A MATRIX BASED INTEGRATED FRAMEWORK FOR MULTI DISCIPLINARY EXPLORATION OF CYBER-INTERNATIONAL RELATIONS

by

GAURAV AGARWAL

Master of Science (2007)
Texas A&M University

Submitted to the System Design and Management Program
in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE IN ENGINEERING AND MANAGEMENT

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

June 2010

Signature of Author. . . . . .
System Design and Management Program
May 13, 2009

Certified by. . . . . .
Dr. Nazli Choucri
Thesis Supervisor
Professor of Political Science
Associate Director, Technology & Development Program

Accepted by. . . . . .
Patrick C. Hale
Director
System Design and Management Program

This page is intentionally left blank.

A Matrix Based Integrated Framework for
Multi Disciplinary Exploration of Cyber-International Relations

Submitted to the System Design and Management Program on May 7, 2010
In Partial Fulfillment of the Requirements
For the Degree of

Master of Science in Engineering and Management

ABSTRACT

Cyberspace is the most pervasive and rapidly adopted communication media and the most disruptive until date. It is now indispensable for almost every facet of modern society and touches, practically, everyone by providing a powerful platform for interaction and innovation. Given the widespread availability of tools to operate in this environment, a growing array of actors are trying to benefit as they seek to control critical decision points in the real world and cyberspace.

It is imperative to understand what cyberspace "is made of" – over and above the Internet and answer the question "*who gets what, when, and how?*" The intent of this research initiative is to contribute to the generation, management and sharing of knowledge to enhance understandings of the emerging area of cyber-international relations as a complex, flexible and adaptive domain of interactions.

The **first contribution** of this thesis is the development of a multi-dimensional *Cyber System for Strategic Decisions* (CSSD) framework. This framework enables a holistic identification of the elements of a system, which are structured as set of nested and hierarchical relationships. It facilitated in mapping the entities that comprise different domains of cyberspace and the dependencies within and across those entities.

The **second contribution** of this thesis is the development of the foundations for an internally consistent and articulate representation of cyber-international relations in terms of a*ctors- individuals and group of individuals, layers of the Internet* and the *context of cyber engagement* that form the basis of the CSSD framework. This approach can be applied to diverse domains to build scenarios and model different facets of both the real world and cyberspace according to the practical needs. *The instruments and intensity of engagement* and *the extent of time of engagement* are the two dependencies that map the interactions among the different entities.

The **third contribution** of this thesis is the development of a robust, comprehensive, and coherent test use-case based on "Intellectual Property Rights (IPR)" domain. The CSSD framework is then adapted to test its applicability to the use-case. IPR has been selected as the test use-case because it provided both the legal understanding and legislative efforts at international level, in as collaborative, effective and uniform manner as possible, to protect the rights of intellectual property owners and to avoid future conflicts.

Thesis Supervisor: Dr. Nazli Choucri

Title: Professor of Political Science.

DEDICATION

This research is dedicated to my family that embraced me through life's challenges and for their unending support regarding my life changing decisions.

ACKNOWLEDGEMENTS

I would like to express my gratitude and thanks to my advisor, Professor Nazli Choucri for providing me with this research opportunity and for her guidance and insights that made this thesis possible. Her enthusiasm and spirited leadership have been a constant source of inspiration for me.

I would like to thank Dr. David D. Clark for being a great mentor. As a leading expert in leading the development of the Internet, he provided valuable feedback and guidance that shaped this research.

I would like to thank all the researchers at MIT and Harvard Kennedy School associated with Minerva Research Initiative for contributing their unique insights from government, industry and academia and their expertise in technology policy practice. I greatly appreciate their support of this research.

I am grateful to my colleagues and fellow graduate students at MIT for invaluable discussions, insights, and suggestions related to this work. Many thanks to Dr. Tsoline Mikaelian for discussions and suggestions related to this work.

I would like to gratefully acknowledge the funding for this research provided through the MIT Department of Political Science by United States Secretary of Defense's Minerva Research Initiative. The contents of this document do not reflect the views, policy, or position of the United States Department of Defense.

NOMENCLATURE

c-DSM	coupled –Dependency Structure Matrix
CSSD	Cyber System for Strategic Decisions
DMM	Domain Mapping Matrix
DSM	Dependency Structure Matrix
IP	Intellectual Property
IPR	Intellectual Property Rights
MIT	Massachusetts Institute of Technology
WIPO	World Intellectual Property Organization

TABLE OF CONTENTS

CHAPTER Page

CHAPTER Page

LIST OF FIGURES

LIST OF TABLES

This page is intentionally left blank.

1. INTRODUCTION

"...Every American depends- directly or indirectly – on our system of information networks. They are increasingly *the backbone of our economy and infrastructure; our national security and our personal well-being"(Obama 2008).*

The Internet is a communication, networking, and entertainment media unlike any that has come before. It has a variety of unique attributes that have made it the quickly adopted communication media and the most disruptive until date. The strategic employment of this information and communication media touches practically everyone. It has provided a powerful platform for innovation and has enabled economic growth, empowered an individual and society as a means to improve the welfare all across the globe.

It is also the first truly global media carrier. It has enabled multi-directional communication between different individuals (or group of individuals), anyone with the Internet access. Further, it allows accessing the information available online, subject to few limitations like firewalls and filters, from anywhere in the world. This far transcends the reach of radio and television - both terrestrial and satellite. Thus, providing individuals (or group of individuals) an access to reach a large potential audience, a privilege that was previously reserved to a few in politics, media and entertainment is now open to all.

As mentioned by Jonathan Zittrain (2008, 197-199), the Internet is a generative tool and allows tinkering and all sort of creative uses. Investments in cyber technologies are being made by businesses and industries for improving and providing new services to capture the economic

---

This thesis follows the Chicago 15th B style.

value and fuel economic growth. This has been demonstrated in fields like intelligent transportation systems, smart-energy grids, medical records, entertainment systems. Heavy investments are also being made in infrastructure development to empower citizens through digital education and e-governance initiatives. Further, military and security agencies are as well aggressively adopting net-centric systems to strengthen the national security.

1.1. Emergent Complexity in Cyberspace

Among the many distinctive features of the Internet, the most important, it is the first truly open source communications media. No one has the overall control on content, transmission, and services provided. Further, its architecture is based on the principles of interoperability and efficiency rather than security (The White House 2009). This has resulted, for example, in a growing array of state adversaries who have the ability to cause widespread disruptions by compromising, stealing, changing and destroying information (Chalaby 2000). These adversaries can deny the legitimate owner the use of information and (or) deliberately destroy or insert erroneous data to render the system inoperable or unreliable (Benkler 2006, Chapter 1).

In addition to this, the Internet is going mobile. With the convergence of traditional telecommunication systems and the Internet, it has become the primary mode of inter-connectivity and operations for many actors and stakeholders. With smart phones and similar computing devices, the information can be accessed from anywhere, a challenge for issues like parental control of use, data protection, security, and privacy.

These properties of cyberspace also create dilemmas for *traditional* approaches to interactions in the real world in which actors do not appear to take benefit of Internet

technologies to leverage the existing tools available to them. Such tools include policy-making and legislation, investment in research and development, procurement standards, and the like.

The digital networks and devices comprising cyberspace transcend national, organizational, and economic sector boundaries. These networks are composed of highly interdependent parts under different administrative control, giving rise to jurisdictional quandaries and a greater risk of disruption, e.g. determining who is responsible for bad actors. Further, as they become global with electronically mediated distributed operations, corporations may also lose control of their intellectual property, technological advantages, and internal hierarchical control.

Undoubtedly, the Internet has been a vital vehicle for a state's soft power (Nye 2004,33-34), but it may also undermine a state's control over the images, discourse and language to which its citizens attend. The Internet, thus, amplifies citizen's political demands. Furthermore, it may also undermine the state's command of their loyalties, identities, and aspirations, by exposing them to competing foreign influences and including them in global conversations about global challenges. Under these conditions a government cannot assume the unquestioned public support for security policies or military actions (The White House 2009).

Analogous limitations apply to cooperative and multilateral strategies. Because cyber-attack tools are widely available and inexpensive, even newly industrialized countries, terrorists groups, and criminal gangs are capable of highly effective exploitation or attacks.

The complexity and the scope of interactions in the cyberspace require that the actors collaborate with other state and non-state actors to tailor and scale effective solutions. Such solutions include the development and implementation of a strategy, creating international conventions, and ratifying international treaties or the like for managing the state stability and

suppressing the black markets for cyber crime that supply increasingly sophisticated tools, data, and skills necessary for cyber-attacks or exploitation.

The United States (and other nations), thus, "face the dual challenge of maintaining an environment that promotes innovation, efficiency, economic prosperity and free trade while promoting safety, security, civil liberties and privacy rights" (The White House 2009).

1.2. Problem Statement and Research Objectives

Even though technology is playing an increasing role for the effective implementation of public policy, in many policy discussions human and organizational issues take preference over the technological issues (Avgerou and McGrath 2007; Whitley and Hosein 2008; Heeks and Stanforth 2007; Horton and Wood-Harper 2006). The due process for taking political decisions may require the use of facts provided by science and technology even though there is no consensus in the scientific community.

Individuals, groups, and institutions, thus, perceive technology differently during the deliberations for a policy change. At times, technology is adapted to satisfy their needs and interests and other times compel them to admit that their perspectives do not match with the facts provided by it. (Pouloudi and Whitley 2000). Thus, both policy and the decision can get influenced by the characteristics and perceptions of technologies (Whitley 2009).

The intent of this research work is to contribute to the generation, organization and sharing of knowledge to enhance the value of the knowledge in the emerging field of international relations within the complex and flexible environment of cyberspace.

1.3. Research Methodology

This thesis will attempt to map out the cyber domains , i.e. what cyberspace "is made of" and address three related questions pertaining to "*who gets what, when, and how?" (Lasswell 1950; Choucri 2009)*

a) "Who can play" in this new arena? Who are the actors that have appeared and influenced the space that a traditional state actor would not regularly expect to deal with?

b) What is this cyberspace, where do these actors act and what are the tools of influence, both direct and indirect?

c) How is the influence exercised and to what extent does cyberspace create distinctive behavior? Is there anything new?

The goal of this thesis is to answer the above-mentioned questions by:

a) Contributing to the development of an analytical framework for exploration of the multi-disciplinary field of cyber-international relations,

b) Developing foundations for an internally consistent and articulate representation of knowledge in the field of cyber-international relations, and

c) Developing a robust and comprehensive use-case to test the framework.

Answering these questions require a design and test methodology for developing both the framework and the logic of knowledge representation of a subject of interest. The methodological approach followed in this thesis is given below (Figure 1-1):

a) First, a framework (Task 1) for mapping the knowledge domain of the subject of interest is designed and developed.

b) Design of a test mechanism (Task 2), follows task one. The test mechanism should follow logic and the laws of transitivity (von Winterfeldt 1989). Representative use-cases are developed for actual testing of the framework.

c) Task 3 involves actual testing of the framework. It helps in identifying the practical problems and inefficiencies in the existing framework.

d) Finally, task 4 involves in determining whether altering the logic of the framework will overcome the shortcoming identified in task 3.

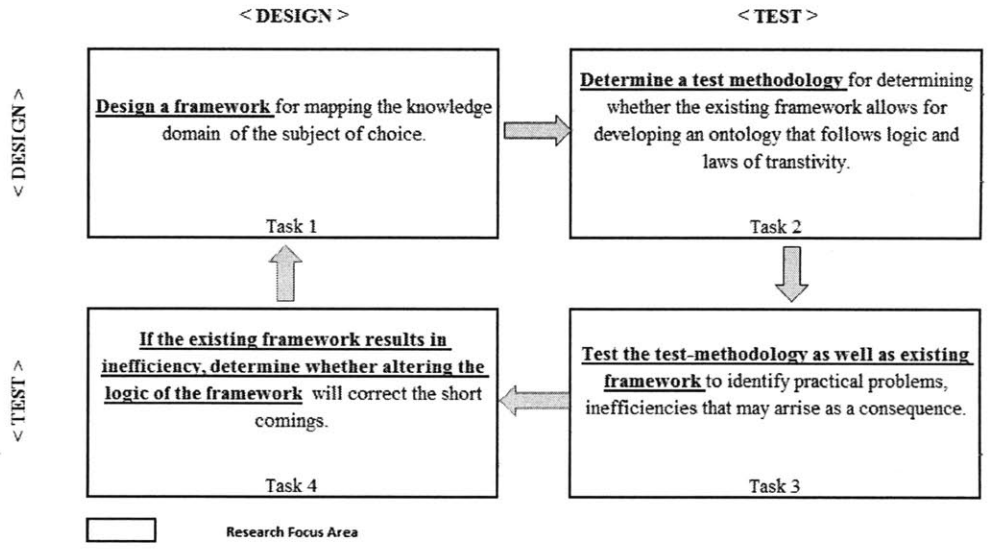


Figure 1-1: Research methodology[1].

One should recognize the limitations of this approach as well as scalability challenges for the complete investigation as this might be daunting for a field like cyberspace. The process is further complicated if the developments in the subject of interest (e.g. intellectual property rights) have been made incrementally over the centuries.

---

[1] Based on author's joint work with Dr. Tsoline Mikaelian for PATFrame research project at Lean Advancement Initiative, MIT, Cambridge, 02139. Fall 2009.

This thesis will focus on the developing a framework for the mapping the knowledge domain of the subject of interest related to cyberspace (i.e. Task 1 in Figure 1-1) and then will attempt to map the well-documented field of Intellectual Property Rights (task 2). Based on the practical problems faced and shortcomings found while mapping Intellectual Property Rights domain to the framework (task 3), necessary changes in the framework will be identified in task 4. Such design changes are made in the task 1 of the second iteration of the research methodology.

The method followed in this research is based on the acceptance of the use of common terms. Such common terms refer to the objects, and relations that may exist between those objects/terms, as applied to the phenomenon of cyberspace, which we agree to constitute or comprise cyberspace. This thesis cannot address the metaphysics question (Koepsell 2000, 25-27) regarding the nature of reality of the knowledge and focuses on the facts of common experience. This approach has set the need to give an account of (Heim 1993, 89):

a) The ways entities exist and interact within the cyberspace, and

b) The ontological status of cyberspace.

1.4. Research Design

This section (and Figure 1-2) details the key activities followed to achieve the thesis goals as identified earlier in section 1.3.

a) **Stage 1, Functional Definition:** The research started by identifying the key trends and drivers that affect the current and future development of the Internet. This process employed scanning diverse range of sources of information in a systematic way to identify and select relevant information. Literature on science and technology studies (STS) was particularly helpful in understanding the relationships and

interactions between technology, policy, and organizational decision-making. Sources of information included expert discussions with Dr. David D. Clark[2] and Professor Nazli Choucri[2], here at MIT and attendance to conferences, public lectures, and invited talks at MIT.

b) **Stage 2, System Definition:** Following a broad range and comprehensive literature survey, the next task was to group and categorize items for identifying and categorizing similar items. The definition of two important elements of cyberspace - *actors* and the *layers of the Internet* were direct contributions from Dr. Clark and Professor Choucri. Built on this two-dimensional model, a third element - *context of cyber engagement* in both real world and cyberspace was added to the framework.

In parallel, the work was also carried out in identifying uncertainties in the real world caused by the cyberspace. Such uncertainties identified were as (i) different domains of activities; (ii) instruments and intensity of the engagement; (iii) extent of time for engagement in identified activities.

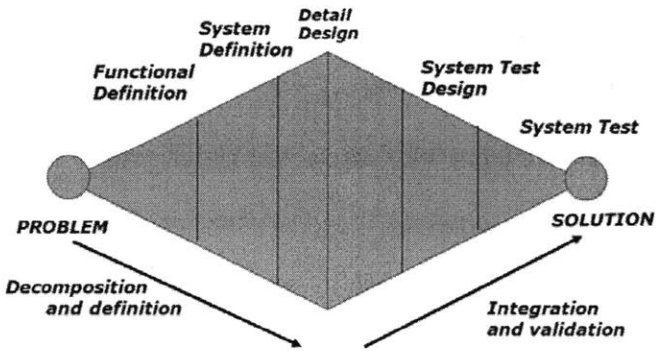


Figure 1-2 : Decomposition and integration stages followed in the research methodology (Quayle 2009).

