS 6155, pp. 163–166, 2010.

2012 45th Hawaii International Conference on System Sciences

# A Retrofit Network Intrusion Detection System for MODBUS RTU and ASCII Industrial Control Systems

Thomas Morris
Mississippi State University
morris@ece.msstate.edu

Rayford Vaughn
Mississippi State University
vaughn@research.msstate.edu

Yoginder Dandass
Mississippi State University
yogi@cse.msstate.edu

## Abstract

*MODBUS RTU/ASCII Snort is software to retrofit serial based industrial control systems to add Snort intrusion detection and intrusion prevention capabilities. This article discusses the need for such a system by describing 4 classes of intrusion vulnerabilities (denial of service, command injection, response injection, and system reconnaissance) which can be exploited on MODBUS RTU/ASCII industrial control systems. The article provides details on how Snort rules can detect and prevent such intrusions. Finally, the article describes the MODBUS RTU/ASCII Snort implementation, provides details on placement of a MODBUS RTU/ASCII Snort host within a control system to maximize intrusion detection and prevention capabilities, and discusses the system's validation.*

## 1. Introduction

National Electric Reliability Council (NERC) Critical Infrastructure Protection (CIP) Standard 005-4a [1] requires utilities and other responsible entities to place critical cyber assets within an electronic security perimeter. Electronic security perimeters must be subjected to vulnerability analyses, use access control technologies, and include systems to monitor and log the electronic security perimeter access. Industrial control system operators from other critical industries have followed the electric transmission and generation industry lead and have begun to adopt the electronic security perimeters to protect cyber assets in both control rooms and in the field. Electronic perimeter security minimizes the threat of illicit network penetrations, however, the concept of defense in depth encourages cybersecurity defenses within the electronic security perimeter including but not limited to virus scanning and deployment of intrusion detection systems (IDS) and intrusion prevention systems (IPS). This work documents an extension of a MODBUS RTU and MODBUS ASCII data logger to enable the use of the Snort [2] intrusion detection and intrusion prevention system features to protect retrofitted industrial control system assets within an electronic security perimeter.

The recent discovery of the Stuxnet [3] worm highlights the need to protect legacy serial based cyber assets such as remote terminal units (RTU) and intelligent electronic devices (IED). As of September 2010, the Stuxnet worm has infected over 100,000 computers in over 155 countries [4]. The Stuxnet worm searches for hosts with the Siemens WinCC human machine interface software package installed. If a WinCC host system is found and the WinCC host is connected to a Simatic S7-417 PLC and certain signatures match the targeted physical process controls, Stuxnet alters the firmware in the PLC. The Simatic S7-400 PLC series supports both Ethernet and serial port communications. This suggests it is possible to alter PLC the firmware of a serially connected RTU, IED, or PLC after a HMI host node is compromised.

A compromised computer serially connected to a control system device may also inject control system commands and false measurements, alter configuration settings on devices, and perform denial of service attacks against devices.

Serially linked control system devices are often connected using industrial radios. Such radio links can be compromised to allow attackers to remotely inject control system commands and false measurements, to perform system reconnaissance attacks, and to perform denial of service attacks [5].

Many security professionals consider serial links secure because they are non-routable protocols. However, the Stuxnet worm and the presence of vulnerable industrial radio links show this to be inaccurate and motivate the need for intrusion detection and intrusion prevention systems to protect RTU, IED, and PLC type devices connected to serial links.

The body of this paper includes a section discussing related works. Next, a section provides discussion on intrusion detection in industrial control systems for various types of threats. Next, a section describes the MODBUS RTU/ASCII Snort implementation including details on MODBUS RTU/ASCII to MODBUS TCP/IP conversion, details on the MODBUS RTU/ASCII Snort software architecture, guide lines for Snort host placement within a MODBUS RTU/ASCII network, and information on how the MODBUS RTU/ASCII Snort was validated. The paper ends with discussion of future works and conclusions.

978-0-7695-4525-7/12 $26.00 © 2012 IEEE
DOI 10.1109/HICSS.2012.78

INTERNATIONAL JOURNAL OF CRITICAL INFRASTRUCTURE PROTECTION 5 (2012) 30–39

Available online at www.sciencedirect.com

SciVerse ScienceDirect

journal homepage: www.elsevier.com/locate/ijcip

# Creating a cyber moving target for critical infrastructure applications using platform diversity*

*Hamed Okhravi*, Adam Comella, Eric Robinson, Joshua Haines*

*MIT Lincoln Laboratory, 244 Wood Street, Lexington, Massachusetts 02420, USA*

ARTICLE INFO

Article history:
Received 15 April 2011
Published online 28 January 2012

Keywords:
Cyber moving target
Cyber survivability
Platform heterogeneity
Diversity
Virtualization

ABSTRACT

Despite the significant effort that often goes into securing critical infrastructure assets, many systems remain vulnerable to advanced, targeted cyber attacks. This paper describes the design and implementation of the Trusted Dynamic Logical Heterogeneity System (TALENT), a framework for live-migrating critical infrastructure applications across heterogeneous platforms. TALENT permits a running critical application to change its hardware platform and operating system, thus providing cyber survivability through platform diversity. TALENT uses containers (operating-system-level virtualization) and a portable checkpoint compiler to create a virtual execution environment and to migrate a running application across different platforms while preserving the state of the application (execution state, open files and network connections). TALENT is designed to support general applications written in the C programming language. By changing the platform on-the-fly, TALENT creates a cyber moving target and significantly raises the bar for a successful attack against a critical application. Experiments demonstrate that a complete migration can be completed within about one second.



## 1. Introduction

Critical infrastructure systems are an integral part of the national cyber infrastructure. The power grid, oil and gas pipelines, utilities, communications systems, transportation systems, and banking and financial systems are examples of critical infrastructure systems. Despite the significant amount of effort and resources used to secure these systems, many remain vulnerable to advanced, targeted cyber attacks. The complexity of these systems and their use of commercial off-the-shelf components often exacerbate the problem.

Although protecting critical infrastructure systems is a priority, recent cyber incidents [1,2] have shown that it is imprudent to rely completely on the hardening of individual components. As a result, attention is now focusing on game-changing technologies that can ensure mission continuity in the face of cyber attacks. In fact, the US Air Force Chief Scientist's report on technology horizons [3] mentions the need for "a fundamental shift in emphasis from 'cyber protection' to 'maintaining mission effectiveness' in the presence of cyber threats" as a way to build cyber systems that are inherently intrusion resilient. Moreover, the White House National Security Council's progress report [4] mentions a "moving target" – a system that moves in multiple dimensions to foil the attacker and increase resilience – as one of the Administration's three key themes for its cyber security research and development strategy.

This paper describes the design and implementation of the Trusted Dynamic Logical Heterogeneity System (TALENT),

* This work is sponsored by the Department of Defense under Air Force Contract FA8721-05-C-0002. Opinions, interpretations, conclusions, and recommendations are those of the authors and are not necessarily endorsed by the United States Government.

* Corresponding author.
E-mail address: hamed.okhravi@ll.mit.edu (H. Okhravi).

1874-5482/$ - see front matter © 2012 Elsevier B.V. All rights reserved.
doi:10.1016/j.ijcip.2012.01.002

THE STATE OF SECURITY (HTTP://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/)

News. Trends. Insights.

FEATURED ARTICLES (HTTP://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/TOPICS/FEATURED/)

LATEST SECURITY NEWS (HTTP://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/TOPICS/LATEST-SECURITY-NEWS/)

TOPICS (HTTP://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/TOPICS/)

RESOURCES (HTTP://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/RESOURCES/)

ABOUT (HTTP://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/ABOUT/)

Search

HOME (HTTP://WWW.TRIPWIRE.COM/STATE-OF-SECURITY) » FEATURED ARTICLES (HTTP://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/TOPICS/FEATURED/) » Cyberterrorists Attack on Critical Infrastructure Could Be Imminent

# Cyberterrorists Attack on Critical Infrastructure Could Be Imminent



(HTTP://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/CONTRIBUTORS/KATHERINE-BROCKLEHURST/)

KATHERINE BROCKLEHURST (HTTP://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/CONTRIBUTORS/KATHERINE-BROCKLEHURST/)

FEB 1, 2015 |

FEATURED ARTICLES (HTTP://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/TOPICS/FEATURED/)



(http://www.tripwire.com/state-of-security/security-data-protection/security-controls/cyberterrorists-attack-on-critical-infrastructure-could-be-imminent/)



The premise of a January 27, 2015, article by CNBC (http://www.cnbc.com/id/102367777) is that there is good evidence that a cyber attack against nearly any country's critical infrastructure could be imminent. This kind of reporting has become so commonplace, but this doesn't seem like just more FUD (fear, uncertainty, and doubt) journalism.

# Cyberattacks Escalate As Critical Infrastructure Providers Remain Confident

By: Krysta Dodd, Staff Writer

07/28/2015 (10:39am)

SHARE

Despite the increasing number of major cyber attacks targeting critical infrastructure, technology and security professionals remain confident in their cyber defenses, revealing a disconnect between these executives and the reality of the current threat landscape, according to a recent report by Intel Security and the Aspen Homeland Security Program.

The *Holding the Line Against Cyber Threats: Critical Infrastructure Readiness Survey*, which was conducted by market research firm Vanson Bourne, interviewed 625 IT decision makers who have a hand in their organization's security structure, including 250 from in the United States and 125 each from France, Germany and the United Kingdom.

Respondents included individuals were from both the public and private sectors, and representatives from organizations concentrating on energy, finance, government and transportation.

"Critical infrastructure organizations are under constant cyber attack, yet no publicly apparent, massive outage has occurred so far," the report stated. Yet, "Energy producers, financial services, transportation companies, telecommunications companies and governments are all potential targets."

According to the survey report, security executives' confidence in their organization's cybersecurity posture is rising as threats are escalating. Surprisingly, however, respondents did not make a connection between threat escalation and their own organization's vulnerability.

The report revealed 75 percent of respondents are either confident or extremely confident in their organization's cyber attack identification protocol, while 68 percent are confident in mitigation techniques and 65 percent are confident in deflection standards.

Respondents believe their own vulnerability to cyber attacks has decreased over the last three years, with only 27 percent feeling very or extremely vulnerable -- compared to 50 percent three years ago.

"According to respondents, attack volume is increasing, security breaches are becoming a frequent occurrence and the rate of code vulnerabilities shows no signs of abating," the report stated. "Yet, respondents across all countries and sectors in the survey believe their own vulnerability to cyber attack has declined."

This overconfidence raises serious concerns, authorities said. Although many leaders believe proper cyber preparedness elements are in place, the sheer volume of actual threats targeting these organizations shows this confidence may be unfounded, which may be opening these organizations up to serious security incidents.

In many instances, serious breaches are spurred by simple mistakes. Demonstrating that no threat, no matter how small, should be overlooked, the report revealed, "Analysis of security incidents at a variety of organizations shows that many of them were breached due to basic security failures in the face of a determined and persistent attacker."

Despite high confidence in their own defenses, US and French respondents in particular rate a serious cyber attack affecting critical services and causing loss of life as highly likely within the next three years. Respondents from the transportation and energy sectors were more likely than their counterparts in other sectors to deem the possibility of such an attack "likely or highly likely."