[2] Refer Appendix A for biographies.

c) **Stage 3, Detailed Design:** This stage involved identification of analytical tools and techniques for system decomposition and integration. Matrix based tools (coupled- Dependency Structure Matrix, c-DSM) were selected for mapping elements of cyberspace, as identified in previous stages, to leverage their capabilities for any future analytical analysis of the system. Representative c-DSMs were developed at different levels of abstraction for assisting future analytic works to gain rich insights into the subject.

d) **Stage 4, System Test Design:** Once the framework was completed, it was tested against a robust test use-case. A robust use-case should be comprehensive and coherent. It should be able to test the system's behavior under different circumstances as it responds to the actions of different actors. It should also be able to represent different scenarios or a series of events depending on the particular action taken and the prevailing environmental conditions.

Activities related to task 2 of the framework (Figure 1-1) included the study of official documents, related to intellectual property rights (IPR), published by World Intellectual Property Organization, Geneva to build a robust test use-case based on it. This was followed by mapping IPR domain to the developed framework. An attempt has been made to ensure that the number of actors and stakeholders who participate in the articulation of propositions, and propositions themselves are accurately represented.

e) **Stage 5, System Test:** This stage involved the identification of inefficiencies in the existing framework (i.e. task 3 of research methodology) as well as mechanisms to correct them (i.e. task 4 of research methodology. Necessary

corrections were made to the framework in the task 1 of the next iteration of the research methodology.

1.5. Research Framework

The main innovative feature of the proposed conceptual, multi-disciplinary framework is that it enables the modeling of complex interdependencies in a socio-economic-technical-political environment. The framework also helps in understanding the interactions and dependencies that exist between technology, policy, and organizational decision-making process. The interactions between the most basic features of a state profile, i.e. people, resources, and technology(Choucri and North 1975, 1-5) are discussed in Chapter 2 & 3.

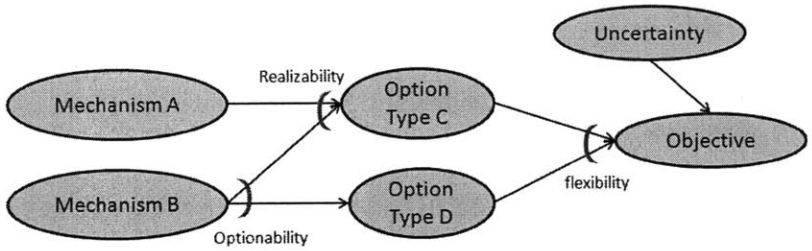


Figure 1-3: Identification of mechanisms and types of options in a dependency model (Mikaelian 2009).

Built on the previous work done Gray (1999, 23-45), Howard (1979, 976-986), and Choucri and North (1975, 14-21) , this thesis extends the current ontological framework used for mapping the knowledge domain of sustainability (Choucri 2007). The framework can be used to manage uncertainties facing an actor through a decision-making process by using analytical tools, which can be applied to it. This work will provide a model and an explicit framework for:

a) End-to-end representation and dependence modeling of the complex world using analytical tools like Dependency Structure Matrix (DSM).

b) Identification of real options-type and mechanisms to manage the "perplexities", where a mechanism is an enabler of the option and type represents the type of flexibility provided by the option as shown in Figure 1-3. The framework will also allow for identifying the flexibility, realizability and optionability of each option (Ross, Rhodes, and Hastings 2007; Mikaelian 2009).

1.6. Thesis Contributions

The intent of this research initiative is to contribute to the generation, management and sharing of knowledge to enhance understandings of the emerging area of cyber-international relations as a complex, flexible and adaptive environment of interactions. This is accomplished through the following specific contributions:

a) The **first contribution** of this thesis is the development of a multi-dimensional *Cyber System for Strategic Decisions* (CSSD) framework. This framework enables a holistic identification of the elements of a system, which are structured as set of nested and hierarchical relationships. It facilitated in mapping the entities that comprises different domains of cyberspace and the dependencies within and across those entities.

b) The **second contribution** of this thesis is the development of the foundations for an internally consistent and articulate representation of cyber-international relations in terms of *actors- individuals and group of individuals*, *layers of the Internet,* and the *context of cyber engagement* that form the basis of the CSSD framework. This approach can be applied to diverse domains to build scenarios and model different

facets of both the real world and cyberspace according to the practical needs. The *instruments and intensity of engagement* and the *extent of time* of engagement are the two dependencies that map the interactions among the different entities.

The complete framework will have individual three-dimensional lattice for each of the identified major domains. Each domain, a collection of a different set of activities around a coherent issue area, can shape the functional specification and architectural outline of the cyberspace. Based on a variety of domains and their nature, user can build different scenarios and model any number of possibilities according to the practical needs.

c) Finally, the **third contribution** of this thesis is the development of a robust, comprehensive, and coherent test use-case based on "Intellectual Property Rights (IPR)" domain. The framework is then adapted to test its applicability to the IPR domain. IPR has been selected as the test use-case because it provided both the legal understanding and legislative efforts at international level, in as collaborative, effective and uniform manner as possible, to protect the rights of intellectual property owners and to avoid future conflicts.

1.7. Outline

The research document is organized in the following manner:

Chapter 2 defines and characterizes the cyberspace and explains the complexity in mapping this Socio-Economic-Technical-Political system and introduces the *Cyber System for Strategic Decisions* (CSSD) framework used to classify the information relevant to the cyberspace.

Chapter 3 expands individual dimensions of the conceptual framework, *Cyber System for Strategic Decisions* (CSSD), presented earlier in the chapter 2.

Chapter 4 presents a use-case to test the applicability of the framework to the explorations of cyber-international relations. It will attempt to map the *intellectual property rights (IPR)* domain to the developed framework.

Chapter 5 concludes with a discussion of the contributions and the limitations of the thesis, and presents recommendations for future work.

This page is intentionally left blank.

2. MAPPING CYBERSPACE

This purpose of this chapter is to define and characterize the cyberspace and to identify key elements that need to be considered while mapping the cyberspace. In this chapter, cyberspace is defined as a socio-economic-technological-political system. This chapter presents the *Cyber System for Strategic Decisions* (CSSD) framework that puts together the key dimensions of "strategy" as identified. The later part of the chapter describes a matrix-based analytic tool, *coupled – dependency structure matrix* (c-DSM) which has been used in prior works to model complex engineering systems. An example of c-DSM is discussed. The chapter will then discuss analysis methods based on DSM. It will also bring to light the challenges faced and methods to mitigate them while developing c-DSMs.

2.1. Defining Cyberspace and Cyber Operations

This research uses the following definition of cyberspace as defined in Joint Publication 1-02, US Department of Defense (DoD) Dictionary of Military and Associated Terms.

a) "**Cyberspace** - a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" (Department of Defense 2009).

b) "**Cyberspace Operations** - the employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid" (Department of Defense 2009).

According to the definition, cyberspace operations can be used to create "cyber power" which is the ability to affect other people to get the outcomes one wants using the electronically interconnected information resources of the cyberspace domain. In one widely used definition, cyber power is "the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power"(Kuehl 2009).

2.2. Characterizing Cyberspace

At a symposium on cyber law held at the University of Chicago in summer of 1996, economist Easterbrook (1996) presented a powerful and challenging presentation. In his paper "Cyberspace and the Law of the Horse," he argued that the subject of "Law of Cyberspace" does not exist and said that "We are at risk of multidisciplinary dilettantism, or, as one of his mentors called it, the cross sterilization of ideas. Put together two fields about which you know little and get the worst of both worlds" (Easterbrook 1996).

A variation of the same challenge again surfaced in Joseph Sommer's (2000) paper *"Against Cyberlaw"* in which he challenged that it is the social phenomenon, not the technologies, that define laws and subject of legal study. Sommer's charge against cyber law is demonstrated at two levels. First, that the technological practices seldom provide a framework of bodies of law, and if they do provide it lack longevity. Even though some technologies may provide new legal processes like oil and gas law, telecommunication law, copyright and media law (Sommerdagger 2000), he supported his hypothesis by showing that technologically defined laws lack longevity. To demonstrate that it is usually useless to define a body of law in terms of a technology, he gave the example of 19th century race law that could have been existed on Cotton Gin Law that being the technology which drove the development of race law (Sommerdagger 2000).

Sommer's further proposes that both technology and law are social endeavors and should be looked through a social interpretation lens, which affects both technology and law. He argues that only the pure technologies and law that do not split into their component social effects have the ability to become the bona fide law in their own right. He further argued that the law of cyberspace can be added to this list if and only if the Internet is considered to be a singular social phenomenon, which is not the case (Sommerdagger 2000).

When technologies pass through this social lens (Figure 2-1), they split into the spectrum of social and political effects. While some technologies have powerful social influence, they may have no or little legal/regulatory impact, such as technologies of the railroad or the steam engine. Such technologies fail to create communities around them and merely serve the existing communities. Others may have an immense social impact and some aspects of the technology affect the legal/regulatory framework. Such socio-legal technologies give rise to new communities linked through the medium of the technology like aviation, print and broadcast media, and telecommunications.

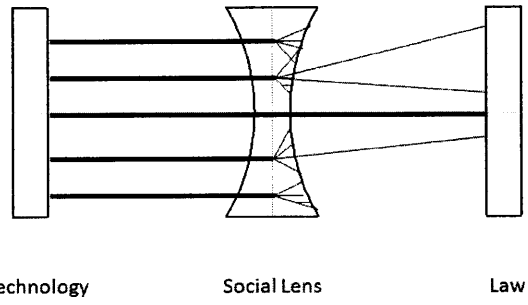


Figure 2-1: The social lens, adapted from (Murray 2007, 13-16).

Cyberspace unarguably passes this social mediation test as a socio-economic-technological-political system. Thus, in this thesis, it is considered to be an ever-growing pervasive, international, digital networks that (Choucri 2009):

a) Enable new strategic interactions among nation states and other actors that can affect national security and well-being;

b) Stimulate competition and collaboration among the actors concerning the Internet governance and control;

c) Transform social, economic, political, scientific, and cultural activities in ways that change the strategic capabilities of the actors.

2.3. Socio-Political Modalities vs. Socio-Economic-Technological-Political Modalities

The answer to the question "why the socio-political modalities cannot be applied to the cyberspace?" lies in the understanding of the difference between socio-political modalities and socio-economic-technological-political modalities of interaction in the physical world. Professor Lessig's thesis on the "Modalities of Regulation" (Lessig 1998) suggests the application of four modalities: law, market, norms and architecture, which can be categorized into two families (a) socially mediated modalities and (b) environmental modalities (Murray 2007,35-38), as shown in Figure 2-2.

The modalities in the physical environmental space face a lot of inertia from the physical laws of the world and will become less regulated over time as the "entropy of systems increases" (Shannon 1948). To overcome this and benefit from the design-based controls, one has to bring external sources, which are resource intensive. Considerable amount of resources are required to be expended on the construction and implementation of design-based systems to overcome this inertia and gain control. For example, in case of transport policy a large amount of resources are spent on the traffic management systems and designing the road layouts.

However, use of socially, politically and legally mediated modalities (e.g. implementation of a license and toll system, which adds an additional layer in the hierarchy or

the regulation) in designing the regulation does not require overcoming the environmental inertia and get a pre-eminence in implementation.

The early literature on the environmental regulation reveals the role played by the technology to be static (Porter and Linde 1995). It was assumed that the inherent design features of the Internet would make the interventions of regulatory bodies, within the Internet, futile. Lessig (2002, 100-108) has demonstrated that there were certain times, when constraints were considered fixed or the cost of making architectural changes was so high as to make the thought of using them strange.

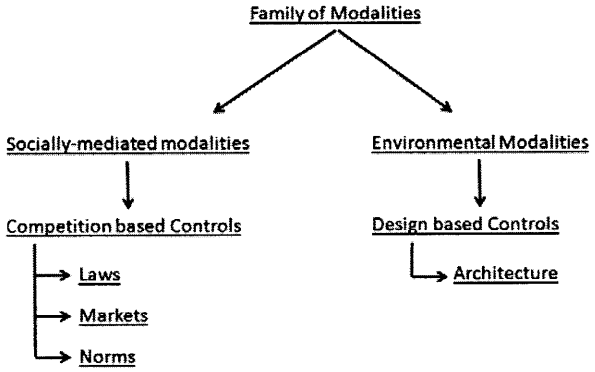


Figure 2-2: Lessig's family of modalities (Murray 2007, 37).

However, once an actor leaves the physical layer and enters the logical and application layer (beyond the wires and router) of the Internet, the environmental inertia is reduced, if not it is disappeared. This changes the relationship between the law, society and technology and the environmental modalities play an equally same functional role (Figure 2-3), forming the basis of and can be exploited in the regulation of the Internet. Thus, it may become necessary to include technology in the regulatory discourse (Lessig 2002, 85-99). For example, the new communication technologies have led to re-examination of many policies and assumptions for the management and regulation of the radio spectrum (Levin 1966).

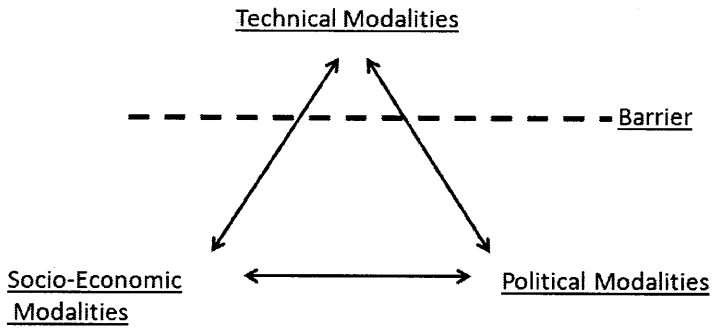


Figure 2-3: Socio-economic-technical-political environment (Murray 2007, 42).

2.4. Mapping Cyberspace- Cyber System for Strategic Decisions

Mapping the socio-economic-technical-political system of cyberspace requires a framework, developed on the theory of strategy that allows for "making sense of all the strategic experience, regardless of the tactical form it may assume" (Gray 1999). Strategy is a "plan of action designed in order to some end; a purpose together with system of measures for its accomplishment" (Wylie 1967, 14). Further, its essence "lies in the realm of consequences of action for future outcomes" (Gray 1999, 18).

Strategy can be classified into social, logistical, operational and the technological categories (Howard 1979). These four categories can be further delineated into 17 dimensions and then re-categorized into three broad categories of (Gray 1999, see Chapter 1) :

a) People and politics (comprising of people, society , culture , politics and ethics),

b) Preparation of war (economics and logistics, organization, military administration, information and intelligence , strategic theory and doctrine and technology), and

c) War proper (comprising of military operations, command, geography friction, adversary and time).

Further, it can be also analyzed with reference to:

a) Geographical environments to which it is specifically applied (i.e. under water, on water, land, air, space, and cyberspace), and

b) Tools used or with focus of the different levels of conflict and the character of the war.

Cyber System for Strategic Decisions (CSSD), which provides a reference framework for characterizing the boundaries of a complex system of the cyberspace, will pursue the dimensions of strategy as mentioned earlier in the chapter. It will try to show what cyberspace *"is made of"* and *what its dimensions are.*

CSSD also acts as a framework for developing an internally consistent and explicit representation of actions, problems, and solution strategies pertaining to factors threatening system stability and to mechanisms reinforcing security. Although cyberspace has a place for all the dimensions, the influence of some dimensions is more pronounced than others, and it will change with the use-case scenario used for the analysis. The basic form of the CSSD framework is a three-dimensional lattice as shown in Figure 2-4.

The **actors-individual and group of individuals** axis of the framework (Figure 2-4) represents *"population,"* one the three master variables of a state profile. The other two master variables are *access to resources* and *availability of technology* (Choucri and North 1975, 1-5). At all the relevant levels of analysis, whether it is for land-power, sea power, air power, space-power, or cyber-power, the real people execute and do strategy.

The second axis of the three-dimensional lattice represents the stratified **layers of the Internet**. Internet is a man-made geographic environment which has evolved in past 40 years of its existence in a piece meal way (The White House 2009). These changes have been designed to accommodate demands for the higher efficiency, simpler connectivity, and improved security or

for the accessibility of data/content. It is, thus, important to understand the function played by the stratified technological layers of Internet in the communication system.

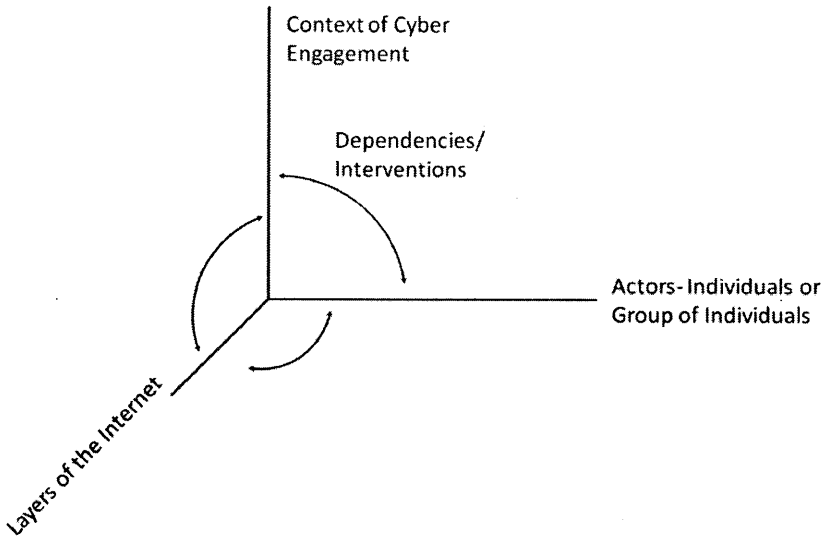


Figure 2-4: Basic CSSD framework[3].

Cyber operations, as explained earlier in section 2.1, can have an impact on the human activities and affects both the people and their environment. The third axis of the lattice, thus, represents the **context of cyber engagement.**

When the demands of a society are unmet or its existing capabilities are insufficient to meet them, there arises a need to develop new capabilities. However, the ability of a society to develop the required capabilities depends exploiting on the existing capabilities. If they are not available within its boundaries at a reasonable cost, society looks for the same beyond its borders (Choucri and North 1975, 20). The level of such engagement ranges from *"protection of interest"* within an actor's own boundaries; *"expansion of interest"* beyond its boundaries; to

[3] Based on author's discussions with Dr. David Clark and Dr. Nazli Choucri at MIT Cambridge 02139. February 2010.

finally *"power projections"* for producing preferred outcomes in cyberspace and in other domains.

In the context of cyberspace, the framework for characterizing the boundaries of a complex system in the real world comprises of different and potentially overlapping domains of engagement. These domains constitute of human individuals (or group of individual) to fully intelligent systems capable of autonomous planning, control and adaptive behavior. They also constitute a different set of activities within the domain that can shape the functional specifications and architectural outlines of the cyberspace. Economy, social system, intellectual property rights, and technological system are a few such domains.

Once the domain boundary of the cyberspace is defined by identifying the system (or system- of-systems), for which the performance and effectiveness should be tested, one may then distinguish the system (or system-of-systems) from the environmental uncertainties in which it operates. These environmental uncertainties (Figure 2-5) may be characterized by external influences or constraints (interventions) upon the system that may affect both the system and the environment.

Because of the complex nature of the environment, one cannot expect to manage the system by just alerting one or few of the interventions. As with any environment, mapping or forecasting interventions between the various entities is difficult. The CSSD framework will attempt to capture the inter-dependencies between any two of the above-mentioned different entities by using the following two dependencies (Figure 2-5):

a) **Instruments and Intensity of Engagement[4]:** It is an actor's ability to use coercive or cooperative tools to affect other's behavior for the protection, expansion, and

[4] Based on Professor Joseph Nye's, former dean of Harvard's Kennedy School of Government, comments at ECIR dinner at MIT faculty club, MIT, Cambridge, 02139 (Nye 2010). February 11, 2010.

projection both of its interests and power across all the layers of the Internet (Nye 2004).

b) **Extent of time[5]:** To help convey the complexity of subject, the activities can be broadly categorized into: (a) far-term, (b) mid-term, and (c) near-term or real time activities based on the tenure of the engagement.

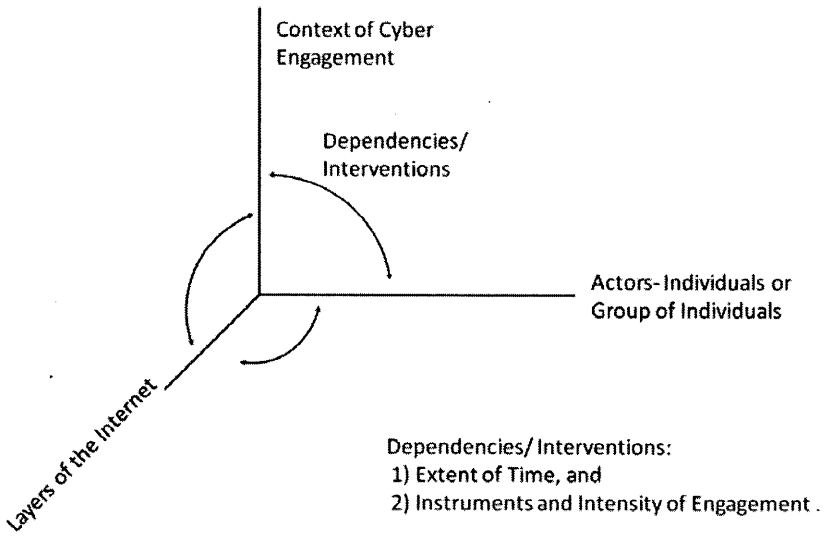


Figure 2-5: Dependency mapping of the interventions.

Individual interventions that directly relate to these dependencies for different systems are stored in a separate two-dimensional array (Figure 2-6), where rows correspond to dependencies, and columns map to different domains. This exercise will help in classifying the dependencies across different domains into generic categories.

The identified axes of actors, layers of the Internet and context of cyber engagement, and the two dependencies – instruments and intensity of engagement, and extent of time for

[5] Based on author's joint work with Dr. Tsoline Mikaelian and Dr. Ricardo Valerdi for PATFrame research project at Lean Advancement Initiative, MIT, Cambridge, 02139. Fall 2009.

engagement will be decomposed in Chapter 3. Building on Chapter 3, the dimensions and dependencies are decomposed once again to map intellectual property rights domain in Chapter 4.

The complete CSSD model will have an individual three-dimensional lattice for each of the identified major domains. These domains (also referred as a system) then can be combined, by giving different weights, to build multiple scenarios (also referred as a system-of-systems) to model any number of possibilities according to the practical needs.

It should be noted that CSSD (Figure 2-7) represents a static view of the elements of the scenario at a specific time stamp. However, the evolution of cyberspace and of its elements over time can be modeled by developing such scenarios for every discrete time-step as shown in Figure 2-7.

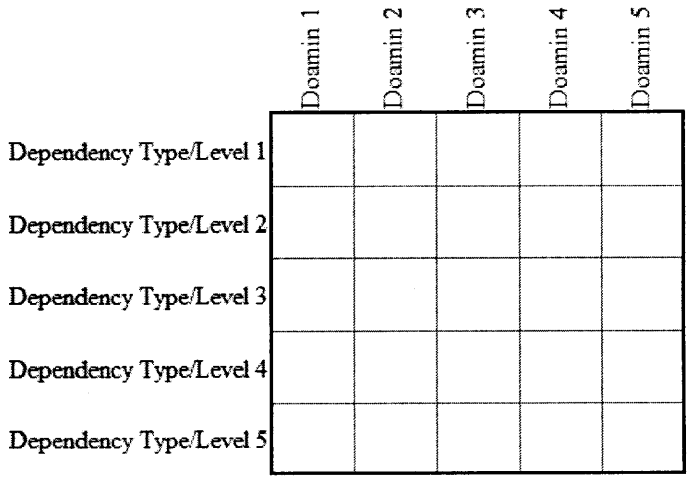


Figure 2-6: A two-dimensional array for classifying and storing different interventions in multiple domains.

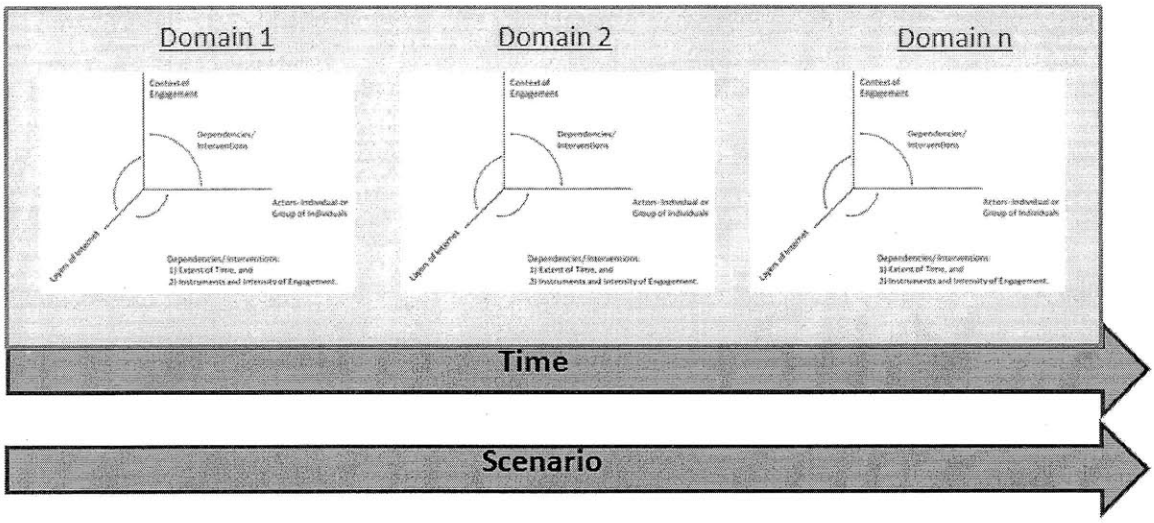


Figure 2-7: Developing cyberspace scenarios using CSSD framework.

2.5. Multi-Disciplinary Knowledge Domain Representation Frameworks

The CSSD framework presented earlier describes the different elements of a domain that constitute cyberspace. The framework, however, does not tell how the information and dependencies within each domain and among the domains are to be represented.

It is, thus, necessary to have an analytic tool for representing information flows and dependencies within the system. Bartolomei (2007) has scanned the literature on the representation frameworks for mapping complex systems. A comparison of different frameworks on multiple criteria is presented in Figure 2-8. A "++" in Figure 2-8 means that the framework scores high on that parameter, "+" means it scores medium and an empty cell represents that framework does not address that parameter.

Bartolomei's work (Figure 2-8) shows that many frameworks do not represent the system completely. A complete representation requires the capturing of "social domain interactions, stakeholder objectives, functional decomposition, technical descriptions of the

system, system development processes, as well as external factors that drive system behavior" (Mikaelian 2009).

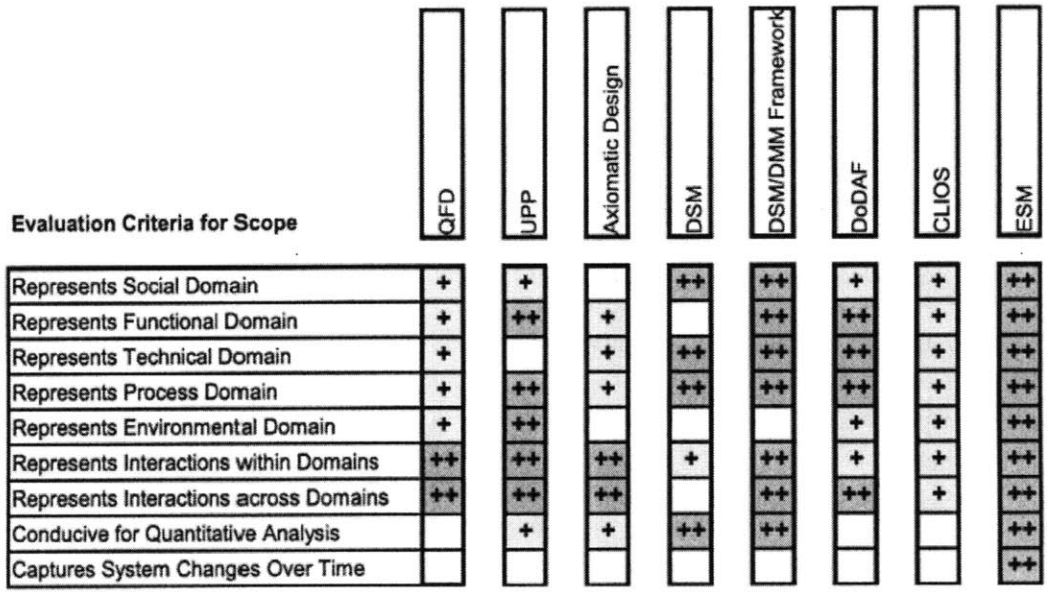


Figure 2-8 Comparison of knowledge representation frameworks[6] (Bartolomei 2007).

Figure 2-8 also shows that Engineering Systems Matrix (ESM) framework, an extension of Dependency Structure Matrix (DSM) and Domain Mapping Matrix (DMM) framework allows for end-to-end representation of a complex system. The next few sections will discuss the

---

[6] QFD- Quality Functional Deployment, (Akao 1990) ;UPP- Unified Program Planning, (Hill and Warfield 1972); Axiomatic Design, (Suh 1998); DoDAF- the Department of Defense Architecture Framework, (Department of Defense 2009); CLIOS- the Complex Large Integrated Open Systems, (Dodder, Sussman, and McConnell 2004); DSM- Dependency Structure Matrix (Steward 1962); DMM- the Domain Mapping Matrix, (Danilovic and Browning 2007); ESM- the Engineering Systems Matrix (Bartolomei 2007).

tools based on Engineering Systems Matrix, ESM or coupled-Dependence Structure Matrix, c-DSM in detail.

2.6. Dependency Structure Matrix

Representation of a system in terms of relationships between its constituent's elements requires system decomposition into sub-systems. This exercise generally involves the following steps (Browning 2001) :

a) Decompose the system into its constituent elements,

b) Understand and document the interactions between elements, and

c) Analyze the potential re integration of the elements.

A Dependency Structure Matrix (DSM) is a matrix-based information exchange tool for representation of the interactions between the elements or activities of a decomposed system. This section describes the basic DSM method and its application for modeling and analysis of a complex system like cyberspace.

Dependencies between two elements of a system may either be represented as a network-graph or can be mapped to an equivalent matrix representation. A DSM is the matrix representation of a network. It is useful for purposes of decomposition and integration of relationships among the element a system or domain. It is a square matrix with identical rows and columns, where both row and columns headers represent the same elements.

DSM indicates all one-step relationships or activity dependency between the two elements that correspond to entries in the cell. A "×" or 1 in an off-diagonal cell (Figure 2-9)

indicates that a dependency exists between the respective elements[7]. A blank cell or "0" represents that no dependency exists between them (Ledet and Himmelblau 1970). The main diagonal may contain the task symbol. Figure 2-9 shows the different type of dependencies that can be mapped using DSMs.

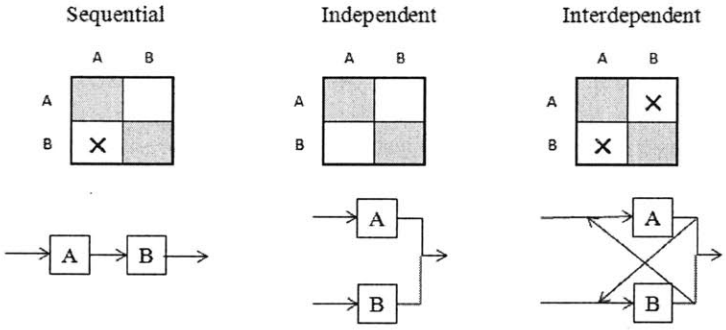


Figure 2-9: Relationships in a dependency structure matrix (Browning 2001).

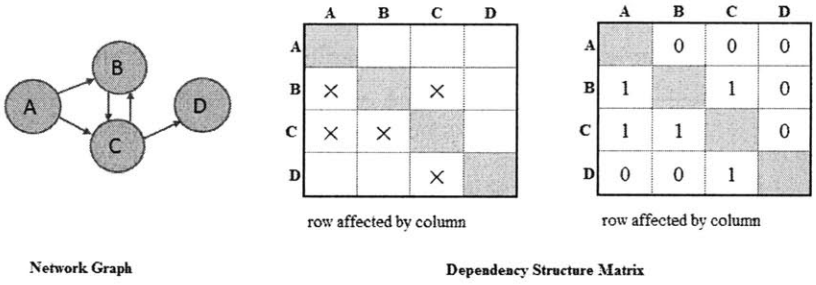


Figure 2-10: A dependency structure matrix example (Weck 2009).