However, 64 percent of respondents believe an attack resulting in fatalities has not happened yet because good IT security is already in place.

Respondents maintained that human error remains the number one cause of successful cyber intrusions. No matter what organizations do to strengthen their security postures, individual employees can still fall victim to phishing emails, social engineering and drive-by browser downloads that successfully infect their organizations' networks.

Interestingly, few executives believe that the proliferation of personal devices at work is a prime cause of cyber attacks, despite the priority assigned to bring-your-own device -- BYOD -- issues by cybersecurity companies.



Channels
DHS
DoD/National Defense
Global
Federal/State/Local
FEMA
The Leading Edge Today
US Coast Guard
US National Guard

Focused Topics
Airport & Aviation
Biometrics & ID Management
Border Security
Counternarcotics, Terrorism & Intelligence
Customs & Immigration
Cybersecurity
Emergency Management/Disaster Preparedness
Information Technology
Infrastructure Security
Interoperable Communications
Port & Cargo
Public Health and Safety
Surveillance, Protection & Detection
Transportation
Education and Training

# A Multidimensional Critical State Analysis for Detecting Intrusions in SCADA Systems

A. Carcano, A. Coletta, M. Guglielmi, M. Masera, I. Nai Fovino, and A. Trombetta

***Abstract*—A relatively new trend in Critical Infrastructures (e.g., power plants, nuclear plants, energy grids, etc.) is the massive migration from the classic model of isolated systems, to a system-of-systems model, where these infrastructures are intensifying their interconnections through Information and Communications Technology (ICT) means. The ICT core of these industrial installations is known as Supervisory Control And Data Acquisition Systems (SCADA). Traditional ICT security countermeasures (e.g., classic firewalls, anti-viruses and IDSs) fail in providing a complete protection to these systems since their needs are different from those of traditional ICT. This paper presents an innovative approach to Intrusion Detection in SCADA systems based on the concept of Critical State Analysis and State Proximity. The theoretical framework is supported by tests conducted with an Intrusion Detection System prototype implementing the proposed detection approach.**

***Index Terms*—Critical states, intrusion detection, supervisory control and data acquisition (SCADA) systems.**

## I. Introduction

IN THE LAST YEARS, the use of Information and Communication Technologies (in the following ICT) in industrial systems increased enormously, dramatically impacting their security. In this paper, the focus is on the security of Supervisory Control and Data Acquisition (SCADA) systems. SCADA systems are widely used in industrial installations to control and maintain field sensors and actuators. The basic components characterizing a SCADA system are: a) *Master Terminal Units (MTU)* which present data to the operator, gather data from the field and transmit control signals and b) *Remote Terminal Units (RTU)* which send control signals to the devices under control, acquire data from these devices, receive commands from the MTU and transmit the data to the MTU. The majority of the SCADA vulnerabilities are related to the communication protocols used to exchange commands and data among masters and slaves. Traditional ICT security technologies are not able (as showed in [1]) to effectively protect industrial systems against ad-hoc SCADA-tailored attacks. In this work, a novel approach for detecting ICT attacks to SCADA systems based on the concept of *Critical State Analysis* is proposed. The following arguments are at the basis of this approach: 1) Because of the consequence of potential incidents, industrial systems are subject of safety analysis processes, therefore the possible critical states are well documented. Moreover, these critical states can be considered, for minimal subsystems, finite in number, and known in advance. 2) An attacker aiming at damaging an industrial system has to interfere with the state of the installation, i.e., forcing a transition of the system from a safe state to a critical state. 3) By monitoring the evolution of the plant process states, and tracking down when the industrial process is entering into a critical state, it would be possible to detect those attack patterns (known or unknown) aiming at putting the process system into a known critical state by using chains of licit commands. 4) In SCADA architectures, the major cyberattack vector is the flow of network commands. Since the proposed IDS keeps track of the chain of packets driving the system into a critical state (storing details about such packets in a remote database and using the Critical State Distance Metric as trigger for logging a chain of packets), it is possible to discriminate between critical states due to cyberattacks and critical states due to faults/physical attacks. This approach has been introduced to cover the inability of traditional IDS techniques in detecting particular types of SCADA attacks based on chains of licit commands. For that reason, it can be considered as an additional feature, which can highly contribute to increase the detection accuracy of existing IDS.

Manuscript received April 30, 2010; revised August 06, 2010 and October 29, 2010; accepted November 25, 2010. Date of publication January 10, 2011; date of current version May 06, 2011. Paper no. TII-10-04-0097.

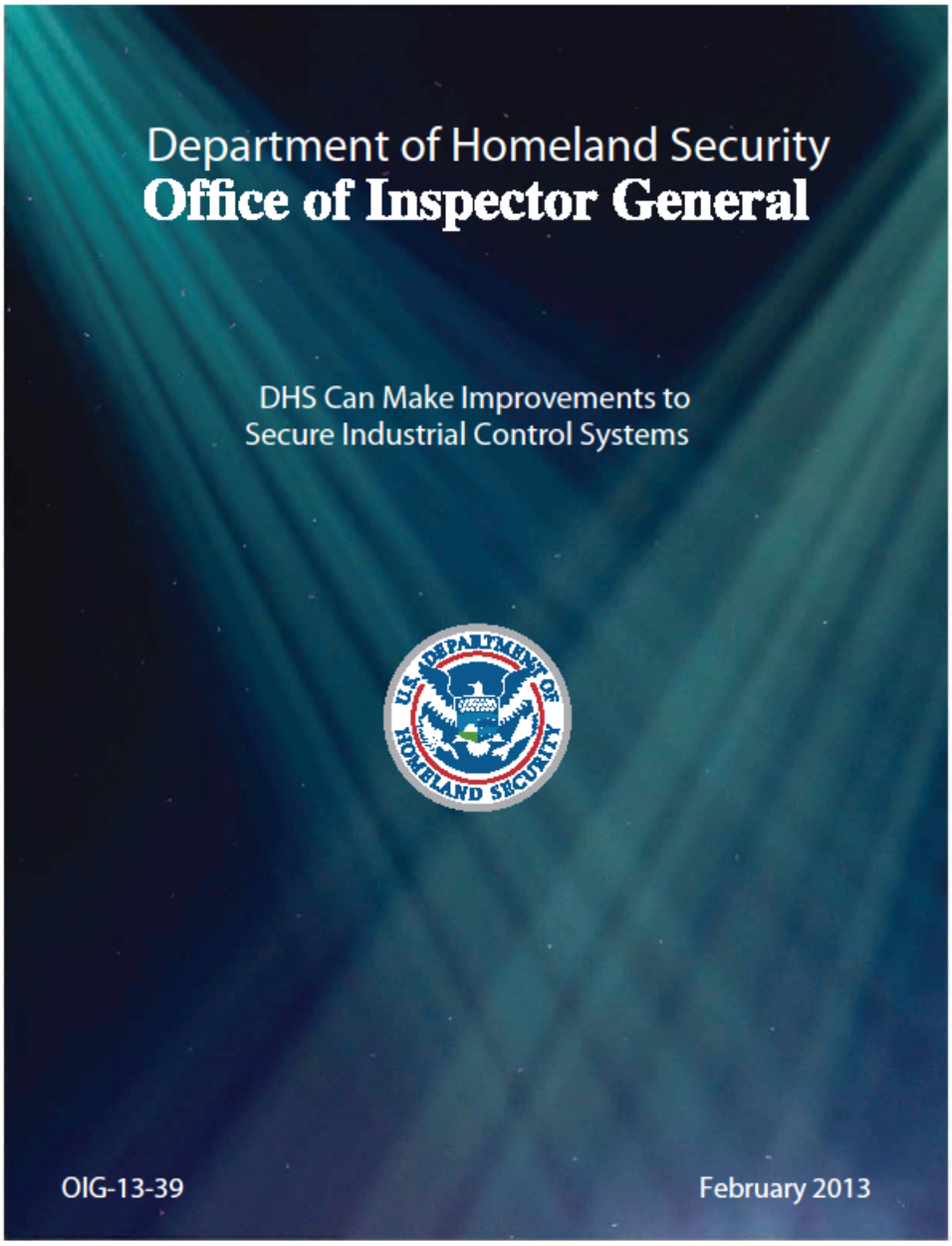
A. Carcano, M. Guglielmi, and A. Trombetta are with the Department of Computer Science, Insubria University, Via Ravasi 1, 21100 Varese, Italy.

A. Coletta, M. Masera, and I. Nai Fovino are with the Institute for the Protection and Security of the Citizen, Joint Research Centre, Via E. Fermi 1, 21027 Ispra, Italy (e-mail: igor.nai@gmail.com).

Digital Object Identifier 10.1109/TII.2010.2099234

## II. Related Work

Intrusion Detection is a well established field of research. In the case of SCADA systems, however, only recently a set of ad-hoc rules and preprocessing modules [2] have been released with the capacity of detecting some attacks to SCADA protocols. With these rules a Network Intrusion Detection System (NIDS) would be able to identify single packet-based attacks; however SCADA attacks are rarely based on the exploitation of a single (see [1] and [7]–[9]); consequently, an *attack correlation* mechanism would be needed. Gross *et al.* [3] proposed a mechanism for collaborative intrusion detection ("selecticast") that uses a centralized server in order to dispatch among the ID sensors information about activities deriving from suspicious IP addresses. This approach is useful for providing a broader picture regarding suspicious events happening in the monitored system. However, it does not provide any kind of specific technique for identifying high level and complex malicious actions. Ning *et al.* [6] proposed a model aiming at identifying causal relationships between alerts on the basis of prerequisites and consequences. The approach proposed by Cuppens and Miege in [5] adopts pre- and postconditions; unfortunately this technique can generate spurious correlation rules, increasing the noise in the IDS alerting system. Looking instead at security solutions for industrial settings and SCADA systems, Nai *et al.* presented a first embryonic IDS for SCADA protocol [10] in


Department of Homeland Security
Office of Inspector General
DHS Can Make Improvements to
Secure Industrial Control Systems
OIG-13-39
February 2013

# A Survey of SCADA and Critical Infrastructure Incidents

Bill Miller
Brigham Young University
Information Technology Program
Provo, Utah
+1 (801) 422 1985
bill_miller@byu.edu

Dale C. Rowe Ph.D
Brigham Young University
Information Technology Program
Provo, Utah
+1 (801) 422 6051
dale_rowe@byu.edu

## ABSTRACT
In this paper, we analyze several cyber-security incidents involving critical infrastructure and SCADA systems. We classify these incidents based on Source Sector, Method of Operations, Impact, and Target Sector. Using this standardized taxonomy we can easily compare and contrast current and future SCADA incidents.

## Categories and Subject Descriptors
C.2.0 [**Computer-Communication Networks**]: General — Security and Protection.

## General Terms
Documentation, Security.

## Keywords
SCADA, Critical infrastructure, Security, Cyber security, Information assurance and security, Cyber attack, Incident response.

## 1. INTRODUCTION
Supervisory Control and Data Acquisition (SCADA) systems are used in many Critical Infrastructure applications. These applications are increasingly becoming the targets of cyber-attacks.

Historically, SCADA systems relied on air-gapped networks and non-standard protocols to protect them from attack. Increasingly, these networks have been connected to corporate networks and thus, the internet. There have also been advances in using standard networking protocols for communications [1].