If there are no iterative relationships between any two tasks, all the dependencies are in the lower triangular matrix, i.e. below the diagonal elements of the DSM. In practice, a level of reverse dependencies (or feedbacks) do exist between the elements and thus, a few elements in

[7] A dependency between an element "*i*" and element "*j*" (or *i* is affected by *j*) is represented by "×" or 1 entry in the row *i* and column j. Therefore, all of the structure of the network is contained in the DSM.

the upper triangular matrix (i.e. above the diagonal elements of the DSM) will be 1 or "×" (Ledet and Himmelblau 1970; Steward 1962). Figure 2-10 shows the DSM representation of a network graph with such iterative dependencies.

Sometimes matrix entries represent the weights of the dependencies. This relationship mapping in DSMs can also be based on a quantification scheme. A *quantification scheme* allows for the weighing the relationships to each other. A number, based on a quantification scheme, replaces the entries in the DSM (Danilovic and Browning 2007; Browning 2001). The quantification scheme can also be developed for probabilistic assessment of the relationship between the two elements. Weighting information is generally obtained by reviewing the system, interviewing domain experts or the like. Table 2-1 shows an example of a quantification scheme. Figure 2-11 shows the weighted model of network.

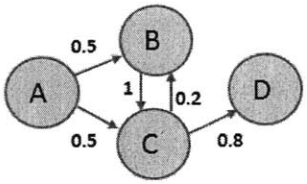
Table 2-1: Example of a quantification scheme (Pimmler and Eppinger 1994).

Required	2	Physical adjacency is necessary for functionality
Desired	1	Physical adjacency is beneficial , but not necessary for functionality
Indifferent	0	Physical adjacency does not affect functionality
Undesired	-1	Physical adjacency causes negative effect, but does not prevent functionality
Detrimental	-2	Physical adjacency must be prevented to achieve functionality

DSMs have been used to represent relationships in a wide variety of domains, such as the parameter based or component based practices. Based on its application, DSMs have been distinguished into two broad categories – Static and Time-based (Browning 1999).

Static DSMs are used for simultaneous representation of the system elements. Such DSMs are generally analyzed by clustering the DSMs. Time-based DSMs indicate the flow of activities through time, i.e. upstream activities in a process precede the downstream activities.

Sequencing techniques are generally used to analyze such DSMs. Section 2.8 will present the analysis techniques for the DSMs.



	A	B	C	D
A		0.5	0.5	0
B			1	0
C		0.2		0.8
D	0	0	0	

row affects column

Figure 2-11: A weighted DSM example.

2.7. Value of Coupled Dependency Structure Matrix

Eppinger et. al showed that the inter-domain analysis can help in identifying relationships between products, and processes and organizations (Sosa, Eppinger, and Rowles 2004; Eppinger and Salminen 2001). However, DSMs had a limited utility for inter-domain analysis. The utility of DSMs was earlier focused for analyzing the relationships within a single domain and have been applied to inter-domain analysis if all the domains have an equal number of elements, (a condition imposed by square DSM matrix) (Danilovic and Browning 2007).

To overcome this limitation, a Domain Mapping Matrix (DMM) can be developed as shown in Figure 2-12. The power of DMM lies in its capability to capture the relationship and dependencies between two domains or DSMs (Danilovic and Browning 2007). While a DSM is always a square matrix, DMM is usually a rectangular matrix where the row and columns map to elements of two different domains.

A coupled-dependency structure matrix (Danilovic and Browning 2007) is a combination of multiple DSMs, each representing a different domain, and corresponding DMMs that map relationships across any two domains. The diagonal matrix of a c-DSM is an array of DSMs, while off-diagonal matrices represent DMMs. The c-DSM provided traceability of interactions and an ability to analyze the impact of uncertainties and changes in the system[8].

Figure 2-12 shows the coupled-dependency structure matrix of a domain for exploring cyber-international relations. This c-DSM is based on the CSSD framework discussed earlier in section 2.1 of this chapter.

Separate c-DSMs will be made for each domain. As mentioned earlier, each domain will have its own set of activities. These c-DSMs can be then combined, by giving different weights to each domain, to build multiple scenarios for modeling any number of possibilities according to the practical needs.

Figure 2-13 shows an example of c-DSM for mapping an engineering research system. Along the diagonal of the c-DSM are two DSMs that model the different actors and their research activities. The off-diagonal matrices of the c-DSM models the intensity of engagement and extent of time of engagement - the two identified dependencies among the elements of different DSMs. The dotted line represents the system boundary. Elements inside the boundary are endogenous to the systems, while the elements outside the boundary are exogenous.

---

[8] At a particular time stamp, a c-DSM may represent the complete view of the system with edges connecting different elements. An element represents various entities such as actors and processes, and edges represent dependencies or influences among the elements. At the next time stamp, all the element and nodes of the c-DSM are updated. It should be noted that in a c-DSM edges do not represent transition among the states, where a state is the complete representation of the system (Mikaelian 2009).

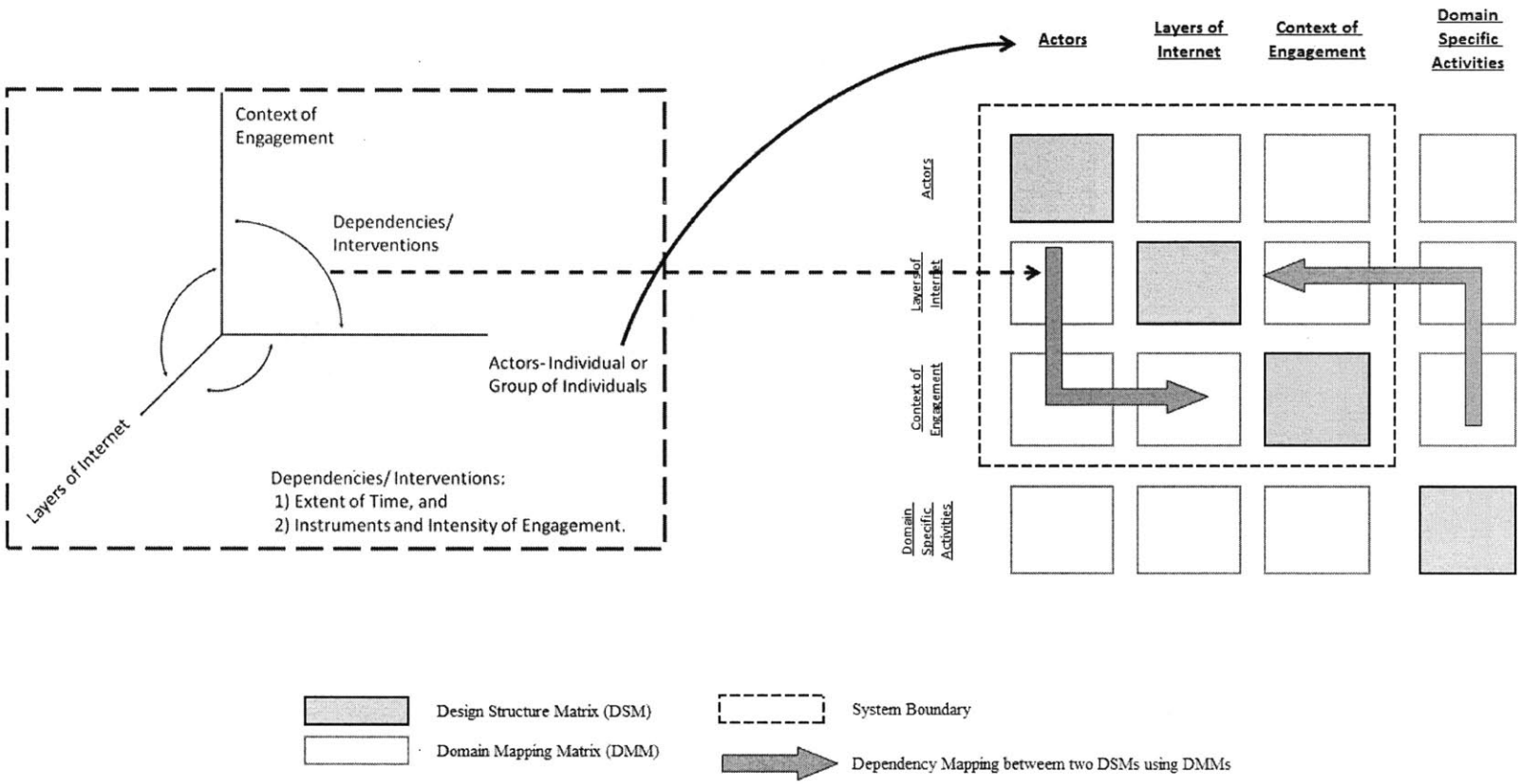


Figure 2-12 Mapping CSSD to c-DSM.

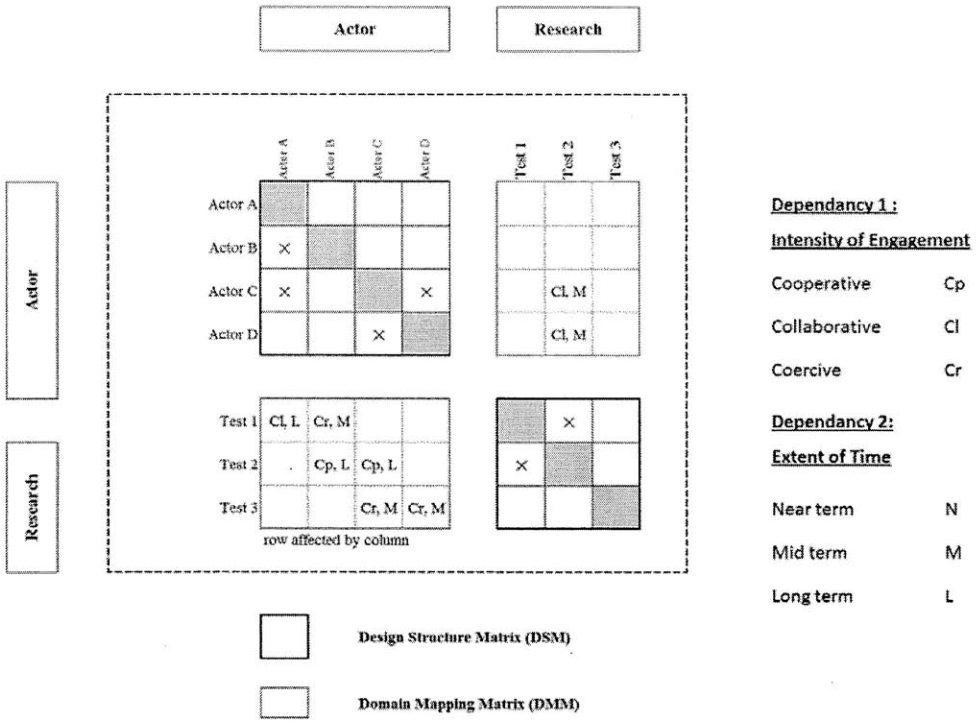


Figure 2-13: A c-DSM example.

The c-DSM acts as a repository of information about the interactions between the actors and the various tests being conducted. For example, from the actor DSM, it can be inferred that the actions of:

a) Actor B is affected by Actor A,

b) Actor C is affected by Actors A and D, and

c) Actor D is affected by Actor C.

In addition, from Research-DSM, one can infer that

a) Test 2 is affected by Test 1, and

b) Test 1 is affected by Test 2.

These two DSMs, independently, however, do not give any information on how these two domains, i.e. actors and the research, are connected to each other. A DMM provides this information. The lower DMM in Figure 2-13, thus, gives us the following information:

a) Test 1 is affected by Actor 1 and Actor 2, where
    i. Actor A's actions are collaborative on long-term basis, while
    ii. Actor B's actions are coercive on mid-term basis for the test.
b) Test 2 is affected by Actor B and Actor C, where actions of both actors are cooperative on long-term basis for the test.
c) Test 3 is affected by Actor C and Actor D, where actions of both actors are coercive on long-term basis for the test.

Further, as the tests are conducted, the results may affect the interactions between the actors, which are documented in the upper right DMM. For example, in this particular case, results of Test 2 changes the interaction of Actor C from long-term cooperation to mid-term collaboration. From the DMM it can also be inferred that Actor D is now interacting on long-term cooperative basis on test 2, which was not present earlier.

2.8. Dependency Structure Matrix based Analysis

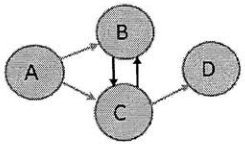
The power of c-DSM representation of a system lies in its ability to focus on interdependencies and relationship between domains. In order to meet this need of information exchange, this section presents two important DSM analysis tools, which are: (a) identification of higher order loops, and (b) clustering or partitioning.

Identification and analysis of higher order couplings between the elements of a system help in identifying feedback loops and gives the information about which activities can be carried out in parallel, in sequence or in a combination thereof. DSM clustering process

identifies where and how the different entities and dependencies can be grouped into meta-structures and how such meta-structures relate to each other. In DMMs, same techniques are used but across two domains.

2.8.1. Identification of Higher Order Loops

Higher order loops or couplings between the activities can be identified using a process of binary matrix multiplication (refer Appendix B for details). When a DSM is multiplied, the rows of DSM^2, DSM^3 and DSM^4, and DSM^5 correspond to the vertices to which the dependencies are directed, and the columns correspond to the vertices from which the dependencies are directed. Each non-zero element of the DSM^k matrix indicates that there is a path going through k edges (a k-step path) from vertex j to vertex i. A k^{th} order loop in the network graph is defined as a set of k vertices each of which is connected to every other vertex of the loop by a closed path. Thus, if a diagonal cell is 1, it can be inferred that there is a loop passing through that element. Figure 2-14 indicates that a two-step path dependency B-C-B exists between nodes B and C. Figure 2-15 shows an example for third-order dependency loop B-C-D-B between elements B, C, and D.



DSM

	A	B	C	D
A		0	0	0
B	1		1	0
C	1	1		0
D	0	0	1	

row affected by column

DSM^2

	A	B	C	D
A	0	0	0	0
B	1	**1**	0	0
C	1	0	**1**	0
D	1	1	0	0

row affected by column

Figure 2-14 : Second-order path dependency in a DSM (Weck 2009).

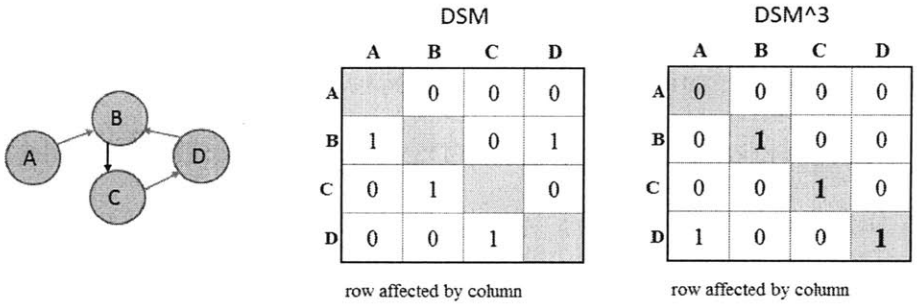


Figure 2-15: Third-order path dependency in a DSM (Weck 2009).

2.8.2. DSM Clustering

DSM clustering (or partitioning) is the process of grouping the constituent elements of the system into subsets that are either mutually exclusive or have a very little dependence/ interface between the subsets. The purpose of DSM clustering is to embed the dependencies internally in a subset, such that the newly identified subsets can be processed either sequentially or in parallel without any iteration among the subsets. Figure 2-16 shows a DSM before and after partitioning.

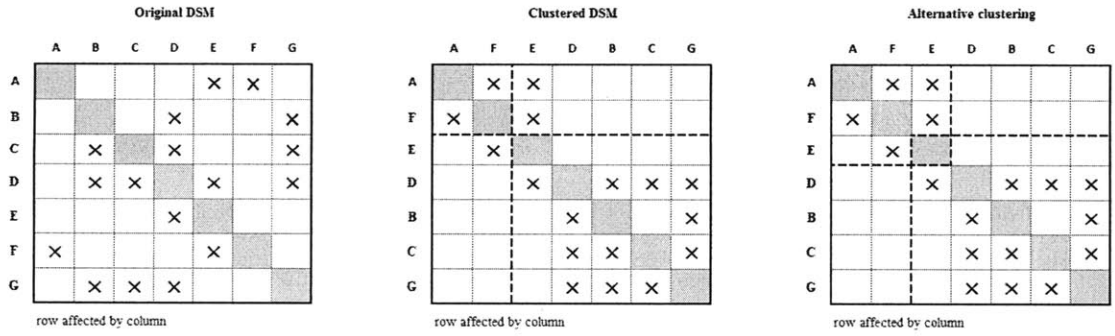


Figure 2-16 : A DSM clustering example, (Sharman and Yassine 2007).