These changes have made SCADA systems more available for attackers to target from anywhere in the world. The critical nature of these systems also makes these intriguing targets. For the first time, attacks in cyberspace can have physical manifestations in the real world. This presents a valuable and in many instances, easy to access target to those who desire to cause disruption to physical services for whatever motive. These factors have combined to increase the number of attacks against SCADA systems.


*SIGITE'12*, October 11–13, 2012, Calgary, Alberta, Canada.


In order to prepare to defend against future attacks against critical infrastructure, it is necessary to understand how these attacks have been carried out in the past. In this paper, we will discuss a sampling of these historical attacks and classify them by factors that allow us to analyze these attacks along with their targets and sources. This analysis will allow us to more clearly understand the nature of these attacks and how they may be carried out in the future.

## 2. CLASSIFICATION OF INCIDENTS
For the purposes of this paper, we use a modified version of the taxonomy presented by Kjaerland to classify attacks based on 'Source Sectors', Method of Operation (MO)', 'Impact', and 'Target Sectors' [5]. Each facet of the classification can be broken down into the terms shown in Table 1 and are subsequently explained.

**Table 1: Taxonomy** [5]

| Source Sectors | Method of Operation(MO) | Impact | Target Sectors |
|---|---|---|---|
| Com | Misuse of Resources | Disrupt | Com |
| Gov | User Compromise | Distort | Gov |
| Edu | Root Compromise | Destruct | Intl |
| Intl | Social Engineering | Disclosure | |
| User | Virus | Death | |
| Unknown | Web Compromise | Unknown | |
| | Trojan | | |
| | Worm | | |
| | Recon | | |
| | Denial of Service | | |
| | Other Sys Failure | | |

### 2.1 Source Sectors
Source of the incident if explicitly identified (all sectors refer to US sites, except Intl.).

*Com* – Denotes a commercial source (including consumer products, industry, small business).

*Gov* – Denotes local or national government (including buildings/housing, emergency services, public benefits, social services, state and federal government, taxes, tribal governments, worker protections, environment, military).

*Edu* – Denotes a postsecondary school.

*Intl* – Denotes a Non-US entity.

*User* – Denotes an individual user.

# A Taxonomy of Cyber Attacks on SCADA Systems

Bonnie Zhu, Anthony Joseph, Shankar Sastry
*Department of Electrical Engineering and Computer Sciences*
*University of California at Berkeley, CA*
{bonniez,adj,sastry}@eecs.berkeley.edu

***Abstract*—Supervisory Control and Data Acquisition (SCADA) systems are deeply ingrained in the fabric of critical infrastructure sectors. These computerized real-time process control systems, over geographically dispersed continuous distribution operations, are increasingly subject to serious damage and disruption by cyber means due to their standardization and connectivity to other networks. However, SCADA systems generally have little protection from the escalating cyber threats. In order to understand the potential danger and to protect SCADA systems, in this paper, we highlight their difference from standard IT systems and present a set of security property goals. Furthermore, we focus on systematically identifying and classifying likely *cyber attacks* including cyber-induced *cyber-physical attacks* on SCADA systems. Determined by the impact on control performance of SCADA systems, the attack categorization criteria highlights commonalities and important features of such attacks that define unique challenges posed to securing SCADA systems versus traditional Information Technology (IT) systems.**

***Keywords*-SCADA; Cyber-Physical Systems; Cyber Attacks;**

## I. Introduction

The utilization of *Supervisory Control and Data Acquisition* (SCADA) systems facilities the management with remote access to real-time data and the channel to issue automated or operator-driven supervisory commands to remote station control devices, or *field devices*. They are the underlying control system of most critical national infrastructures including power, energy, water, transportation, telecommunication and are widely involved in the constitutions of vital enterprises such as pipelines, manufacturing plants and building climate control.

Remote locations and proprietary industrial networks used to give SCADA system a considerable degree of protection through isolation [16], [29]. Most industrial plants now employ networked process historian servers for storing process data and other possible business and process interfaces. The adoption of Ethernet and transmission control protocol/Internet protocol TCP/IP for process control networks and wireless technologies such as IEEE 802.x and Bluetooth has further reduced the isolation of SCADA networks. The connectivity and de-isolation of SCADA system is manifested in Figure 1.

This work is supported by the National Science Foundation Award CCF-0424422 for the Team for Research in Ubiquitous Secure Technology (TRUST).

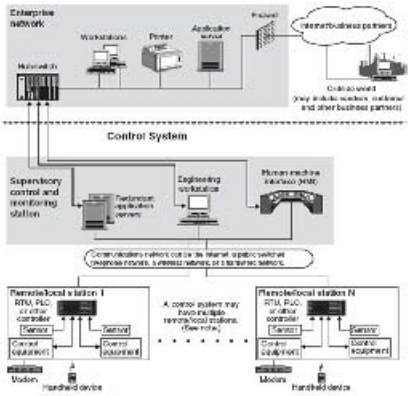



Figure 1. Typical SCADA Components Source: United States Government Accountability Office Report. GAO-04-354 [29]

Furthermore, the recent trend in standardization of software and hardware used in SCADA systems makes it even easier to mount SCADA specific attacks. Thus the security for SCADA systems can no longer rely on obscurity or on being a function of locking down a system.

These attacks can disrupt and damage critical infrastructural operations, cause major economic losses, contaminate ecological environment and even more dangerously, claim human lives.

The British Columbia Institute of Technologys Internet Engineering Lab (BCIT/IEL) maintains an industrial cyber security incident database [4] with more than 120 incidents logged since the initiation. Baker et al at McAfee in their 2011 sequel report [3] surveyed 200 IT security executives in 14 counties from critical electricity infrastructure enterprises, where SCADA systems are widely used, and found out most facilities have been under cyber attacks.

Being one of most sophisticated SCADA malware known

# Advanced Key-Management Architecture for Secure SCADA Communications

Donghyun Choi, *Student Member, IEEE*, Hakman Kim, Dongho Won, and Seungjoo Kim, *Member, IEEE*

***Abstract*—Supervisory control and data-acquisition (SCADA) systems are control systems for many national infrastructures. In the past, SCADA systems were designed without security functionality because of the closed operating environment. However, the security of SCADA systems has become an issue with connection to open networks becoming more common. Any damage to the SCADA system can have a widespread negative effect to society. In this paper, we review constraints and security requirements for SCADA systems and then investigate whether the existing key-management protocols for the SCADA systems satisfy these requirements. Afterward, we propose an advanced key-management architecture fitted for secure SCADA communications. The contributions of our work are two-fold. First, our scheme supports both message broadcasting and secure communication. Second, by evenly spreading much of the total amount of computation across high power nodes (MTU or SUB-MTU), our protocol avoids any potential performance bottleneck of the system while keeping the burden on low power nodes (RTU) at minimal.**

***Index Terms*—Key management, power system security, supervisory control and data-acquisition (SCADA) systems.**

## I. Introduction

SCADA (Supervisory Control And Data Acquisition) systems are control system for many national infrastructures. In the past, the SCADA systems used proprietary communication mechanisms. Nowadays, the SCADA systems increasingly use standard protocols, such as DNP3 [1].

The use of standard protocols, combined with increased interconnectivity with other networks, has exposed them to wide range of network security problems. Thus the SCADA systems can be vulnerable to a variety of attacks. Successful attacks on the SCADA systems could have devastating consequences, such as endangering public health and safety [2]. In other words, any damage to the SCADA system can have a widespread negative effect to society. To prevent the damage, several professional organizations have been researching the security of SCADA systems. As the results of this research, the organizations have been developing several standards and reports. We provide a brief overview of this work.

Manuscript received June 27, 2008; revised July 30, 2008. First published May 02, 2009; current version published June 24, 2009. This work was supported by the Ministry of Knowledge Economy, Korea, under the Information Technology Research Center support program supervised by the Institute of Information Technology Advancement under Grants IITA-2008-C1090-0801-0028 and IITA-2008-C1090-0801-0016. Paper no. TPWRD-00488-2008.

D. Choi, D. Won, and S. Kim are with the Information Security Group, Sungkyunkwan University, Gyeonggi-do 440-746, Korea (e-mail: dhchoi@security.re.kr; dhwon@security.re.kr; skim@security.re.kr).

H. Kim is with the Department of Electrical Engineering, Incheon City College, Incheon 402-808, Korea (e-mail: hmkim7@icc.ac.kr).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TPWRD.2008.2005683

ISA (Instrumentation Systems and Automation)-SP99 committee released two technical reports on the SCADA systems security. The first report ANSI/TSA-TR99.00.01-2007 [4] focuses on the security technologies of manufacturing and control systems. The second report ANSI/ISA-TR99.00.02-2004 [5] addresses the integration of security components in manufacturing and control system environments. The goal of these documents is to provide security guidelines to people in the SCADA industry.

NIST (National Institute for Standards and Technology) produced a PP (Protection Profile) for the SCADA systems [6]. The PP aims to define the minimum security requirements.

API (American Petroleum Institute) released API-1164 Pipeline SCADA Security Standard [8]. This standard provides guidelines, operator checklist and a security plan template for system integrity and security.

AGA (American Gas Association) produced a standard for effective implementation of cryptographic functions on SCADA networks to protect communications. The AGA-12 part 1 describes cryptographic system requirements and test planning for security devices [9]. The AGA-12 part 2 discusses retrofitting serial communications and encryption of serial communication channels [10].

In this paper, we review security requirements based on fore mentioned standards and reports for the SCADA systems. According to the security requirements, most SCADA systems require message broadcasting and secure communications. In this context, several key-management schemes were suggested. The SANDIA report proposed a key establishment for SCADA systems (SKE) [11] and Robert *et al.* proposed the SCADA key-management architecture (SKMA) [12]. However, although the existing key-management schemes for SCADA systems provide secure unicast communications, these schemes do not support secure message broadcasting. Therefore, we propose a key-management protocol to support both message broadcasting and secure communications. Moreover, by evenly spreading much of the total amount of computation across high power nodes (MTU or SUB-MTU), our protocol avoids any potential performance bottleneck of the system while keeping the burden on low power nodes (RTU) minimal.

The rest of this paper is organized as follows. Section II describes the SCADA architecture. Section III introduces security requirements for the SCADA system. The summary of related work appears in Section IV. We propose a key-management protocol for the SCADA systems in Section V. In Section VI, we compare with the existing key-management protocols and show security analysis. Finally, Section VII concludes this work.