The original DSM is now clustered into two meta-tasks (AF and EDBCG), which now contain most of the dependencies. The dependencies outside the meta-tasks act as the

interface between the meta-tasks. The alternate clustering scheme as element E common in both meta tasks (AFE and EDBCG) (Sharman and Yassine 2007).

While the above discussion was focused on DSM, the methods can be applied to DMMs and c-DSMs. Bartolomei (2007) and Danilovic et al.(2007) have investigated the application of these DSM tools to DMMs and c-DSMs in detail. However, temporal and spatial changes in the dependencies make their application to c-DSM challenging. The next section will discuss some of these challenges.

2.9. Challenges Faced in Dependency Structure Matrix Implementation

Because of both temporal and spatial nature of the c-DSM, the c-DSM framework presents two challenges related to its scalability. First being, whether the framework itself is scalable or not and if it is, is the level of effort required to make it scalable (Mikaelian 2009).This first issue is addressed by ensuring that the integrative elements (e.g. data busses) which interact substantially with all the meta-tasks are outside the meta-tasks and if required, they are clustered as "control meta-tasks" that interact with all other meta-tasks (Browning 2001). Mikaelian (2009) has presented an example based on swarm of unmanned aerial vehicles, addressing the same issue.

The second issue of scalability can be addressed by selecting an appropriate level of abstraction. Selecting a correct level of abstraction is challenging (Bartolomei 2007). A very high level of abstraction may result in c-DSM in which all the elements are dependent on each other, while a highly decomposed c-DSM may have details irrelevant to the problem.

This issue can be addressed by using a distributive method to make c-DSMs in which stakeholders themselves make multiple c-DSMs. This process helps in increasing the emphasis on the representation of dependencies and helps in identifying and developing scenarios

important to different groups of actors. It also helps in identifying the conflicting scenarios (Mikaelian 2009). The disadvantage of this method, that it will require a lot of effort in coordinating the efforts of multiple individuals (Mikaelian 2009).This issue can be addressed by developing an automated tool to capture different actors, processes etc, and the interdependencies between them.

2.10. Summary

This chapter focused on the task 1 of the research methodology, i.e. developing a knowledge mapping framework. It presented the research done in characterizing the cyberspace as a socio-economic-technical-legal system. It also presented an analytical tool for knowledge representation for modeling the cyberspace.

The first part of the chapter presented the background of complex systems like cyberspace and importance of different modalities while mapping multi-disciplinary knowledge domain of cyberspace. The chapter then presents Cyber System of Strategic Decisions (CSSD) framework of describing the cyberspace through three dimensions and two interdependencies among those dimensions. This framework enables a holistic identification of the elements of a system, which are structured as set of multi-dimensional and hierarchical relationships

The second part of the chapter describes a matrix-based analytic tool, *coupled – dependency structure matrix* (c-DSM). The c-DSM was then adapted to the CSSD framework. The chapter then discusses analysis methods based on DSM. It also discusses the scalability challenges faced and methods to mitigate them while developing c-DSMs.

The following chapter will expand the individual dimensions of CSSD, which is important for making the framework robust, effective, and uniform manner across multi domains.

This page is intentionally left blank.

3. CYBER SYSTEM FOR STRATEGIC DECISIONS FRAMEWORK

The purpose of this chapter is to expand individual dimensions of the conceptual Cyber System for Strategic Decisions (CSSD) framework, presented earlier in the Chapter 2. The motivation for this chapter is the need to enhance the visibility of the information to improve the decision making under uncertainty, as it affects the current and future shape of the Internet and actors who control it. This chapter focuses on the dimensions of *actors- individuals and group of individuals*, *layers of the Internet* and the *extent of engagement*, and the two dependencies- *the instruments and intensity of engagement*, and *the extent of time of engagement*. The structure of the chapter is shown in Figure 3-1. The chapter then discusses a few important domains – economy, social, and technology domain. Activities in these domains affect both the real environment and the cyberspace.

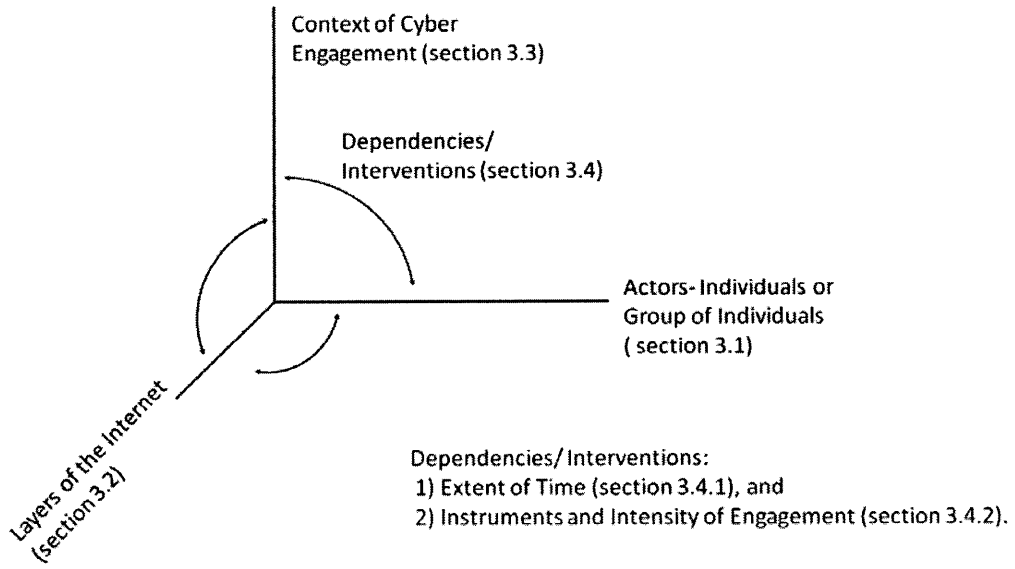


Figure 3-1 : CSSD dimensions.

3.1. Actors- Individual and Group of Individuals

This section catalogues the different types of actors which are involved in the creation, management, regulation, control and use of cyberspace, and all others whose operation in the cyberspace affect all the other actors in the real world as well as in cyberspace. It is necessary to understand that most of these actors are multi-faceted and complex, and cannot be classified into one class based on one attribute.

Appreciation of this social dimension of strategy requires that "strategy is made and executed by the individuals, social institutions, and (or) communities formed by the human beings" (Gray 1999, 1-6). Further, their respective needs lie within the Clausewitz's remarkable trinity- "composed of primordial violence, hatred, and enmity ... the play of chance and probability, and the element of subordination" (Clausewitz et al. 2006, 89).

These institutions are governed by some form of decision-making bodies and are defended by a protection mechanism. Civil remedies (e.g. regulatory and judicial actions) and ultimate use of armed forces are few examples of such protection mechanisms. The complex relationship between an individual, community/institutions/society, government and the protection mechanisms requires a balance amongst different actors (Kollock 1998).Figure 3-2 shows the different categories of actors considered in this thesis.

3.1.1. Individuals

The human dimension of the strategy is the most basic dimension. At all the relevant levels of analysis, whether it is for land-power, sea power, air power, space-power, or cyber-power, the real people make and execute strategy. Strategy is made and executed to serve the interests of human communities by tactics and tactics are applied by communities and forces in which human beings do the fighting (Gray 1999, 26).

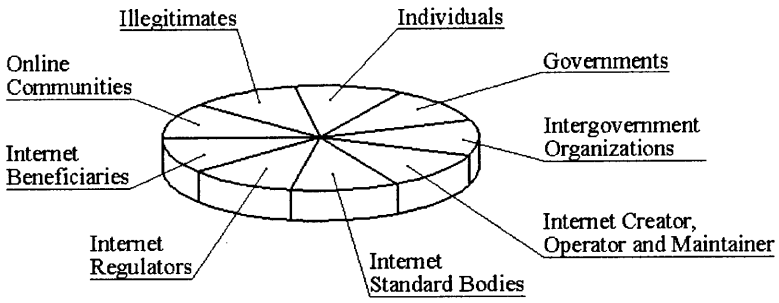


Figure 3-2: Categorization of actors- individuals and group of individuals[9] (Clark 2010).

A form of strategic power can be exercised through attacks on the global information grid. It is plausible that people may become somewhat removed from the physical act of warfare, and it may not be difficult to forget the real people who execute and do strategy. However, this statement is only valid if so-called 'strategic information warfare' proves to be a war-winning instrument (Rattray 2001). Rapid recovery of Estonia after the 2007 denial-of service attack suggests that the extent of such strategic attacks is limited (Lonsdale 2009). Nonetheless, it is still the people, who normally decide and are required to face the harsh realities of any act.

3.1.2. Governments and Intergovernmental Cooperative Agencies

Being the traditional actors on the stage of international relations, governments and "intergovernmental cooperative agencies" play an important role in this analysis (Clark 2010). They can have multiple objectives and have many tools at their disposal. Such tools, which are generally traditional and may not exploit the features of cyberspace, include policy making and legislation, investments in infrastructure development and in research etc. However, they can act

[9] Based on author's discussions with Dr. David Clark and Dr. Nazli Choucri at MIT Cambridge 02139. February 2010.

directly in cyberspace, and can induce direct actions by other actors. Such actions include use of power instruments, which range from coercive to cooperative actions.

3.1.3. Real Communities

Communities that have an extensive impact on an individual's day-to-day life can be differentiated into real and online communities. The **real communities** not only have a physical presence, but also often have rigid community standards or norms. Further, they enforce those standards or norms to preserve the values and legitimacy of the community (Murray 2007, 129-132). It is difficult to think of purely online equivalents of real communities like businesses (e.g. General Electric Company, ABB, etc.), and professional organizations (e.g. IEEE and AIAA) and the like. The online presence of such communities is an extension of their physical presence. Leaving the online equivalent is easy and quick but for leaving the real community, a switching cost may be exerted on its members. For the Internet environment, these communities can be classified into:

a) **Internet Creators, Operators, and Maintainers:** This community includes the businesses that create and support the cyberspace and the Internet.

b) **Internet Standards Bodies and Regulators:** At the technical level, Internet is made possible by the design, development, testing, and implementation of such Internet standards developed by a diverse group of standards bodies and regulators.

c) **Internet Beneficiaries**: This is a group of established commercial and non-commercial communities (or for profit and not-for profit), which are highly affected by using Internet services.

3.1.4. Online Communities

Online communities are focused on a particular aspect of an individual's life, usually social life. Such communities have lower entry and exit barriers. Further, the switching cost of this mobility is much lower than the real communities (Murray 2007, 145).

The virtual nature of cyberspace diminishes the possibilities of the creation of online-real communities. Further, it acts as an extension to real world with very low barriers to leave and return to the real world. It is a place where we "visit" not live for pleasure or to do transactions.

3.1.5. Illegitimates

This category includes communities that are deliberately structured to protect its members from the legitimate actions of the authorities. The actors include emerging state and non-state actors using tools like P2P networks and terrorism. The activities involve classic crime categories such as confidence games, extortion, fraud, identity theft, etc.

3.2. Layers of the Internet

It is essential to recognize the function played by the stratified layers in the communication system to understand the socio-economic-technological-political system of cyberspace.

The architecture of the Internet can be classified into the transmission layer, the computer layer, the software layer or the content layer as identified by Tim Berners Lee in his book "*Weaving the Web*" (Berners-Lee and Fischetti 1999). This model is a simplified version of the seven-layer "*Open System Interconnection*" *(OSI)* reference model (Zimmermann 1980).

The characteristic of this model is that it divides the functions of the protocols into a series of layers and functionality in each layer is built on the layer below it.

The regulation and control of the Internet in this model is possible vertically only in one direction. By changing the operating envelope in one the supporting layers, it is possible to change or regulate the activities in the upper layer(s). Further, this control can be implemented in either hardware or software, or both. These two models can further be reduced to three layers as shown in Figure 3-3 (Clark 2010, 2009, 2010). These three layers are:

a) The physical infrastructure layer,

b) The logical infrastructure layer, and

c) The information layer.

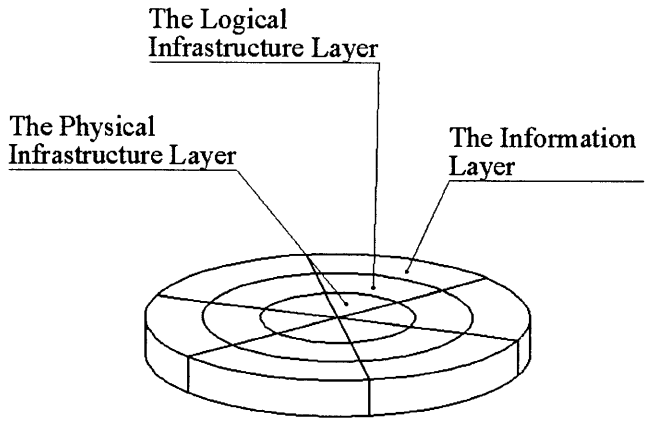


Figure 3-3: Layers of the Internet[10] (Clark 2010, 2009).

3.2.1. The Physical Infrastructure Layer

The physical layer of cyberspace is the foundation layer of Internet. It includes all the essential physical devices on which it is built and is essential for the network to function. These

[10] Based on author's discussions with Dr. David Clark at MIT Cambridge 02139. February 2010.

tangible devices, which have grounded sense of location, are capable of processing and two-way transmission of intelligent information over a link between spaced apart locations. The term "intelligent" used above is intended to include the capability for transmission of speech or data (e.g., music and data), rather than restriction to a specified audible signal, such as a bell or buzzer. The devices that constitute the Internet include computing devices like end-user terminals (PCs, laptops, mobile devices including smart phones), servers, sensors and transducers, and all sort communication channels.

3.2.2. The Logical Infrastructure Layer

The logical infrastructure layer sits on the top of the physical infrastructure layer. The layer constitutes all the necessary software components (e.g. operating systems and browsers) and network protocols like TCP/IP, HTTP UMTS and many others (Protocols.com 2010) that are necessary for the creation, transfer and delivery, storage of data/information. This layer provides logic and inter-connectivity between different devices. Logical infrastructure layer provides both the strength and limitations of the cyberspace as the decisions that design and regulate the cyberspace appear on this layer.

The logical infrastructure layer allows an actor to build a completely different system by taking a different logic of interconnectivity, using the same physical infrastructure within the constraints of laws of physics(Clark 2010).[11] For example, it is possible to make a closed and rigid system with fixed functionality using a different architecture like in an air-traffic management system.

---

[11] Based on author's discussions with Dr. David Clark at MIT Faculty Club, MIT Cambridge 02139. February 2010.

Further, it also allows for an open-platform architecture of the Internet, ensuring that "there would be no global control at the operational level" of the Internet (Barry M. Leiner et al. 2010). Open-platform architecture has published external programming interfaces that allow the system to function in other ways than the original actor intended, without requiring modification of the underlying logic. It can, thus, act as a platform on which new capabilities can be built, which in turn can become the platform for the next round of innovation (e.g. Facebook.com, which is built on a platform, further acts as a platform for different applications) (Clark 2010).

The physical infrastructure is important, but it is bounded by the laws of physics. The logical infrastructure layer allows for governing the fluidity of the system. Further, in order to have a maximum control on the Internet one has to identify the vulnerabilities or the "hooks" (which allows for attempts for phishing and denial of service attacks) in this layer where regulatory controls can be enforced to have a maximum effect on the Internet users.

3.2.3. The Information Layer

On the top of the logical infrastructure layer sits the information or content layer. This layer encompasses all the digital material created, processed, stored, transmitted, or accessed using the logical and physical infrastructure layer. This information can take various "intelligible" forms like – web pages; music and video; photographs and books; business databases and records; meta-data about the information itself.

This data, which was processed by individually by isolated computers before the availability of network capability, is now done on shared resources of supercomputers or through distributed computational resources like cloud computing. Similarly, this information was earlier stored on isolated storage devices, like compact disks, is now available on distributed storage devices like a data warehouse and can be " mined" for extracting the useful meaning.