Forbes http://onforb.es/1zKFEy3



Capital FlowsContributor
*Guest commentary curated by Forbes Opinion.*

OPINION 11/11/2014 @ 6:07PM | 7,940 views

# America's Critical Infrastructure Is Vulnerable To Cyber Attacks

GUEST POST WRITTEN BY
**Michael Assante**
*Mr. Assante is director of Industrial Control Systems as well as Supervisory Control and Data Acquisition Networks for the SANS Institute.*



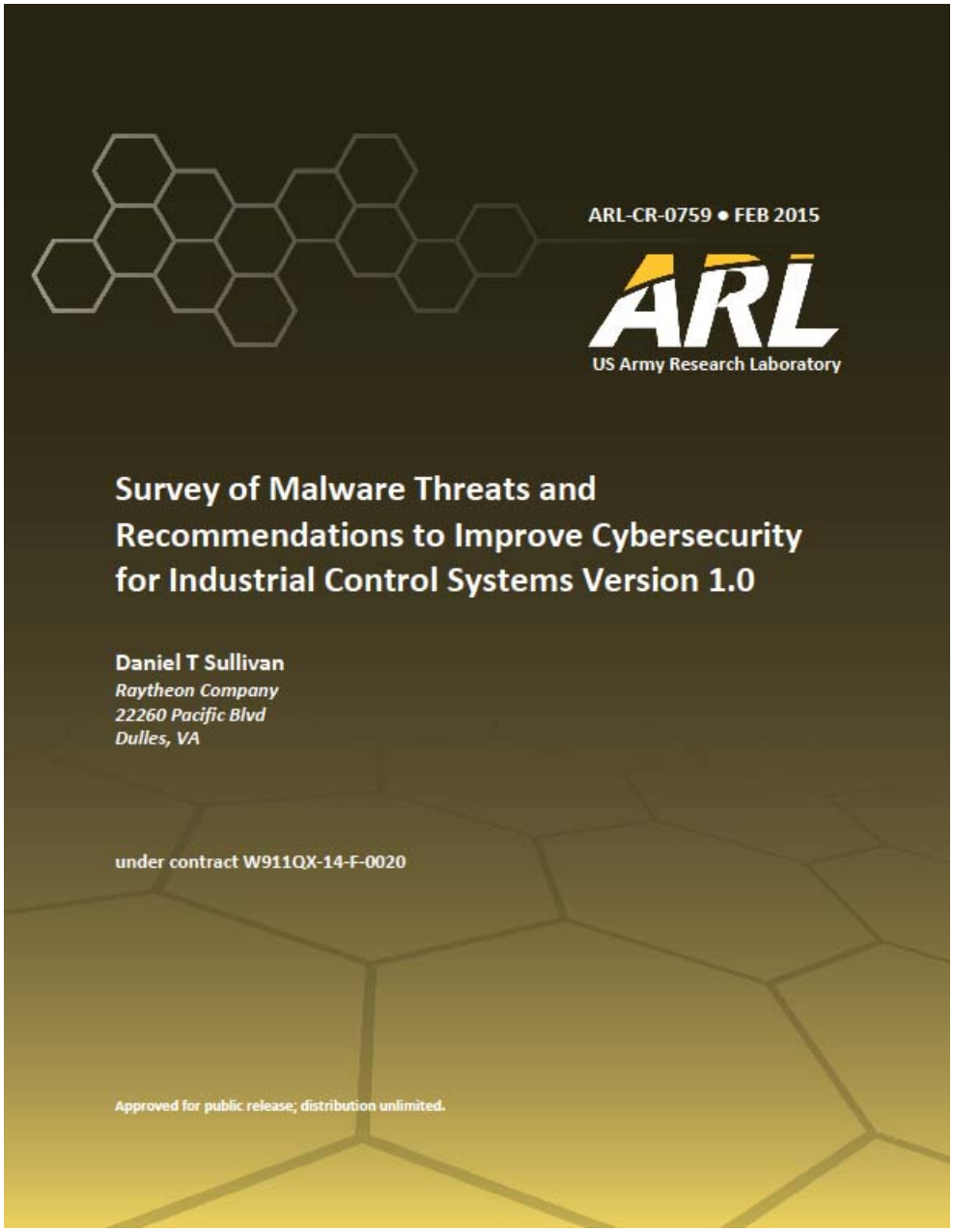
America's critical infrastructure—the utilities, refineries, military defense systems, water treatment plants and other facilities on which we depend every day—has become its soft underbelly, the place where we are now most vulnerable to attack.

Over the past 25 years, hundreds of thousands of analog controls in these facilities have been replaced with digital systems. Digital controls provide facility operators and managers with remote visibility and control over every aspect of their operations, including the flows and pressures in refineries, the generation and transmission of power in the electrical grid, and the temperatures in nuclear cooling towers. In doing so, they have made industrial facilities more efficient and more productive.

But the same connectivity that managers use to collect data and control devices allows cyber attackers to get into control system networks to steal sensitive information, disrupt processes, and cause damage to equipment. Hackers, including those in China, Russia and the Middle East, have taken notice. While early control system breaches were random, accidental infections, industrial control systems today have become the object of targeted attacks by skilled and persistent adversaries.

**Industrial control systems are being targeted**

The recently discovered Industrial Control System modules of the HAVEX trojan are one example. The malware infiltrated an indeterminate number of critical facilities by attaching itself to software updates distributed by control system manufacturers. When facilities downloaded the updates to their network, HAVEX used open communication standards to collect information from control devices and send that information to the attackers for analysis. This type of attack


ARL-CR-0759 • FEB 2015
ARL
US Army Research Laboratory
Survey of Malware Threats and Recommendations to Improve Cybersecurity for Industrial Control Systems Version 1.0
Daniel T Sullivan
Raytheon Company
22260 Pacific Blvd
Dulles, VA
under contract W911QX-14-F-0020
Approved for public release; distribution unlimited.

INTERNATIONAL JOURNAL OF CRITICAL INFRASTRUCTURE PROTECTION 2 (2009) 170–178

available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/ijcip

# Critical infrastructure dependency assessment using the input–output inoperability model

*Roberto Setola*[a,*], *Stefano De Porcellinis*[a], *Marino Sforna*[b]

[a] *Complex Systems and Security Laboratory, University Campus BioMedico, Rome, Italy*
[b] *TERNA – Italian Transmission System Operator, Rome, Italy*

ARTICLE INFO

*Article history:*
Received 26 November 2008
Received in revised form
30 July 2009
Accepted 17 September 2009

*Keywords:*
Inoperability input–output model (IIM)
Complex systems
Interdependencies
Impact analysis
Influence analysis

ABSTRACT

The input–output inoperability model (IIM) is a simple, but powerful, mechanism for analyzing the cascading effects induced by critical infrastructure dependencies and interdependencies. IIM typically uses financial data as a measure of the dependency phenomena. Since financial data is only one of the many dimensions for analyzing dependency phenomena, the quality of IIM parameters and, thus, the reliability of IIM results can be affected negatively. This paper proposes a methodology for evaluating IIM parameters based on technical and operational data. The data is collected by interviewing experts and is processed using a fuzzy set based methodology. A case study involving Italian critical infrastructure sectors is used to demonstrate the effectiveness of the methodology.



## 1. Introduction

Technological and organizational infrastructures are the pulsating heart of developed countries. In order to improve their ability to provide goods and services efficiently and cost-effectively, infrastructures within a country and infrastructures in different countries must interact with one another at various levels. However, these interactions increase infrastructure dependencies, rendering the entire system extremely complex and prone to "domino failures".

Several accidents have occurred that underscore the significance of infrastructure dependencies. The 1998 failure of the Galaxy IV satellite system degraded US telecommunications services, resulting in cascading effects in other infrastructures. About 40 million pagers ceased working. More than twenty United Airlines flights were delayed due to the lack of high-altitude weather data. Interestingly, the road transportation infrastructure was also affected because highway refueling stations were unable to process credit cards as their satellite links were down.

In 2004, the failure of a service plant for an important Telecom Italia node in Rome shut down fixed and mobile telecommunications services for several hours. The outage affected the financial infrastructure (5000 bank branches and 3000 post offices lost connectivity) and air transportation. (70% of the check-in desks at Rome's Fiumicino airport were forced to use manual procedures, resulting in numerous flight delays.)

These and other incidents (see, e.g., [1]) illustrate the significance of dependencies existing between critical infrastructures. Critical infrastructures are complex, non-linear, geographically-dispersed clusters of systems, and the task of

* Corresponding author.
E-mail address: r.setola@unicampus.it (R. Setola).

1874-5482/$ - see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.ijcip.2009.09.002

The Economist

Special report:
Cyber-security

Critical infrastructure

# Crashing the system

**How to protect critical infrastructure from cyber-attacks**

Jul 12th 2014 | From the print edition

IN THE HIGH desert some 50 miles west of Idaho Falls, the terrain is so rugged that the vehicle in which your correspondent was touring the facilities at Idaho National Laboratory (INL) ended up with two shredded tyres. Originally set up in the 1940s to test naval artillery, the high-security government lab now worries about weapons of a different kind. Some of its elite engineers help protect power grids, telecoms networks and other critical infrastructure in America against cyber-attacks and other threats.

The lab boasts its own 61-mile (98km) electrical grid and seven substations. It also has a wireless network and an explosives test bed. These can all be used by government agencies and businesses to run experiments that would be hard or impossible to conduct in an operational setting. "There are not many places in the world where you can crash a power system without incident," says Ron Fisher, who oversees the Department of Homeland Security's programme office at the lab.

The tour covers the site of a 2006 experiment that subsequently got a lot of attention. Known as the Aurora test, it demonstrated how it was possible to launch a cyber-attack on a big diesel generator by exploiting a weakness in a supervisory control and data acquisition (SCADA) system. Such systems are used to monitor and control physical equipment in everything from power stations to water-treatment plants. In a video of the attack on YouTube, bits can be seen flying off the generator, followed by black smoke.

Teams from the INL and other engineers have since been advising utilities on how to secure SCADA systems. Many of these were designed to work in obscurity on closed

MarketWatch

# New Survey Reveals Critical Infrastructure Cybersecurity Challenges

By
Published: July 20, 2015 12:01 a.m. ET

## Aspen Institute, Intel Security Critical Infrastructure Survey Shows 86% of Respondents Want More Public-Private Cooperation; Of Those who Experienced Cyberattacks, 59% Reported Physical Damage

ASPEN, Colo., Jul 20, 2015 (BUSINESS WIRE) -- Information technology (IT) executives within critical infrastructure organizations see a need for public-private threat intelligence sharing partnerships (86% of respondents) to keep pace with escalating cybersecurity threats, according to a survey released today by The Aspen Institute and Intel Security. A majority (76%) of survey respondents also indicated they believe a national defense force should respond when a cyber attack damages a critical infrastructure company within national borders. Additionally, although most respondents agree that threats to their organizations are on the rise, they maintain a high degree of confidence in existing security.

The survey *Holding the Line Against Cyber Threats: Critical Infrastructure Readiness Survey*, reveals that the critical infrastructure providers surveyed are pleased with the results of their efforts to improve cybersecurity over the last three years, but at the same time many (72%) said that the threat level of attacks was escalating. Almost half of all respondents (48%) believe it is likely that a cyberattack on critical infrastructure, with the potential to result in the loss of human life, could happen within the next three years.

"This data raises new and vital questions about how public and private interests can best join forces to mitigate and defend against cyberattacks," said Clark Kent Ervin, Director, Homeland Security Program, Aspen Institute. "This issue must be addressed by policymakers and corporate leaders alike."

Survey results suggest there may be a disconnect between critical infrastructure providers and the current threat landscape:

- **Perceived Improvements**: Respondents believe their own vulnerability to cyberattacks has decreased over the last three years. When asked to evaluate their security posture in retrospect, 50% reported that they would have considered their organizations "very or extremely" vulnerable three years ago; by comparison, only 27% believe that their organizations are currently "very or extremely" vulnerable.
- **Government Involvement Encouraged**: Private industry is often hesitant when it comes to government's involvement in private sector business; however, 86% of respondents believe that cooperation between the public and private sectors on infrastructure protection is critical to successful cyber defense. Furthermore, 68% of respondents believe their own government can be a valuable and respectful partner in cybersecurity.
- **Confidence in Current Solutions**: Sixty-four percent believe an attack resulting in fatalities has not happened yet because good IT security is already in place. Correspondingly, more than four in five are satisfied or extremely satisfied with the performance of their own security tools such as endpoint protection (84%), network firewalls (84%), and secure web gateways (85%).
- **Disruptions Increasing**: More than 70% of respondents think the cybersecurity threat level in their organization is escalating. Around nine in ten (89%) respondents experienced at least one attack on a system within their organization, which they deemed secure, over the past three years, with a median of close to 20 attacks per year. Fifty-nine percent of respondents stated that at least one of these attacks resulted in physical damage.
- **Loss of Life?**: Forty-eight percent of respondents believe it is likely that a cyberattack that will take down critical infrastructure with potential loss of life will occur within the next three years, although there were no additional survey questions to determine the circumstances under which respondents believed the loss of life could occur. More US respondents thought this scenario was "extremely likely" to occur than did their European counterparts.

INTERNATIONAL JOURNAL OF CRITICAL INFRASTRUCTURE PROTECTION 10 (2015) 47–58

Available online at www.sciencedirect.com

ScienceDirect

www.elsevier.com/locate/ijcip

# Constructing cost-effective and targetable industrial control system honeypots for production networks

*Michael Winn*[a], *Mason Rice*[a,*], *Stephen Dunlap*[a], *Juan Lopez*[b], *Barry Mullins*[a]

[a]Department of Electrical and Computer Engineering, Air Force Institute of Technology, Wright-Patterson Air Force Base, OH 45433, USA

[b]Applied Research Solutions, 51 Plum Street, Beavercreek, OH 45440, USA

ARTICLE INFO

*Article history:*
Received 11 January 2015
Received in revised form
1 April 2015
Accepted 15 April 2015
Available online 1 May 2015

*Keywords:*
Industrial control systems
Programmable logic controllers
Production networks
Honeypots

ABSTRACT

Critical infrastructure assets – and especially industrial control systems – are at risk. Malicious actors are constantly developing exploits that sneak past security controls. Honeypots offer an opportunity to acquire knowledge about the tactics, techniques and procedures used by malicious entities to compromise sensitive systems. However, the proprietary, and often expensive, hardware and software used by industrial control systems make it very challenging to build flexible, economical and scalable honeypots. This paper describes a technique that uses proxy technology to produce multiple high-interaction honeypots using a single programmable logic controller. The technique provides a cost-effective method for distributing multiple, authentic, targetable honeypots at slightly more than the cost of a single programmable logic controller.

Published by Elsevier B.V.

## 1. Introduction

On November 20, 2014, the Director of the National Security Agency, Admiral Michael Rogers, stated that several entities, including China, Russia and others, have the ability to disrupt electric utilities and other energy assets throughout the United States, potentially causing physical destruction, personal injury and even death [4]. Admiral Rogers expressed the desire to share threat information with the private sector, but he also implied that the private sector lacks the ability to collect data that could help prevent, detect and recover from cyber attacks. This is due, in part, to the reliance of IP-based protection devices such as intrusion detection systems and firewalls.

Further compounding the problem, malicious actors have a good understanding of current signature-based sensor technologies and can engineer malware that eludes such systems, making their activities almost undetectable. A honeypot is a proven method for learning about attacker tactics, techniques and procedures. However, the financial cost of implementing practical honeypots in industrial control networks is a major barrier.

This paper presents a technique for constructing low-cost industrial control system honeypots that are both authentic and targetable. The following section describes the background and establishes the context for the honeypot technique. Next, the technique involving the use of proxy technology is developed and the evaluation methods are described. Finally, the results of the evaluation are presented, along with the main conclusions and directions for further research.

## 2. Background

Successful honeypots balance authenticity, targetability, cost and risk. An authentic honeypot mimics the features of an operational system. More realistic features yield a more complex honeypot

*Corresponding author.
E-mail address: mason.rice@afit.edu (M. Rice).

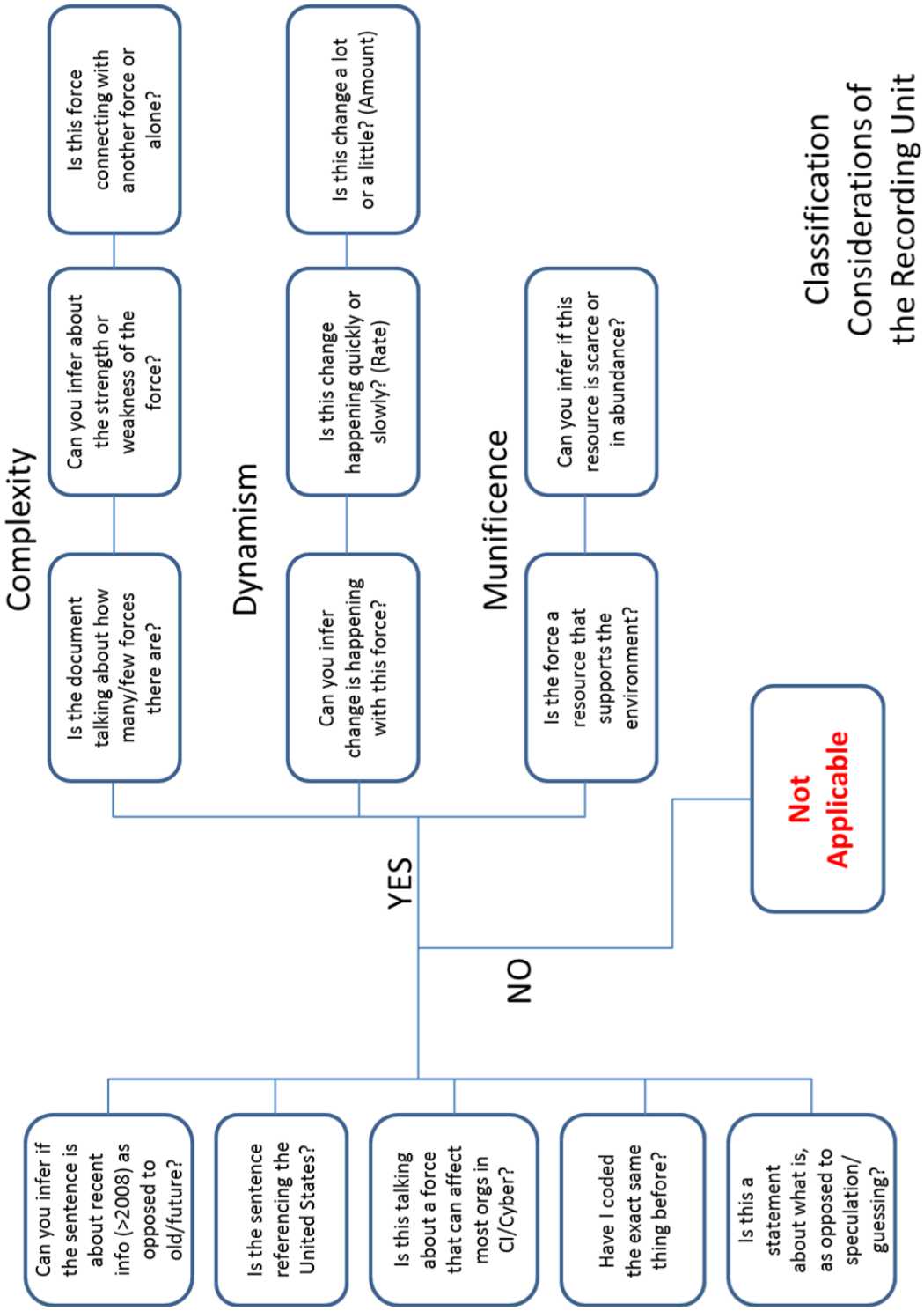
http://dx.doi.org/10.1016/j.ijcip.2015.04.002
1874-5482/Published by Elsevier B.V.

## Appendix B. Artifacts Meeting Selection Criteria

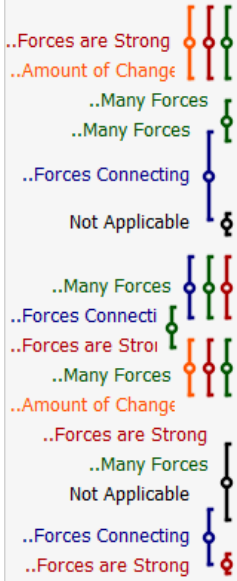
A A Survey of SCADA and Critical Infrastructure Incidents
A A Taxonomy of Cyber Attacks on SCADA Systems
A A Web-Based Remote Lab for SCADA
A Advanced Key for Secure SCADA
A Capabilities of Dynamic Reconfiguration MB ICS
A CI Dependency Assessment
A Creating a Cyber Moving Target for CI
A Critical Infrastructure Dependencies
A Cyber CI Protect Payload Anomaly Detection
A Cyber Security Risk Assessment for SCADA and DCS Networks 2007 ISA Transactions
A Decentralized Risk Management CI
A Detecting Intrusions in SCADA Systems
A Event Triggered Strat IC S
A FPGAs in Industrial Control Applications
A GSM SMS Based Monitoring Control Systems
A Improving Security for SCADA Control Systems
A Intrusion Detection in SCADA
A Methodologies and Applications for CI
A Network Intrusion Detection M0DBUS ICS
A Networked Control System Overview and Research Trends
A Probabilistic Risk in CI
A Public Private CI
A Rethinking Security Properties SCADA
A SCADA Security in Light of Cyber Warfare
A SCADA Testbed
A Security lssues in SCADA Networks
A Security Retrofit for SCADA
A Security Strategies for SCADA Networks
A State of the Art in CI Protection
A Stealthy Deception Attacks on Water SCADA Systems
A The Cyber Threat Landscape Challenges and Future Research Directions Computers Security
A The SCADA Challenge Securing Critical Infrastructure 2009 Network Security
A Wind Turbines SCADA
A Winn Honeypots
P Americas CI is vulnerable to Cyber Forbes
P Automation World scada-attacks-double-2014
P Crashing the System CI The Economist

P Critical Infrastructure Security Vulnerability Tripwire
P CSIS Insuring ICS Security
P Cyberattacks Escalate CI Homeland Sec Today
P DHS Phishing CI The Hill
P In the Crossfire
P McAfee In the Dark Private CI View
P McAfee on CI General
P Protecting the Nations CI from Cyber
P SANS ICS CI Response
P Study Half of CI pros Attack SC Magazine
P Survey Reveals CI Issues
P Trend Micro- Report on Cybersecurity and Critical Infrastructure in the Americas
P Verizon Data Breach
P Verizon Energy CI
G Army Research Lab ICS Security
G CI Assessment Smart Grid Security
G Cyber Threats from CRI Protecting CI
G DHS IG Secure ICS
G DHS Strategy for Securing Control Systems
G DHS Year End Assessment
G Executive Order Improving CI Cybersecurity
G GAO CI Protect Observations
G GAO Maritime CI Protection
G GAO-15-290, High-Risk Series CI
G ICS Summary Report
G Identifying, Understanding, and Analyzing CI Interdepend
G NIST cybersecurity framework
G NIST Guide to ICS Security 2008
G NIST Guide to Industrial Control Systems Security 2011
G PPD CI Security
G Presidential Cyberspace Policy Review

Appendix C. Recording Unit Classification Diagram



# Appendix D. Coded Artifact Example






Forbes http://onforb.es/1zKFEy3



Capital FlowsContributor
*Guest commentary curated by Forbes Opinion.*

OPINION 11/11/2014 @ 6:07PM | 7,940 views

## America's Critical Infrastructure Is Vulnerable To Cyber Attacks

GUEST POST WRITTEN BY
**Michael Assante**
*Mr. Assante is director of Industrial Control Systems as well as Supervisory Control and Data Acquisition Networks for the SANS Institute.*



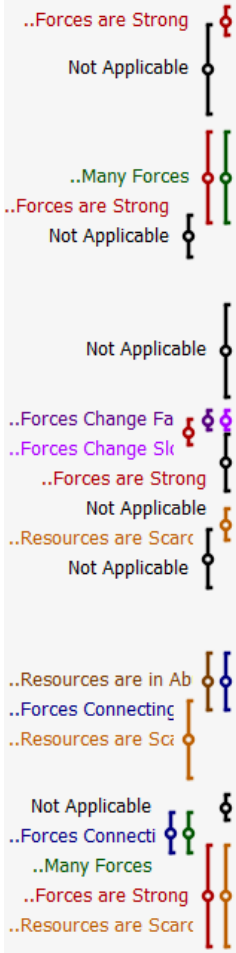
America's critical infrastructure—the utilities, refineries, military defense systems, water treatment plants and other facilities on which we depend every day—has become its soft underbelly, the place where we are now most vulnerable to attack.