Based on the logical and physical infrastructures, the information can now be dynamically "personalized" and made available on demand, thus blurring the boundaries between storage and computation. Further, rights over ownership, authenticity, and dependability will be of more concern and critical as more and more information moves online.[12]

3.3. Context of Cyber Engagement

When the demands of a society are unmet or existing capabilities are insufficient to meet them, there arises a need to develop new capabilities. However, the ability of a society to develop the required capabilities depends on the existing capabilities. If they are not available within its boundaries at reasonable, it looks for the same beyond its borders. Choucri and North (1975, 16-19) have referred this process as Lateral Pressure. The lateral pressure theory has three distinctive aspects, which are:

a) The disposition to extend activities beyond the national boundaries,

b) The particular activities that result from the disposition of the act, and

c) The impact of these activities has on the people of another country and their environment.

Operations in cyberspace have affected this process of lateral pressure in almost all the domains ranging from commerce to war. In comparison to other domains of control and influence, the barriers to entry in the cyberspace are so low that non-state actors and small states can play significant roles at low levels of cost. For many actors, it has become a foundation domain to extend their influence or superiority. Further, operations in cyberspace acts as an enabler in domains outside cyberspace like critical infrastructure, financial institutions and net-

---

[12] Based on author's discussions with Dr. David Clark at MIT Faculty Club, MIT Cambridge 02139. February 2010.

centric warfare military in the existing under water, water, land, air and space domains, while providing a new space where it can deliver effects.

The **context of cyber engagement** (Figure 3-4) is broadly divided into three categories to produce a preferred level of cyber operations:

a) **Protection of Interest** is the "ability to keep an unblinking eye on any entity-to provide warning on capabilities and intentions, as well as identify needs and opportunities"(Berg 2008, 12).

b) **Expansion of Interest** is the "ability to move, supply or position assets--with unrivaled velocity and precision anywhere" (Berg 2008, 12).

c) **Power Projections** is the "ability to create and sustain effects of all kinds" (Berg 2008, 12) in each of the cyberspace domain based on ability to both protect and expand interests.

Three cost functions (Brooks and Breazeal 2006) should be used to compute the cost of an action when acting, deterring or being dynamically agile. The first cost is associated with the evaluation of current spatial and temporal location to determine if the new state is safer than the current one. This is followed by evaluating the cost associated to taking an action. This will help in evaluating multiple options available and preferring one over the others. The final cost is associated with the cost to reach each new location. This heuristics gives the user an estimate of the cost of each action and allows for making informed decisions to selecting (or sacrificing) options for execution speed over the optimality guarantees cost to reach each location.

3.3.1. Protection of Interest

Protection of interest is " the ability to keep an unblinking eye on any entity--to provide warning on capabilities and intentions, as well as identify needs and opportunities" (Berg 2008).

The vigilant activities that form are required for the protection of interest include (Jabbour 2009) :

a) Persistent, global multi-domain situational awareness,

b) Assurance and trust, and

c) Threat avoidance.

Situational Awareness is a "combination of perception of elements in the environments within a volume of time and space, the comprehension of their meaning and the projection of their status in near future" (Endsley 1995).

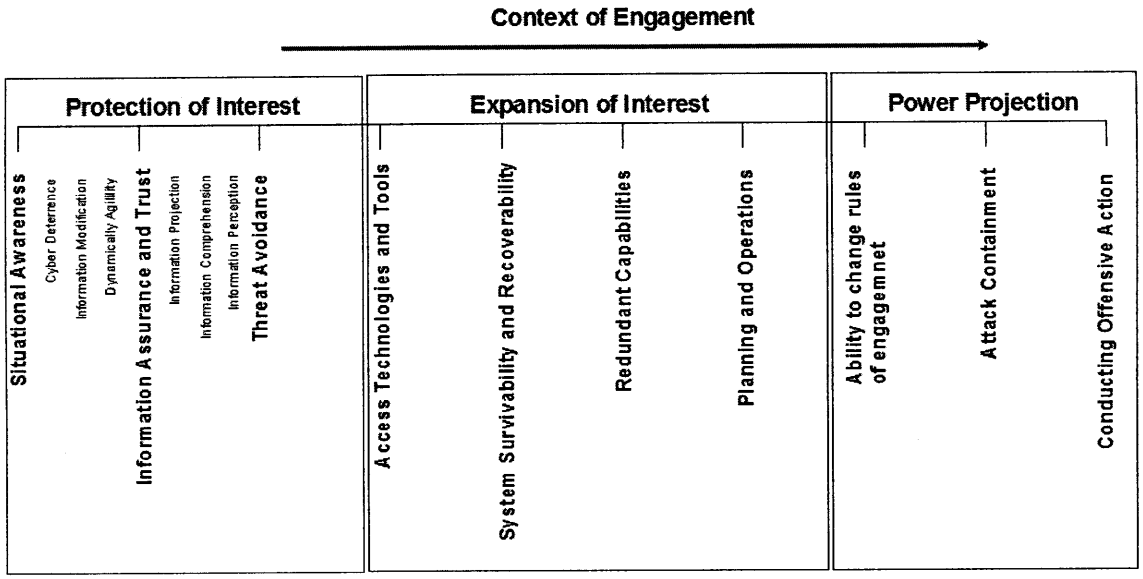


Figure 3-4: Context of cyber engagement.

Perception includes the activities of sensing, real-time collection, long-term storage, and aggregation of meaningful data/information. **Comprehension** of the perceived data/ information involves the understanding and contextual placement in the control environment, and making a sense of their meaning. Based on the current status, **projection** allows for

understanding the plausible strength, weakness, opportunities, and threats in the future and possible course-of-actions within pre-negotiated rules-of-engagement.

The Joint Publication 3-13 (Department of Defense 2006) defines the **information assurance** as "measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities." It is further necessary to have a **trust** on the hardware, software and on the integrity of both static and dynamic data as it is generated by the system.

The defensive strategy of **threat avoidance** allows an actor to reduce or eliminate a need to get into a conflict. The treat avoidance includes activities of **deterrence** to prevent initiation of conflict, make an attack irrelevant by **modifying** the domain or making it inaccessible. Further, one can evade the threat by being **dynamically agile** through the detection of anomalous activities, quick analysis and anticipation of future behaviors and effects (Jabbour 2009).

3.3.2. Expansion of Interest

Expansion of interest is the *"ability to move, supply or position assets--with unrivaled velocity and precision anywhere" (Berg 2008).*

The system should have the **redundant capabilities** to **survive, recover and function continually** during and after an incident or attack, thus, reducing the system vulnerability to damage and failure events. These survivable systems require that the redundancy of the auxiliary control system (or the governing mechanism) be greater than or equivalent to the redundancy inherent in the system (Drew and Scheidt 2004). Richards et al. (2008) presents a process for an empirical validation of design principles for survivable system architectures.

3.3.3. Power Projection

Power projection is the *"ability to create and sustain effects of all kinds"* (Berg 2008, 12) in each of the cyberspace domain based on the ability to both protect and expand interests.

Delivery of this global power requires command and control over communication networks and computer systems, and its integration with traditional intelligence and surveillance tools. Furthermore, it requires an actor's ability to develop and deliver cyber munitions, and to estimate and act on first-order and subsequent higher order effects of any cyber operations both in cyberspace and in the real world. Cyber power also empowers an actor to change rules-of-engagement in a socio-economic-technological- political environment by (Nye 2004, Chapter 1):

a) Making others do something contrary to their initial preferences or strategies;
b) Framing the environment which limits the options available to other actors by discounting their strategies;
c) Shaping other actors preferences in such a way that the other actor never considers certain options/strategies;
d) Acting for attack containment within rule-of-engagement and conducting offensive action.

3.4. Dependencies

Because of the complex nature of the environment, one cannot expect to control the system by just alerting one or few of the interventions. As with any environment, mapping or forecasting interventions between the various entities is difficult.

In CSSD, the **Instruments and Intensity of Engagement,** and **Extent of Time** for engagement are two the identified dependencies, which will be used to map the interactions between any two or more of the above mention different entities.

3.4.1. Instruments and Intensity of Engagement

The due process of the protection, expansion, and projection of both interests and power by different actors across the different layers of the Internet goes through a process of discussion, deliberation, and debate to pass a democratic test. Further, the dynamics of engagement does not rely on a single-state deliberative process. One's ability to affect other's behavior ranges from coercive to cooperative action as shown in Figure 3-5 (Nye 2004, 8; 2010). For analytical modeling, each behavior can be estimated on either a linear or an exponential scale.

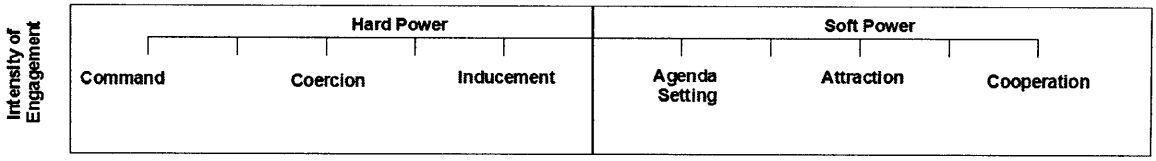


Figure 3-5: Intensity of engagement, adapted from Nye(2004, 8; 2010).

Coercive or hard power is the ability to change what other do by use inducement. Cooperative or soft power is the ability to shape the needs of the other actors based one's attractiveness or ability to manipulate one's preferences in a manner that makes other fail to express it (Nye 2004, 6-8). Carr (1981, 108) has further classified the intensity of engagement into three categories of power: power over opinion, economic power and military power with different relative strengths in different situations.

The Internet/ cyberspace have enabled the creation of online communities, which extend beyond the national boundaries. In this arena, both governmental and non-governmental actors are playing a big role and are trying to increase their soft power. Players who have multiple communications channels to share information for framing issues and have their cultures and norms close to global norms are likely to gain soft power and enhance their credibility. They can make use of other jurisdictions to circumvent their own jurisdiction. Further, they can pursue

roles in global communities that suit their purpose and interests and, when opportunities arise, they can move to other such communities or organization structure.

3.4.2. Extent of Time

The final dimension to be introduced is the "extent of time."[13] The evolution, deployment, execution, and sustainment of the system are affected by the clock speed. The clock speed aids in strategic decision-making and cyberspace has offered to accomplish such operations more rapidly than in the past. To help convey the complexity of the subject, the activities on the time are broadly categorized into the following categories (Figure 3-6):

a) Far-term planning decisions and investments;

b) Mid-term system /policy planning;

c) Mid-term system and policy deployment;

d) Near-term/real time system/policy execution.

Long-term planning decisions and investments can be implemented through the creation of prioritized solutions like roadmaps. These roadmaps help in documenting the programs of record, identifying future missions and operational needs, needs and expectation from future technologies and systems. The extent and intensity of such engagements have been discussed earlier in sections 3.3 and 3.4.1.

Long-term planning also helps in the identification the capabilities of the systems that are in development today and support (e.g. test and evaluation) needed for those capabilities. These activities are generally governed by 10-year, 5-year, biannual, or annual budget cycles.

---

[13] Based on author's joint work with Dr. Tsoline Mikaelian and Dr. Ricardo Valerdi for PATFrame research project at Lean Advancement Initiative, MIT, Cambridge, 02139. Fall 2009.

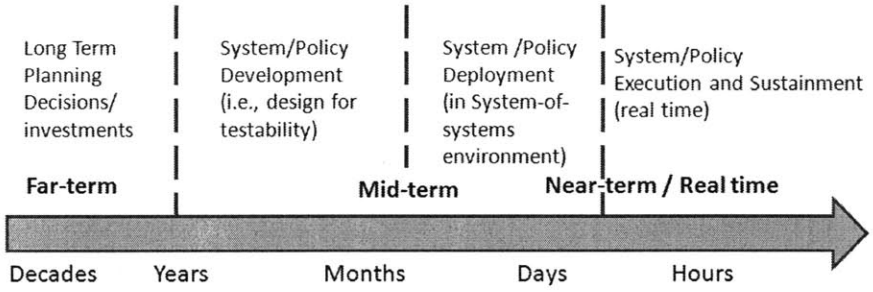


Figure 3-6: Extent of the time of engagement[14].

When examined as a collection, the technologies and policies identified in the separate platform roadmaps or in the family-of-systems roadmap for the system/policy planning and deployment, **mid-term** activities can be phase lagged from far-term to near-term needs (ranging from years to days). Activities in this time frame help in fostering the development and practice of policies, standards, and procedures that enable safe and effective operations between different systems both manned and unmanned.

The **near-term/real-time** execution of the system involves monitoring of system/policy effectiveness and operational assessment of capabilities at the component level, the system level, and the family-of-systems level. To analyze performance, measures of performance need to be expanded to include measures of effectiveness and 'ilities' such as adaptability, flexibility, and collaborative interoperability.

3.5. Cyberspace Environment

In context of cyberspace, the framework for characterizing the boundaries of a complex system in the real world comprises of different domains of engagement. These domains, which

---

[14] Based on author's joint work with Dr. Tsoline Mikaelian and Dr. Ricardo Valerdi for PATFrame research project at Lean Advancement Initiative, MIT, Cambridge, 02139. Fall 2009.

exist in the real world, constitutes of human individuals (or group of individual) to fully intelligent systems capable of autonomous planning, control and adaptive behavior. They also constitute different set of activities within the domain that can shape the functional specification and architectural outline of the cyberspace.

Economy, social system, technological system, intellectual property rights are a few such domains. The CSSD model will have an individual three-dimensional lattice for each of the identified major domains. The list of driving forces discussed here is not comprehensive and can be expanded further. Chapter 4 will attempt to explore the applicability of CSSD to intellectual property rights domain as test use-case.

3.5.1. Economy Domain

Internet has a major influence on the design of economic activities for general business activities (like telemarketing) to sector platforms like banking, logistics and retail. As the nations and businesses continue to build an Internet-based economy to improve the key factors like accessibility, affordability, and utility of products and services, it is important to comprehend how the intensity of demand for Internet based economy is set by prosperity, constrained by trust, business confidence, education in technology, and technical constraints such as throughput per unit cost.

Efficient ways for information flow, enabled by Internet, has provided opportunities to business for more effective organizational styles and structures, **business practices** through which they may gain certain advantages. Further, this domain should explore and reflect on the role of Internet on(Brown et al. 2010):

a) Commercial interests of businesses (both profit and non-profit) using mass-market tools based on the Internet;

b) Internet infrastructure providers;

c) Web censorship i.e. freedom of speech and thought that comes with global Internet exchange;

d) Government attitude and its role in controlling and endorsing commercial environment;

e) Identification and authentication interactions: Identification and authentication are distinct activities. Identification is a process whereby someone's identity is revealed whilst authentication is a process that results in a person being accepted as authorized to engage in, or perform some activity;

f) Privacy, which is the ability of an individual to protect his/her information;

g) Security, which is the ability to protect the information already available in public domain.

Discussions on the above (trust, identity, ubiquity, inclusion, and openness) may lead to the overarching theme of how can governments shape technology.

3.5.2. Technology Domain

The Internet has provided a universal and even platform to share information. It is further desirable that information from anybody can be related to anybody (though some actors like owners of knowledge may not find it desirable). The technology implemented, thus, should (Brown et al. 2010):

a) Provide a plain level- field for interactions, i.e. low cost barrier to enter with no jurisdictional boundary between state and non-state actors;

b) Provide an open-architecture with some safety net to cover any failure;

c) Allow Internet to be flexible enough to shift among different future scenarios to avoid any long-term lock-in in any one scenario or technology;

d) Provide with a capability to preserve generality and allowing it to evolve.

3.5.3. Social Domain

The Internet has also become a major interaction platform and it act as channel to facilitate a communication between humans through human signs and markers e.g., visual, audio, gestural and tactic. It is important to understand how new technological standards both affect and are affected by societal norms. This domain should explore and reflect on the role of Internet on (Brown et al. 2010):

a) Social norms or the acceptable behavior, i.e. constraints set by communities on capabilities and activities;

b) Self-actualization of an individual's (or group of individuals) participation on the Internet through personalization of services;

c) Social exclusion of an individual because of lack of individual skills, capabilities to access Internet and role played by Internet (and language used) for and against segregation.

It is also important to understand how new technological standards may or may not (Brown et al. 2010):

a) Affect the psychology of trust and hence privacy;

b) Propagate linguistic and cultural barriers;

c) Facilitate relationships and change the form human relationships;

d) Impacts an individual's position in the society;

e) Desire for immediacy and rich media interactions.