Over the past 25 years, hundreds of thousands of analog controls in these facilities have been replaced with digital systems. Digital controls provide facility operators and managers with remote visibility and control over every aspect of their operations, including the flows and pressures in refineries, the generation and transmission of power in the electrical grid, and the temperatures in nuclear cooling towers. In doing so, they have made industrial facilities more efficient and more productive.

But the same connectivity that managers use to collect data and control devices allows cyber attackers to get into control system networks to steal sensitive information, disrupt processes, and cause damage to equipment. Hackers, including those in China, Russia and the Middle East, have taken notice. While early control system breaches were random, accidental infections, industrial control systems today have become the object of targeted attacks by skilled and persistent adversaries.

**Industrial control systems are being targeted**

The recently discovered Industrial Control System modules of the HAVEX trojan are one example. The malware infiltrated an indeterminate number of critical facilities by attaching itself to software updates distributed by control system manufacturers. When facilities downloaded the updates to their network, HAVEX used open communication standards to collect information from control devices and send that information to the attackers for analysis. This type of attack




represents a significant threat to confidential production data and corporate intellectual property and may also be an early indicator of an advanced targeted attack on an organization's production control systems.

Other hacks represent a direct threat to the safety of U.S. citizens. Earlier this year, the FBI released information on Ugly Gorilla, a Chinese attacker who invaded the control systems of utilities in the United States. While the FBI suspects this was a scouting mission, Ugly Gorilla gained the cyber keys necessary for access to systems that regulate the flow of natural gas.

Considering that cyber attackers are numerous and persistent—for every one you see there are a hundred you don't—those developments should sound alarms among executives at companies using industrial controls and with the people responsible for protecting American citizens from attacks. To their credit, both businesses and the U.S. government have begun to take action; however, neither is adequately addressing the core of the issue.

**The threat isn't static**

Businesses continue to believe that cybersecurity issues can be addressed solely through technology. The problem was created by technology so the solution must be more technology, they reason, ignoring the spirit of Einstein's observation that "no problem can be solved from the same level of consciousness that created it."

Technology is static and the threat is not. Hackers will always find a way to beat technology-based solutions. That's why we have to do more than create barriers to keep out intruders. We have to man our digital borders with people who have the same skill and determination as the attackers.

Similar to the use of technology, the ability to regulate a solution is inherently limited. Regulation creates a compliance mentality in which policies and investments are based on achieving and maintaining compliance. Compliance is predictable, which makes it the hacker's best friend.

**Lack in security professionals who understand both digital security and control system technology**

Legislation (HR 3696) has been introduced in the U.S. Congress that would increase the sharing of information related to control system breaches to better arm security professionals to prevent future breaches. That is a worthwhile goal; unfortunately, there is a dire lack of security professionals with an understanding of both digital security and control system technology to benefit from this information sharing.

Filling this gap is where the lion's share of the cybersecurity effort must go. It is estimated in the latest Project SHINE report that the United States has more than half a billion control system devices connected to the Internet. The SANS Institute, the largest cybersecurity training organization in the world, estimates that in the U.S. power industry alone thousands of new or existing control systems security professionals must be deployed or further developed in the next five years to adequately address the challenge of control system security within the electric sector.

**Steps to fill the gap**

Not Applicable

..Resources are in Abun

..Resources are in Ab

Not Applicable

..Resources are in Ab

Not Applicable

Not Applicable

Not Applicable

The first step in that process is defining the baseline of knowledge required by the new breed of security professional who will bridge the gap between control system engineers and information technology security specialists.

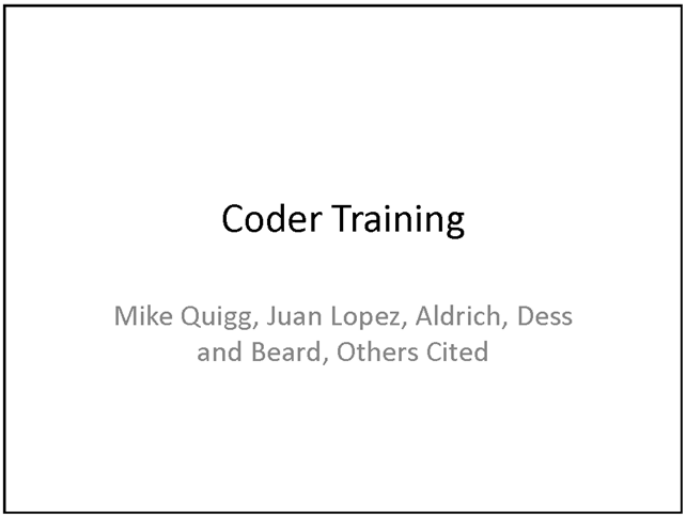
This important first step has already been accomplished with the development of the Global Industrial Cyber Security Professional (GICSP) certification—developed through a joint effort by control system manufacturers, control system users and security specialists. This certification sets a standard that allows organizations at risk to build control system security teams with the confidence that those teams have the knowledge they need to be successful.

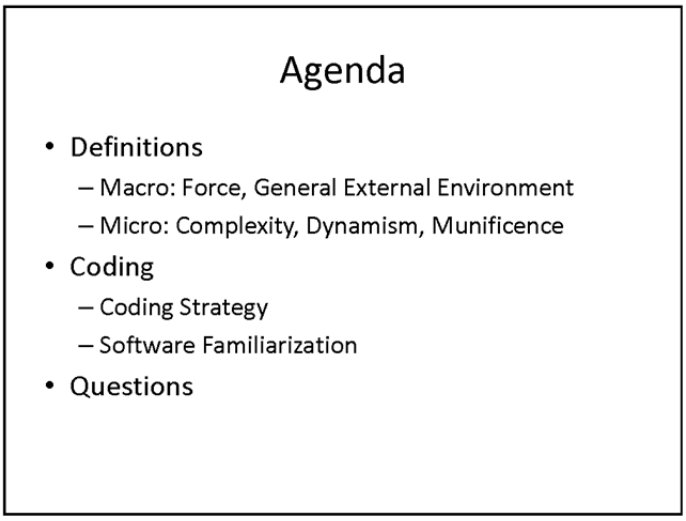
The second step is training. A training infrastructure exists to support information technology security and this infrastructure must now be expanded quickly to prepare a small army of engineers and technologists for GICSP certification. A core group of industry veterans has established the curriculum for such training and the early graduates of these classes are now entering the workforce. The challenge will be scaling quickly to meet the projected need for GICSP-trained professionals while providing continuing education that allows certified professionals to expand their knowledge base and share their experience.

The final step is knowledge sharing. As trained professionals work actively to defend critical control networks they will generate, and benefit from, shared information on vulnerabilities, threats and best practices.

With the certification in place, the focus now needs to be on training. The sooner we reach a critical mass of GICSP-certified professionals, the sooner we will have a determined and dynamic force capable of successfully defending the systems our country and its businesses depend on.

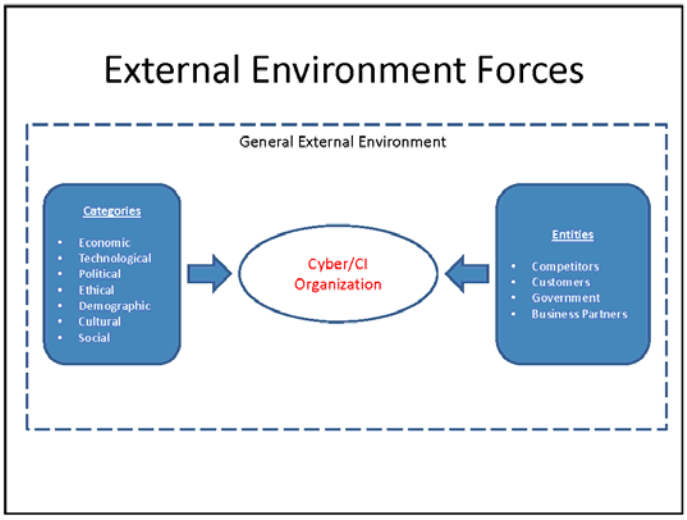
Appendix E. Coder Training Briefing

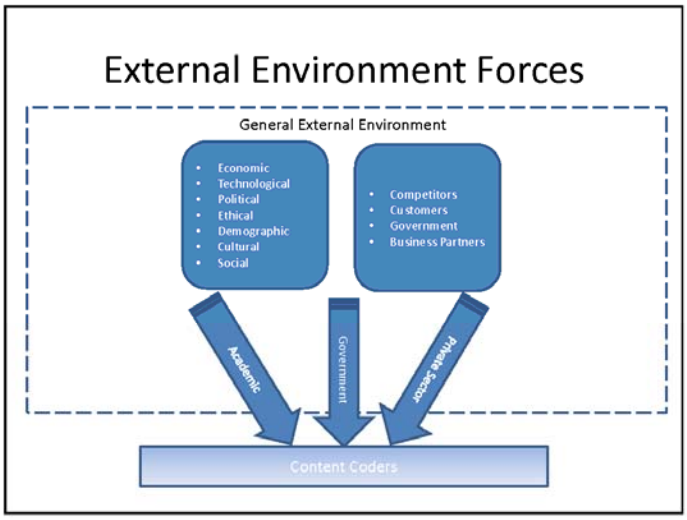


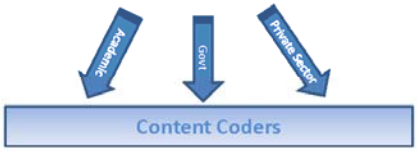
## Macro Definitions

- What is the **General External Environment**? The "relevant physical and social factors outside the boundaries of [an] organization" (Duncan, 1972) which generally effect most organizations within the CI/Cyber domain.
- What is a **Force**? An entity external to CI/Cyber organizations that can effect change in their environment… these factors can be competitors, customers, economic, technological, political, ethical, demographic, cultural and social (Daft, Sormunen, and Parks, 1988; Van de Ven/Ferry 1980, Duncan, 1972)