3.6. Shared Goals

The reference framework and dimensions presented in this chapter seeks to characterize the boundaries of a complex domain (or system) of the cyberspace. These domains (also referred as a *system*) can then be combined, by giving different weights to each domain, to build multiple scenarios (also referred as a *system-of-systems*) to model any number of possibilities according

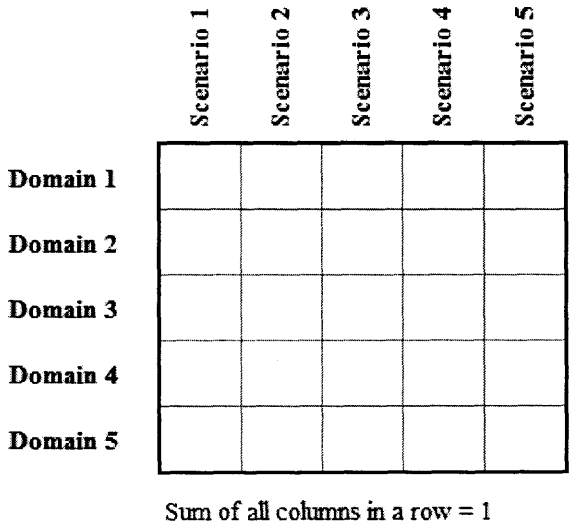


Figure 3-7: A scenario matrix.

to the practical needs. The weights can be added in the matrix, as shown in Figure 3-7, to give the relative weight age (or the probability of happening) of each domain in a particular scenario. It should, however, be noted that CSSD represents a static view of the scenario, i.e. it shows the view of the world at a specific time stamp. However, the evolution of cyberspace can be modeled by developing such scenarios for discrete time steps.

3.7. Summary

This chapter focused on the individual dimensions of CSSD framework and the dependencies across those dimensions as presented in Chapter 2, forming the foundation of task 2 and 3 of the research methodology.

This decomposition of the framework was based on generic and commonsense terminology used in the knowledge representation. This was done for ensuring that the framework can be used to map different domain (e.g. economy, social, and technology domain) that affect both the cyberspace and the real world.

Care was taken to ensure that the number of actors and stakeholders who participate in the articulation of propositions, and propositions themselves are accurately represented. Figure 3-8 represents the individual categories within each dimension of actors- *individuals and group of individuals*, *layers of the Internet* and the *extent of engagement*, and the two dependencies- *the instruments and intensity of engagement*, and *the extent of time of engagement.*

Finally, a method was presented to combine different domains by giving different weights to each domain to build multiple scenarios to model any number of possibilities according to the practical needs. The next chapter will focus on a use-case for testing the application of the framework in one of the domains.

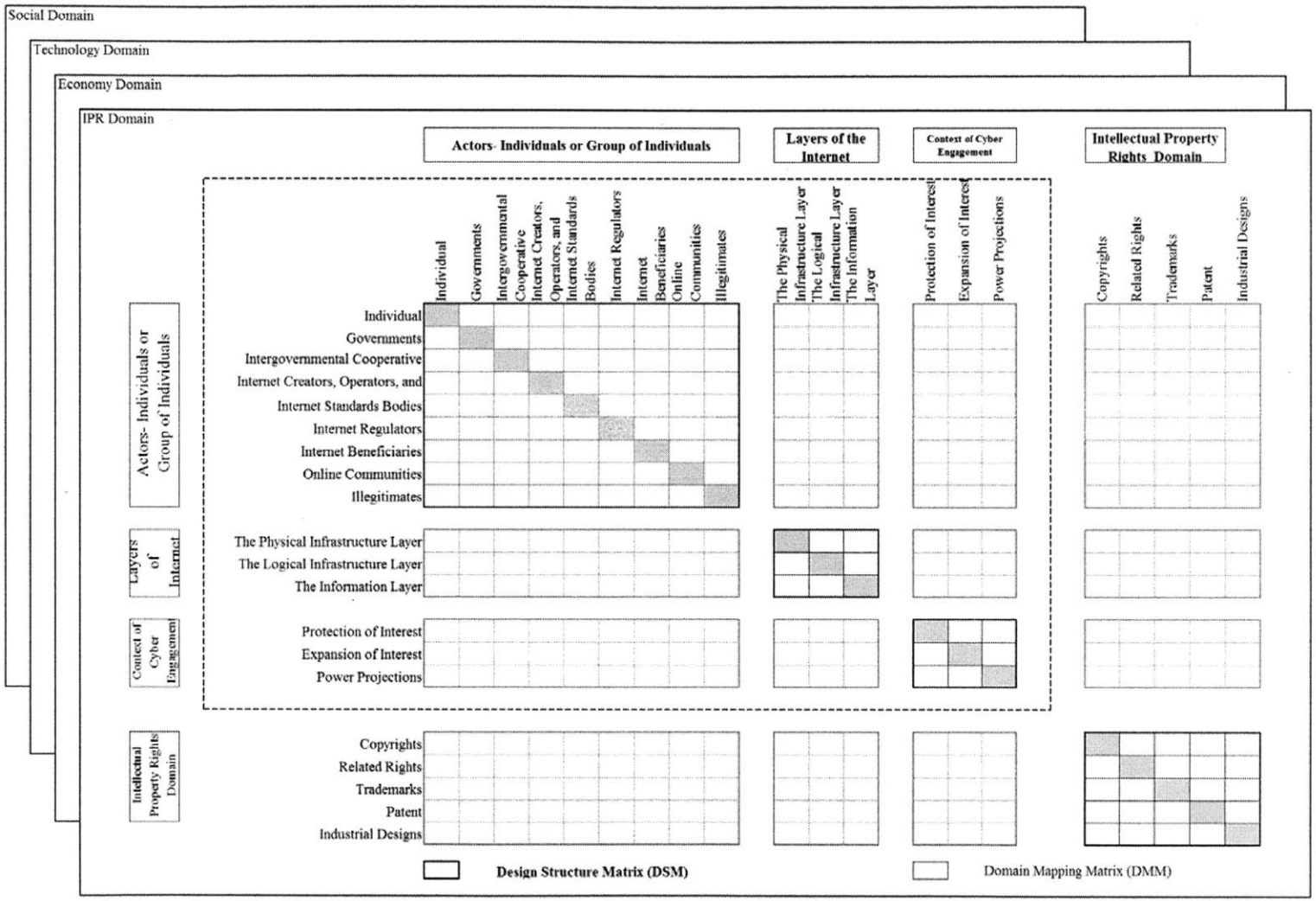


Figure 3-8 c-DSM for a single CSSD domain.

4. MODELING CSSD FOR INTELLECTUAL PROPERTY RIGHTS

This chapter presents a strong, comprehensive, and coherent use-case that tests the CSSD framework and its elements, introduced in the previous chapters. The selected use-case should be robust and accurate to surface out the practical problems and inefficiencies related to the framework. Passing the test in this strong use-case ensures that the framework is robust and the problems associated with weak frameworks are avoided.

"Intellectual Property Rights (IPR)" domain has been selected as the test use-case because it provides both the legal understanding and legislative efforts at international level, in as collaborative, effective and uniform manner as possible, to protect the rights of intellectual property owners and to avoid future conflicts.

The chapter first defines and characterizes the domain of IPR, which categorized into copyrights, related rights, trademark, patents, and industrial rights. The information is based on the official treaties and documents from World Intellectual Property Organization.

Based on this classification, different individual and group of individuals are identified who play an active role in shaping this domain. The chapter then discusses the context of cyber engagement, which is protection of interests, expansion of interests, and the power projection. Finally, the instruments and intensity of engagement are interpreted in the context of prior definition of engagement in IPR domain in reference to cyberspace. The structure of the chapter is shown in Figure 4-1.

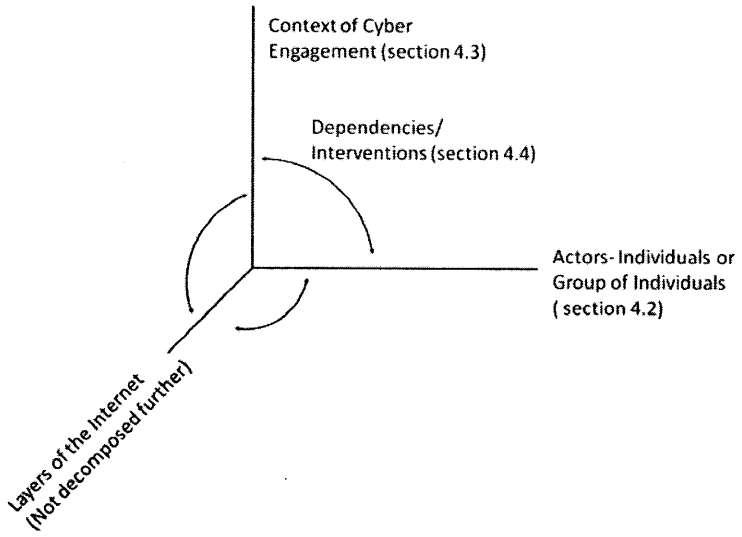


Figure 4-1: Dimensions of the CSSD framework expanded in context of IPR use-case.

4.1. Intellectual Property Rights Domain

Like any property, intellectual property provides the lawful rights to the legitimate owner of a property to use it for free and excludes others from using it. The term "intellectual property" is reserved to types of property that are creations of human mind. The states that drafted the convention establishing World Intellectual Property Organization" chose to offer an inclusive list of the rights as relating to,

"Literary artistic and scientific works; performances of performing artists, phonograms, and broadcasts; inventions in all fields of human endeavor; scientific discoveries; industrial designs; trademarks, service marks, and commercial names and designations; protection against unfair competition; and "all other rights resulting from intellectual activity in the industrial, scientific, literary or artistic fields" (WIPO 2003, Article 2, § viii).

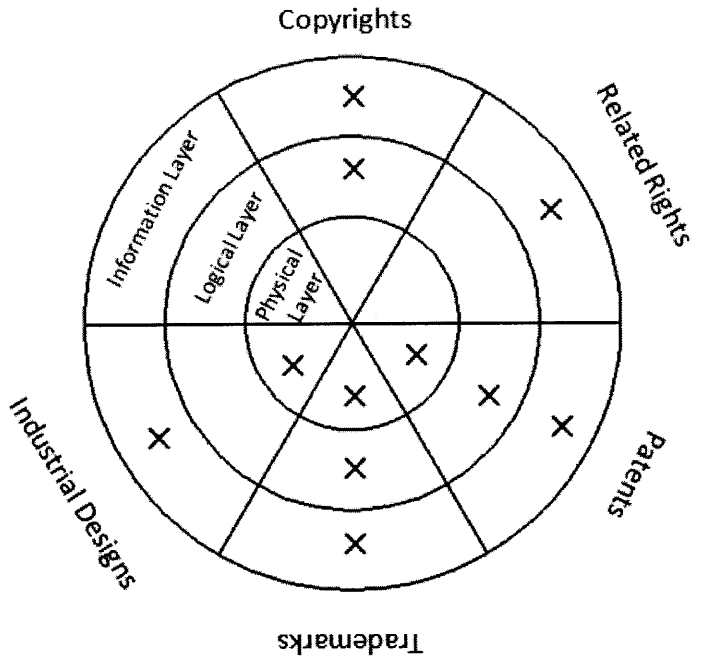


Figure 4-2: Categories of intellectual property rights and their mapping to the Internet layers.

The following five main categories (Figure 4-2) mostly cover all the tangible and intangible knowledge, which span over the three identified layers of the Internet environment. These are (WIPO 2001, see chapter 2 & 3; 1994; WIPO Academy 2007):

a) **Copyright** laws provide relevant protection to the creators/authors of scientific, literary, and artistic works (e.g. like books, song lyrics, and paintings).

b) **Related Rights** laws provide relevant protection to works derived from copyrighted works, broadcasts, performances, and recording and reproduction of performances (e.g. concerts, translation of books).

c) **Trademarks**, service marks, collective marks, commercial names, and geographical indicators are used for identifying a good or service from others (e.g. logos or names for a product).

d) **Patent** laws provide to relevant protection to inventions of a new product or process (e.g. new form of automobile engine, or a new way ordering goods on Internet).

e) Protection for **industrial designs** (e.g. new way of packing goods) is available through either patents or copyright laws or through its own specialized laws.

The term "law" in the IPR includes international treaties, conventions, and national laws non-binding recommendations or guidelines. The following subsections give the details of the type of works protected under each category mentioned above.

4.1.1. Copyright

As mentioned earlier, an author is afforded copyright protection in relation to the work, he has authored. This work should constitute within the meaning of the concept of "literary and artistic works" of Article 2 of the Berne Convention. The works mentioned in the Article 2 of the Berne Convention (WIPO 1995) have been divided into the following categories (WIPO Academy 2007, 11) :

a) Books, pamphlets and other writings;

b) Lectures, addresses, sermons and other works of the same nature;

c) Dramatic and dramatico-musical works, choreographic works, and entertainments in dumb show;

d) Musical compositions with or without words;

e) Cinematographic works to which are assimilated works expressed by a process analogous to cinematography;

f) Works of drawing, painting, architecture, sculpture, engraving, and lithography;

g) Photographic works to which are assimilated works expressed by a process analogous to photography;

h) Works of applied art;

i) Illustrations, maps, plans, sketches and three-dimensional works relative to geography, architecture, or science;

j) Translations, arrangements of music, adaptations and other alterations of literary and artistic works;

k) Collections of literary and artistic works;

l) Special types of works including :

   i. Computer programs,

   ii. Databases, and

   iii. New technology products and online distribution of works.

4.1.2. Related Rights

Rome Convention (WIPO 2002) extends the list of works protected by Berne Convention and includes works that are derived from other, existing sources. These works are generally referred as "derivative works" and include (WIPO Academy 2007):

a) Translations of works into a different language;

b) Adaptations of works, such as making a film scenario based on a novel;

c) Arrangements of music, such as an orchestra version of a musical composition initially written for piano;

d) Other alterations of works, for example an abridgement of a novel;

e) Compilations of literary and artistic works, such as encyclopedias and anthologies. In such a case, the originality resides in the choice and arrangement of the materials.

4.1.3. Trademark

A trademark is a distinctive sign that is capable of distinguishing certain goods and services with which it is associated. These marks are a crucial component of business assets and help the trademark owner to:

a) Help consumers identify and distinguish products or services;

b) Enable companies to differentiate between their products;

c) Use as a marketing tool and the basis for building a brand image and reputation.

Further, it may be licensed and provide a direct source of revenue through royalties or can be useful for obtaining finance. In addition to trademarks, the following categories of marks also exist (WIPO 2001,67-70; WIPO Academy 2007).

a) **Collective marks** are used for distinguishing goods or services produced or provided by members of an association. (e.g. AIAA, Wool Mark, etc. (Figure 4-3)).

Figure 4-3 : Examples of collective marks.

b) **Certification marks** are marks used for distinguishing goods or services that comply with a set of standards and have been certified as such (e.g. The UL symbol to show that products comply with performance specifications set down by the Underwriter Laboratory (Figure 4-4)).

Figure 4-4 : Examples of certification marks.

c) **Geographical Indicator** is a used for stating that a given product originates in a given geographical area and possesses qualities or reputation due to that place of origin (e.g. Darjeeling tea (Figure 4-5)).

Figure 4-5: An example of a geographic indicator.

d) **Domain names** are used for accessing websites (equivalent to addresses in the real world) on the Internet (e.g., mit.edu). These names map to unique Internet protocol (IP) numbers that serve as routing addresses on the Internet, thus, providing a connection between the real and the virtual world

Domains names generally include trademarks within them (e.g., mit.edu where MIT is the registered trademark of Massachusetts Institute of Technology) and allow consumers to distinguish and identify products or services in the online environment.

4.1.4. Patent and Industrial Design

Patents are one of the oldest forms of intellectual property protection. A patent grants exclusive rights to protect an invention, which may be a product or an innovative process of doing something. An invention must meet the following conditions to be eligible for a patent protection (WIPO 1998, 2009; WIPO Academy 2007):

a) It must be new or novel, that is, it must show some new characteristic which is not known in the body of existing knowledge (called "prior art") in its technical field;

b) It must be non-obvious or involve an inventive step, that is, it could not be deduced by a person with average knowledge in the technical field;

c) It must be useful or capable of industrial application;

d) Finally, the invention must be part of the so-called "patentable subject matter" under the applicable law.

By providing limited exclusive rights, patent plays an important role in justifying the investment and expenditures made in research and development of new products and processes. Patents[15] are also granted for business processes, which are related to electronic commerce, data processing, electronic sales, advertising models, and other such business practices (e.g. class 705 of USPTO).