External Environment Forces
General External Environment
Categories
Economic
Technological
Political
Ethical
Demographic
Cultural
Social
Cyber/CI Organization
Entities
Competitors
Customers
Government
Business Partners


External Environment Forces
General External Environment
Economic
Technological
Political
Ethical
Demographic
Cultural
Social
Competitors
Customers
Government
Business Partners
Academic
Government
Private Sector
Content Coders

## Coding Categories




- ***Munificence*** = Resource Availability
  - (1) Amount
- ***Complexity*** = Presence of external Forces:
  - (1) Strength (strong vs. weak)
  - (2) Number (quantity or numerical)
  - (3) Interconnectedness (corroboration)
- **Dynamism** = Change
  - (1) Amount
  - (2) Speed

## Micro Definitions

## Munificence (Resource Availability)

- **Resource Scarce/Abundant: Is the resource widely available and easy to obtain from several sources?** This relates to amount of resources available to support the ICS/CERT Cyber domain. If the resource is undesirable it is considered in excess. Look for: Fighting over, competing over, few exist, the demand is low, scarce, a lot, a little, etc.
  - "…only two pipelines distribute oil in the U.S. and both are connected to the internet" **Scarce**
  - "…few programmers exist to protect the equipment…"**Scarce**
  - "…money is abundant and available to protect these assets…" **Abundant**
- What is the resource that supports this cyber ICS/CERT environ? The industry resource is not being considered (oil, gas, water, etc.)…only the cyber aspects of CI (programmers, equipment, networked etc.)
- Resources: Key question: Is the document talking about something that supports the environment being in great supply or scarcity…

## Complexity

- **Force Strong/Weak**: Are the forces in this environment strong (opposed to weak)? This relates to strength of forces in the ICS/CI environment. Here are examples of what to look for:
  - Key words like strong, strengthen, weak, weakening.
  - "…China and various other nations are able to disrupt utilities at will…" **Strong**
  - "…few countries currently have the power to cause effects that would harm the US infrastructure" **Weak** (because the external entities aren't strong enough to cause much change)
  - "…the technology is tremendously disruptive to the industry…" **Strong**
  - "…public outcry is forcing serious policy changes" **Strong**
  - "…no one seems to care about CI cyber security so nothing is being done" **Weak**

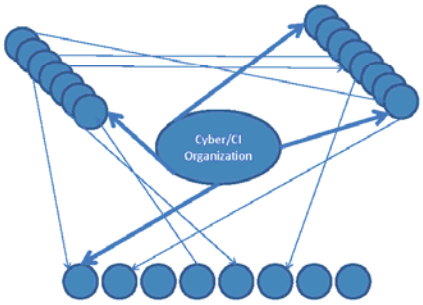
## Complexity

- **Force Many/Few:** Are the forces in this environment many (opposed to few)? This relates to the shear number of forces in the environment. Here is what to look for:
  - "…the amount of companies with critical infrastructure assets is considerable" **Many**
  - "…the U.S. has few enemies that can effect change in critical assets" **Few**
  - " …only a couple of politicians are active in CI/ICS" **Few**
  - "…thousands of attacks penetrated systems last year alone" **Many**
  - "…few countries can exploit CI systems" **Few**

## Complexity

- **Forces Interconnected/Disconnected:** Are the forces in this environment interconnected (opposed to disconnected)? This relates to how forces are interacting in the environment. Look for evidence of things working together or combining.
  - "…governmental and corporate forces are united in their attempts to stall policy…" **Interconnected**
  - "…the hacker worked alone" **Disconnected**
  - "…politicians are working together to solve this problem. **Interconnected**
  - "…power is now networked all over the united states…" **Interconnected**
  - "…no one is talking to each other about the problem" **Disconnected**

## Interconnectedness




## Dynamism

- **Change Amount High/Low**: How much are the forces in the environment changing? This relates to the quantity of change that occurs. Look for: great amount, huge change, little change.
  - "…technological growth is limited throughout the field." **Low**
  - " …the devices across the industry have received little modification." **Low**
  - "…the majority of the public has changed on this issue." **High**
  - "…CI control systems have transformed considerably." **High**
  - "…little is being done to change the status quo." **Low**

## Dynamism

- **Change Fast/Slow:** How quickly do the forces in the environment change over time? This relates to the speed by which change happens. Look for: Fast, slow, quickly
  - "…economic support to ICS has quadrupled in the last 5 years" **Fast**
  - "…the mood of Americans has changed rapidly on this issue" **Fast**
  - "…politicians are moving slowly on protection laws" **Slow**
  - "…in just a few months CI has had five new policy revisions to security" **Fast**
  - "…the same policy exists to protect these systems from before they were networked" **Slow**

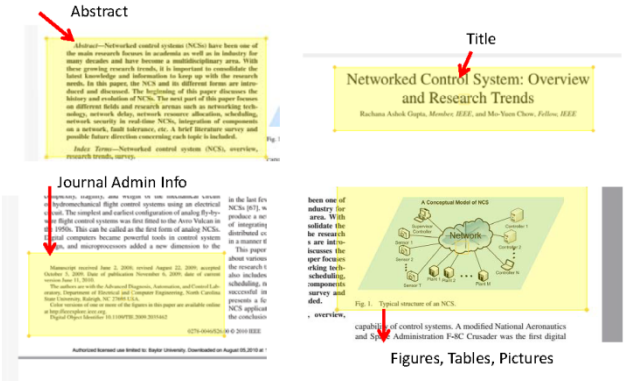
## Coding and Software Familiarization

# Coding Strategy

- Unit of Analysis
  - Document
- Recording unit
  - Sentence: smallest segment
- Code only by drawing a yellow box
- **DO NOT** highlight the text by using the mouse drag technique (this shows as a black highlight)

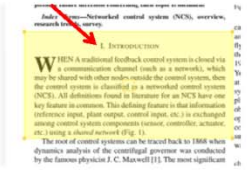
- Recording Constraints:
  - Tables
  - Pictures
  - Figures (and captions)
  - Copyright statements
  - Abstracts
  - Document titles
  - Section titles
  - Paragraph: Largest segment
  - Author information/Bio
  - Source information

# Examples of what NOT to Code

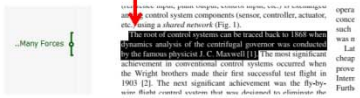


# Examples of what NOT to Code

The Titles of Paragraphs



The text was highlighted black using the selector tool drag method, instead of highlighting with a yellow box



An Entire Paragraph can only be coded NAP

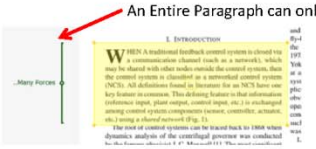


Figure Captions

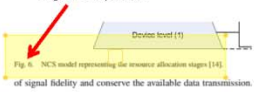




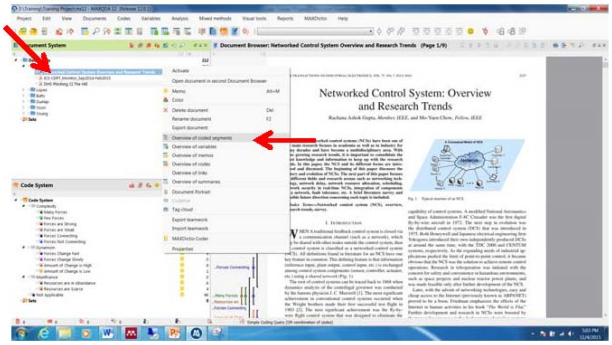
Fig. 6. NCS model representing the resource allocation stages [14].

of signal fidelity and conserve the available data transmission.

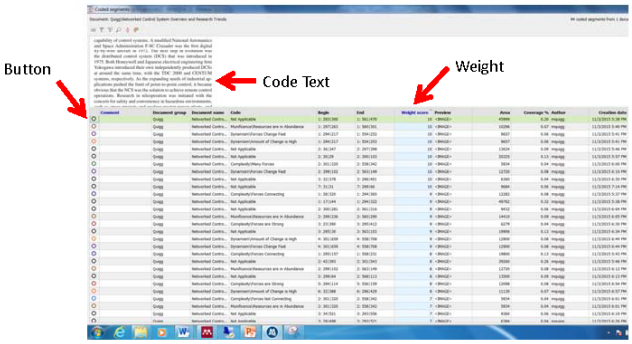
# Weight

- Weighting needs to be completed for each code. It expresses your level of confidence in the code on a scale of 1-10 (1 being least confident, 10 being most confident)
  - There are a few techniques to assign the weights:
    - Assign them right after applying the code (Recommend)
    - Assign them after each page is coded
    - Assign them at the end of coding the artifact (Least Recommended as the codes will not be as fresh to you)
- You can check to see if you've coded everything by highlighting the document in your folder, "right clicking" and selecting "overview of coded segments"

# Weight




By clicking on the button on the far left of the screen the code text appears in the top window. Change the weight by double clicking in the appropriate weight box.



## Coding Strategy cont'd

- Hints and Tips
  - Read paragraph first, then code segments
  - **Code** complete thoughts in text
    - Can include bullets
  - Code present realities (within the last 7 years) not statements about the distant past, or future
  - Code "Not Applicable" portions of qualified ***TEXT*** only
  - **Do Not** code figures, tables, copyright info, titles, abstract, legal statements as NAP, rather you ignore it from consideration
  - Do not interact with other coders. This is intended to be your work alone.
  - MAXQDA autosaves everything you do.

## Coding Strategy cont'd

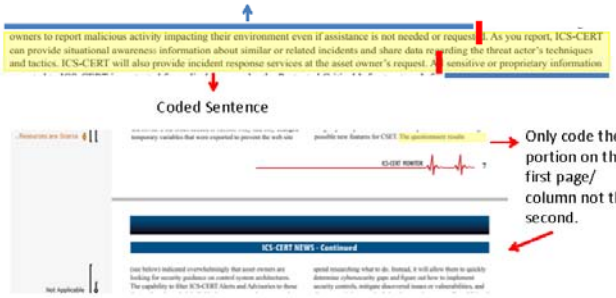
- Hints and Tips
  - If you code something once, do not code the same information again in the same artifact i.e. **Many Forces**: "…a huge amount of vendors are involved.." and " the tremendous amount of vendors contributed a lot of feedback."
  - If there is new information about the force, or different information, then it can be coded again or coded something different.

## Coding Strategy cont'd

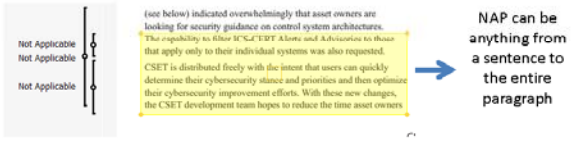
- Hints and Tips
  - Code only the sentence with the yellow box if you can, if not then it is acceptable to code a limited amount of the adjoining sentence.
  - If a sentence runs on into the next page code the first part of the sentence on the first page only. Apply to that segment the codes for the entire sentence. (even if its just one word)
  - NAP can cover multiple sentences combined not just a sentence or paragraph.

## Coding Strategy cont'd

It is alright to draw a box around a portion of the other sentence



## Coding Strategy cont'd




## Coding Strategy cont'd

- Hints and Tips
  - Whether something is strong or weak is from the perspective of the force in the external environment. i.e. "the organization was compromised by the hackers" the external environmental force is the hacker, the hacker is strong since compromising a system is a display of strength in CI/Cyber.

## Coding Strategy cont'd

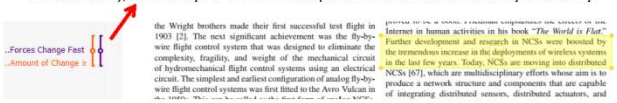
- Hints and Tips
  - Information that is about some other country than the U.S. is a "not applicable" code. If the U.S. is included than it is applicable. This research is about the U.S.
  - Take a break every 50 minutes to clear your head.
  - During that time copy the project from the thumb drive folder to another folder to back it up.
  - Code text "Not Applicable" that represent guesses, speculations, or uncertainties (e.g. we encourage, should likely, probably, maybe, etc.)

## Coding Strategy cont'd

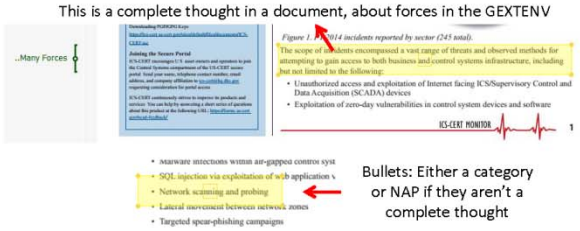
- Hints and Tips
  - If just a number is given, use your knowledge of this area to determine if it is a lot or a little, i.e. "1600 industry reps attended the government briefing…"
  - This is the same for all code categories, use your knowledge of the phenomena to make a decision.

# What is Acceptable to Code

Two or more codes in the same sentence if applicable (Caution more than 2 codes is a rare case), evaluate your codes at this point to determine if it's truly necessary.




This is a complete thought in a document, about forces in the GEXTENV




Bullets: Either a category or NAP if they aren't a complete thought

# Questions?

Bibliography


1. H. Aldrich, Organizations and Environments, Stanford University Press, Stanford CA, 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 NY, 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 IL, 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. S. Boyer, SCADA: Supervisory Control and Data Acquisition (4th Edition), The Instrumentation, Systems, and Automation Society, Durham NC, 2010.

9. O. Brafman and R. Beckstrom, The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations, Penguin, New York NY, 2006.

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

11. T. Burns, and G. Stalker, The Management of Innovation, Oxford University Press, New York NY, 1961.

12. J. Child, Organizational structure, environment and performance: The role of strategic choice, Sociology, vol. 1(6), pp. 1-22, 1972.

13. R. Clarke and R. Knake, Cyber War, Harpercollins, New York NY, 2014.

14. J. Cohen, A coefficient of agreement for nominal scales, Educational and Psychological Measurement, vol. 20(1), pp. 37-46, 1960.

15. S. Collyer and C. Warren, Project management approaches for dynamic environments, International Journal of Project Management, vol. 27(4), pp. 355-364, 2009.

16. J. Colquitt, J. Lepine and M. Wesson, Organizational Behavior: Improving Performance and Commitment in the Workplace, McGraw-Hill, New York NY, 2011.

17. 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.

18. G. Dess and D. Beard, Dimensions of organizational task environments, Administrative Science Quarterly, vol. 29(1), pp. 52-73, 1984.

19. 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.

20. P. DiMaggio and W. Powell, The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields, American Sociological Review, vol. 48(2), pp. 143-166, 1983.

21. L. Donaldson, Strategy and structural adjustment to regain fit and performance: In defence of contingency theory, Journal of Management Studies, vol. 24(1), pp. 1-24, 1987.

22. L. Donaldson, The contingency theory of organizational design: Challenges and opportunities, in Organization Design, R. Burton, B. Eriksen, D. Hkonsson and C. Snow (Eds.), Springer, New York NY, pp. 19-40, 2006.

23. L. Donaldson, The normal science of structural contingency theory, in Studying Organizations: Theory and Method, S. Clegg and C. Hardy (Eds.), Sage, Thousand Oaks, California, pp. 51-70, 1999.

24. R. Duncan, Characteristics of organizational environments and perceived environmental uncertainty, Administrative Science Quarterly, vol. 17(3), pp. 313-327, 1972.

25. 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.

26. R. Flesch, How to Write Plain English: A Book for Lawyers and Consumers, Harper and Row, New York NY, 1979.

27. M. Gladwell, Blink: The Power of Thinking Without Thinking, Back Bay Books, New York NY, 2007.

28. R. Gooding and J. Wagner III, A meta-analytic review of the relationship between size and performance: The productivity and efficiency of organizations and their subunits, Administrative Science Quarterly, vol. 30(4), pp. 462-481, 1985.

29. 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.

30. Government Accountability Office, Content Analysis: A Methodology for Structuring and Analyzing Written Material, Washington DC, 1996.

31. R. Harris, Organizational task environments: An evaluation of convergent and discriminant validity, Journal of Management Studies, vol. 41(5), pp. 857-882, 2004.

32. A. Ilinitch, R. DAveni and A. Lewin, New organizational forms and strategies for managing in hypercompetitive environments, Organization Science, vol. 7(3), pp. 211-220, 1996.

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

34. P. Khandwalla, Environment and its impact on the organization, International Studies of Management and Organization, vol. 2(3), pp. 297-313, 1972.

35. 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, Naval Technical Training Command Millington TN Research Branch, Millington TN, 1975.

36. T. Koppel, Lights Out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath, Crown Publishers, New York NY, 2015.

37. K. Krippendorff, Content Analysis: An Introduction to its Methodology, Sage Publications, Thousand Oaks, California, 2013.

38. J. Landis and G. Koch, The measurement of observer agreement for categorical data, Biometrics, vol. 33(1), pp. 159-174, 1977.

39. P. Lawrence, and J. Lorsch, Differentiation and integration in complex organizations, Administrative Science Quarterly, vol. 12(1), pp. 1-47, 1967.

40. 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.

41. 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.

42. M. Lombard, J. Snyder-duch and C. Bracken, Content analysis in mass communication, Human Communication Research, vol. 28(4), pp. 587-604, 2002.

43. 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.

44. P. Olson, We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency, Back Bay Books, New York NY, 2012.

45. W. Orlikowski, The duality of technology: Rethinking the concept of technology in organizations, Organization Science, vol. 3(3), pp. 398-427, 1992.

46. M. Patten, Understanding Research Methods: An Overview of the Essentials (7th Edition), Pyrczak Publishing, Glendale CA, 2009.

47. J. Pfeffer, Organizations and Organization Theory, Pitman, Boston MA, 1982.

48. J. Pfeffer and H. Leblebici, The effect of competition on some dimensions of organizational structure, Social Forces, vol. 52(2), pp. 268-279, 1973.

49. J. Pfeffer and G. Salancik, The External Control of Organizations: A Resource Dependence Approach, Harper and Row, New York NY, 1978.

50. D. Pugh, The measurement of organization structures: Does context determine form?, Organizational Dynamics, vol. 1(4), pp. 19-34, 1973.

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

52. M. Savin-Baden and C. Major, Qualitative Research: The Essential Guide to Theory and Practice, Routledge, Abingdon, United Kingdom, 2012.

53. G. Seffers, Cyber commander expects damaging critical infrastructure attack, Signal, December 1, 2014.

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

55. M. Tushman and R. Nelson, Introduction: Technology, organization, and innovation, Administrative Science Quarterly, vol. 35(1911), pp. 18, 1990.

56. U.S. Army, *Force Development and Documentation*, Department of the Army, AR 71-32, Government Printing Office, Washington DC, 2013.

57. A. Van de Ven and D. Ferry, Measuring and Assessing Organizations, John Wiley and Sons, New York NY, 1980.

58. R. Weber, Basic Content Analysis (Second Edition), Sage Publications, Thousand Oaks CA, 1990.

59. S. Worrall, Is the United States Prepared for a Massive Cyberattack?, National Geographic, Washington DC (news.nationalgeographic.com/2015/11/151108-cybercrime-cyberattack-ted-koppel-computers-hacking-internet-ngbooktalk), 2015.

60. R. Yin, Case Study Research Design and Methods, Sage Publications, Thousand Oaks, California, 2014.

# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 074-0188*



| **1. REPORT DATE** *(DD-MM-YYYY)* | **2. REPORT TYPE** | **3. DATES COVERED** *(From – To)* |
|---|---|---|
| 24-03-2016 | Master's Thesis | Aug 2014 - Mar 2016 |

**4. TITLE AND SUBTITLE**
Cyberspace and Organizational Structure: An Analysis of the Critical Infrastructure Environment

**5a. CONTRACT NUMBER**

**5b. GRANT NUMBER**

**5c. PROGRAM ELEMENT NUMBER**

**6. AUTHOR(S)**
Quigg II, Michael D., Captain, USA

**5d. PROJECT NUMBER**
JON: 15G264

**5e. TASK NUMBER**

**5f. WORK UNIT NUMBER**

**7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)**
Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way, Building 640
WPAFB OH 45433-8865

**8. PERFORMING ORGANIZATION REPORT NUMBER**
AFIT-ENV-MS-16-M-177

**9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)**
Department of Homeland Security ICS-CERT
POC: Neil Hershfield, DHS ICS-CERT Technical Lead
ATTN: NPPD/CSC/NCSD/US-CERT Mailstop: 0635,
245 Murray Lane, SW, Bldg 410, Washington, DC 20528
Email: ics-cert@dhs.gov phone: 1-877-776-7585

**10. SPONSOR/MONITOR'S ACRONYM(S)**
DHS

**11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

**12. DISTRIBUTION/AVAILABILITY STATEMENT**
DISTRIBUTION STATEMENT A. APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

**13. SUPPLEMENTARY NOTES**


**14. ABSTRACT**
Now more than ever, organizations are being created to protect the cyberspace environment. The capability of cyber organizations tasked to defend critical infrastructure has been called into question by numerous cybersecurity experts. Organizational theory states that organizations should be constructed to fit their operating environment properly. Little research in this area links existing 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 analysis to identify opportunities for improvement.

This thesis analyzes the cyber-connected critical infrastructure environment using the dominant organizational structure theories. By using multiple case study and content analysis, 2,856 sampling units relating to environmental uncertainty (complexity, dynamism, and munificence) are analyzed to show the general external environment of cyber organizations tasked to protect critical infrastructure is highly uncertain thereby meriting implementation of organic structuring principles.

**15. SUBJECT TERMS**
Cyber organizations, organizational structure, critical infrastructure protection, content analysis, multiple case study

| **16. SECURITY CLASSIFICATION OF:** | | | **17. LIMITATION OF ABSTRACT** | **18. NUMBER OF PAGES** | **19a. NAME OF RESPONSIBLE PERSON** |
|---|---|---|---|---|---|
| **a. REPORT** | **b. ABSTRACT** | **c. THIS PAGE** | | | Rice, Mason, ENG, LTC, Ph.D, USA |
| U | U | U | UU | 103 | **19b. TELEPHONE NUMBER** *(Include area code)* (937) 255-3636 x4620 (mason.rice@afit.edu) |