An **industrial design**, on the other hand, is the aesthetic, ergonomic and usability aspect of an article for improving a products manufacturability and marketability. A few design features include shapes, patterns, and colors.

---

[15] In many countries, certain subject matters are not considered patentable. A few of such subjects include scientific theories, mathematical methods, plant or animal varieties, discoveries of natural substances, commercial methods, or methods for medical treatment (WIPO 2001; 1998, Chapter 2) .

4.2. Actors - Individuals and Group of Individuals

This section catalogues the different types of actors, both individuals and group of individuals, who are involved in the creation, management and regulation, control, and use of cyberspace. Their actions in the intellectual property rights domain affect all the other actors in both real and virtual space. It should be kept in mind that most of the actors, real as well as online, are multi-faceted and cannot be classified into one class based on one attribute.

4.2.1. Individuals

This thesis will classify the individuals based on two categories. The first one is based on the nationality of an individual and place where an individual first presented his work. Various international intellectual treaties provide protection to (WIPO 1995):

a) Authors/Inventors/ Creators who are **citizens** of one of the countries that has ratified an international treaty and, there is member of the Union, and

b) Authors/Inventors/ Creators who are **not** citizens of one of the Union countries, but their work is published in one of those countries that are member of the Union.

The second classification is based on the ownership of rights. There are two aspects to intellectual property (specifically related to copyright laws). An owner is granted the **economic rights** to protect the financial interests in his/her work. A form of monopoly is granted to the owner (who can also be the creator of IP) in relation to the exploitation of his/her work. It means that the author/creator is the only one to exercise them and can prevent third parties from doing so unless they have his/her authorization.

The **owner of the moral rights** is the creator of the intellectual property and these rights cannot be transferred to others. These rights are of a personal character whose aim is to protect

the personal interests of the author/creator in the work (WIPO 1995; WIPO Academy 2007, 2007, 2007).

4.2.2. Internet Creators, Operators, and Maintainers

This community includes the businesses that create and support the cyberspace and the Internet, which include (Clark 2010)[16]:

a) Internet intermediaries and service providers (e.g. British Telecom, Vodafone, Comcast, Verizon, ATT, etc.);

b) Computing service providers (e.g. Amazon Web Services, etc.);

c) Higher-level service providers (e.g. content delivery services or social networking sites such as facebook.com);

d) Equipment manufacturers and suppliers (e.g. Huawei, etc.);

e) Supply chain behind them (electronic chips, software, etc.).

4.2.3. Internet Standard Bodies

At the technical level, Internet is made possible by the design, development, test and evaluation, and implementation of Internet standards developed by a diverse group of standards bodies. Each standards body (or category of) has a specific charter to shape cyberspace by the setting of standards, thus giving them a different standing in this space. These standard bodies, essentially a self-decreed standards bodies, have coordinated the establishment of the influential worldwide standards (e.g. use of the radio spectrum) for promoting interconnections between a wide variety of communication systems. A few such organizations are listed below:

---

[16] Based on author's discussions with Dr. David Clark at MIT Department of Political Science, February 2010.

The formal representative to the **International Telecommunications Union** (ITU), a United Nations entity, comes from a state's government. Traditionally, the role of the ITU was to set telephony standards, and since in most countries the telephone service was provided by state-run organization, the participation of the state made sense. However, role of the ITU in the shaping of the Internet is both complex and complicated.

The **International Organization for Standardization** (ISO), world's largest standards developer and publisher of International Standards, is a non-governmental organization. The purpose of ISO is to bridge the gap between the public and private sectors by building consensus on solutions that meet both the business requirements and the broader needs of society.

The **International Electro-technical Commission** (IEC) is another non-profit, non-governmental international standards organization that prepares and publishes International Standards related to electrical, electronic, and related technologies.

The **Internet Society** (ISOC) acts as a host management organization for coordinating and chartering the work of other standards bodies that support running of the Internet. It oversees the work of key technical standard bodies like Internet Engineering task Force (IETF), the Internet Advisory Board (IAB), the Internet Engineering Steering Group (IESG) and the Internet Research Task Force (IRTF). Most of the participation in these organizations comes from Internet equipment suppliers, Internet operators, and academics, with a very less government presence.

Below are some of the other agencies, which are involved in the development of the Internet protocols:

a) The Defense Advanced Research Projects Agency of the United States (DARPA).

b) The Internet Corporation for Assigned Names and Numbers (ICANN), which was formed in 1998 to privatize and internationalize the management of domain names.

c) Internet Assigned Numbers Authority (IANA) was primarily responsible for assigning IP addresses and maintaining the technical parameters of the DNS.

d) Regional Internet Registries, which are allocated blocks of unassigned IP addresses from IANA, assist in the coordination of the domain name system. The following registries have jurisdiction to assign names in the ccTLDs[17] only:

   i. American Registry for Internet (ARIN),

   ii. Reseaux IP Européens (RIPE), and

   iii. Asia Pacific Network Information Center (APNIC).

e) National Science Foundation (NSF), which, in 1991, assumed responsibility for coordinating and funding the non-military portion of the Internet infrastructure. It solicited bids to provide a variety of services associated with the infrastructure including DNS registration.

f) Network Solutions, Inc. (NSI) received the NSF contract for DNS registration. It managed registration, coordination, and maintenance functions of the DNS until competition was introduced. Its contract expired in early November 1998. It now acts as a registrar, and registers domain names in the gTLDs on a first-come, first-served basis. NSI is a subsidiary of VeriSign, Inc., the registry for inters alia, .com, and .net domains.

---

[17] A country code top-level domain (ccTLD) is a two-letter Internet top-level domain. It is generally used or reserved for a sovereign state (Postel 1996).

4.2.4. Internet Regulators

Professor Lessig's thesis (1998) on the "Modalities of Regulation" suggests the application of four modalities: law, market, norms and architecture (Figure 4-6) for the regulation of the cyberspace. Each modality has the following unique properties:

a) **Law** constrains the actions of an individual (or group of individual) by defining a command/rule that, if broken, threatens punishment. It is imposed by a state.

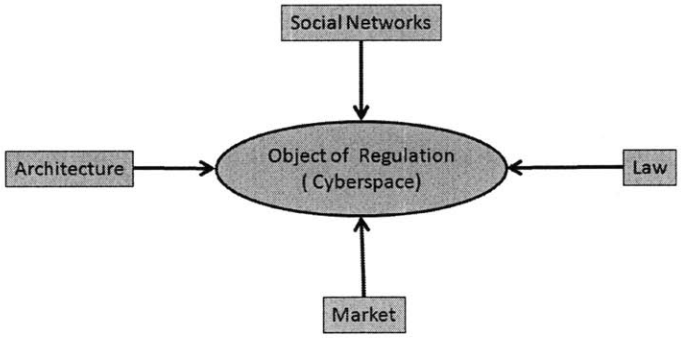


Figure 4-6 : A framework for cyberspace regulation (Lessig 1998).

b) **Markets** are characterized by activities that lead to an exchange of value between two parties. It is regulates through price mechanism (or direct monetary exchange). Internet creators, operators, and maintainers impose this type of control.

c) A **social norm** regulates the behavior of an individual through a dishonor or social exclusion that a community (not a state) imposes. Deviation from a norm makes an individual (or group of individual) socially abnormal, which can have negative effects, such as alienation from a community. Internet content developers impose this type of control.

d) **Architecture** (or "code") of the Internet regulates the user behavior through the restrictions it can impose. Such restrictions can be implemented automatically in

real-time environment. Such identification and authentication tools include services provided by authentication certificate/service providers, who support in implementing this type of control.

Below are some of the players that play an important role in the regulation of the Internet in each category of the modality:

a) Law-based Regulators

State laws can affect the use of the Internet in ways that may hinder or encourage its use for good purposes. For example, state laws like the America's First Amendment, on one hand, can empower individuals (and group of individuals) to harness the power of the Internet for meeting their demands for a positive action. Other the hand, state intervention can also be used to suppress the activities (e.g. free speech) of its Internet users both in the cyberspace and in the real world. For example, China has criminalized all forms of nonconformist online speech to its policies and ideologies, thus hurting the civil liberties (Chalaby 2000).

b) Market-based Regulators

Internet access price can act as a market regulator. Since the Internet provides a universal and level platform to share information, an increased access to Internet may lead to a greater and broader population of its users. A lower cost barrier to access Internet allows transfer of information from anybody to anybody (though some actors like owners of knowledge may not find it desirable). It also increases an individual's potential to educate, enhances his personal independence, and fosters communal discussions.

However, it can also be used as a control mechanism to (a) limit an individual's access to Internet and (b) keep him/her away from the Internet, thus, regulating his/her activities on the

Internet, like preventing him/her from engaging in a communal dialogue, that they might otherwise do if they could afford access (Chalaby 2000).

c) Social Regulators

The different social norms or the acceptable behaviors, i.e. constraints set by communities on capabilities and activities, affect the regulation of the Internet. On one hand, these activities may promote the self-actualization for an individual's (or group of individuals) participation on the Internet through personalization of services. On the other hand, it may lead to the social exclusion or alienation of an individual because of lack of individual skills, capabilities to access Internet and role played by Internet (and language used) for and against segregation. For example, if the web content is not written in the lingua franca of a community, it will hinder their participation in the cyberspace.

d) Architecture (or code) Regulators

The architecture based regulatory techniques include:

Encryption technologies (e.g. SSL and PGP) work by transforming information using an algorithm to make it unreadable to anyone except those possessing special knowledge. It also ensures the authenticity and integrity of a message.

Filtration technologies prevent an individual to access information that is available otherwise. Such controls are used by state actors to block access to politically sensitive web sites to its citizens (Kalathil and Boas 2006).

4.2.5. Governments

Being the traditional actors on the stage of international relations, **Governments** are clearly important in this analysis (Clark 2010). They can have multiple objectives and have many tools at their disposal. Such tools are generally traditional and may not exploit the features of cyberspace. These tools include policymaking and legislation, investments in infrastructure development and in research, etc. However, Government can act directly in cyberspace, and can induce direct actions by other actors. Such actions include use of power instruments and their power, which range from coercive to cooperative actions. For the protection of intellectual property rights, the organizational structure of a government machinery can be divided into three categories (see WIPO 2001, Chapter 4 & 6):

a) Agencies and bodies operated directly by the government machinery i.e.
    i. Patent Office and a Policy Unit, e.g. United States Patent and Trademark Office (USPTO),
    ii. Trademark Office, and
    iii. Industrial Design's Office.

b) Agencies and bodies, which are outside the government machinery but may have its supervisory control like:
    i. The patent attorneys or agents,
    ii. National Association of Patent Agents, and
    iii. International Association of Patent Agents, e.g.
        - *Fédération Iinternationale des Conseils en PropriétéIndustrielle (FICPI)* based in Switzerland.
        - *Association Internationalepour la Protection de la PropriétéIndustrielle (AIPPI)* based in Switzerland.

c) Special arrangements in courts of law.

4.2.6. Intergovernmental Cooperative Agencies

Intergovernmental cooperative agencies are based on international treaties and conventions. They are meant for facilitating cooperation in the administration of intellectual property rights between the member nations. The representation in these agencies is from the state governments. Some of the organizations include:

a) African Regional Industrial Property Organization (ARIPO);

b) African Intellectual Property Organization (OAPI);

c) Eurasian Patent Organization;

d) European Patent Organization;

e) Cooperation among the state members of the European Union through:

   i. The Office of Harmonization in the internal Market, and

   ii. The Benelux Trademark Office and the Benelux Designs Office;

f) Sub regional Integration of the Andean Community;

g) Common market of the South (MERCOSUR);

h) Group of three (Columbia , Mexico and Venezuela);

i) North American Free Trade Agreement;

j) The ASEAN Framework Agreement on IP Cooperation;

k) Hanoi Plan of Action.

These agencies are based on the following WIPO administered major systems of intellectual property registration:

a) Patent Cooperation Treaty (PCT);

b) Madrid Agreement concerning the International Registration of Marks;

c) the Protocol Relating to Madrid Agreement concerning the international Registration of Marks;

d) Hague Agreement Concerning the International Deposit of Industrial Designs.

A number of other international organizations deal with issues relating to electronic commerce in their particular areas of expertise. The following is a partial list of such organizations.

a) Hague Conference on Private International Law (http://www.hcch.net/);

b) International Telecommunication Union (ITU) (http://www.itu.int/);

c) Organization for Economic Co-operation and Development (OECD) (http://www.oecd.org/topic/0,2686,en_2649_37441_1_1_1_1_37441,00.html);

d) United Nations Conference on Trade and Development (UNCTAD) (http://r0.unctad.org/ecommerce/);

e) United Nations Commission on International Trade Law (UNCITRAL) (http://www.uncitral.org/);

f) World Trade Organization (WTO) (http://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm);

g) World Intellectual Property Organization (WIPO) (http://wipo.int).

4.2.7. Internet Beneficiaries

Internet has been a very important driver of change and along with other technologies, like a cellular phone, it has changed an organization's approach to doing business and, hence, the competition. It has facilitated commerce in both tangible and intangible products. For commerce, involving tangible products (e.g. books etc.), Internet acts as an online platform for facilitating sales and payment transactions. The actual delivery of goods is done physically. For commerce

involving intangible products (e.g. e-books etc.), it acts as both facilitation and delivery platform for goods and services. There are two defining characteristics of this type of commerce facilitated by Internet (WIPO Academy 2007):

a) First, the Internet provides even a small business an access to worldwide market, and
b) It blurs the traditional line between the business sectors that are based on the physical manifestations of goods and service provided.

This established group of **Internet beneficiaries,** which is highly affected through the use of Internet services can be categorized as

a) For-profit commercial establishments (Clark 2010)
    i. Telephone companies and their suppliers,
    ii. Financial institutions and real businesses,
    iii. Entertainment and advertising industry,
    iv. Publishing industry and print media, and
    v. "Brick and mortar" merchants of various sorts.
b) Not-for-profit commercial establishments
    i. Charitable organizations (e.g. Bill and Melinda Gates Foundation. etc),
    ii. Humanitarian agencies (e.g. Red Cross, Amnesty International, Oxfam, etc), and
    iii. Public art organizations (e.g. museums, etc),

4.2.8. Online Communities

The real communities, discussed earlier, not only have a physical presence, but often have rigid community standards or norms and they enforce them to preserve the values and legitimacy (Murray 2007, 129-132). It is difficult to think of purely online equivalents of real

communities like real businesses (e.g. General Electric Company, ABB, Wal-Mart), and professional organizations (e.g. IEEE and AIAA), and regulatory agencies (e.g. ITU and ICANN). The online presence of such communities is an extension of their physical presence. Leaving the online equivalent is easy and quick but for leaving the real community, a switching cost may be exerted on its members.

Table 4-1: Classification of online communities (Murray 2007, 42).

Class	*Primary Purpose*	*Example*
Commercial Communities	Market functions, trade, payment, transactions, trust	Amazom.com; ebay.com
Online/offline Communities	Online discussions of offline topics	Twitter.com
Gaming Communities	Gaming progress, rewards and respect of other gamers	Xbox live; Gambling sites
Café Communities	Discussion and chat	Facebook.com; myspace.com
Knowledge Communities	Help and advice, distribution of information and knowledge	Tripadvisor.com ; Apple Developer Forums
Creative Communities	Creation of cooperative products and services.	Wikipedia.com

Online communities focus on a particular aspect of an individual's life, usually social life. Such communities have lower barriers to entry and exit. Further, the switching cost of this mobility is much lower than the real communities (Murray 2007, 145). The taxonomy of the online communities can be classified into six broad categories based on their purpose as shown in Table 4-1. Further, it should be kept in mind that most of the communities are multi-faceted and complex and cannot be classified into one class based on one attribute.

4.2.9. Illegitimates

This category includes individuals, group of individuals and communities deliberately structured or have intentions to participate in unfair competitions and acts, which are considered contrary to honest practices in an industrial, social or commercial context. It is difficult to precisely define and encompass all such existing dishonest acts as the standards and norms for fairness of activities not only differ from society to society but also evolve over time. Based on the Paris Convention for the Protection of Industrial Property (Article 10 and 10^{bis}) (WIPO 1998), illegitimates can be defined as one:

a) who may act *"to create confusion by any means with the establishment, the goods or the industrial or commercial activities of a competitor"* (e.g. using a trademark identical or similar to another with respect to goods of the same category);

b) who may act to constitute *"false allegations in the course of trade of such a nature as to discredit the establishment, the goods, or the industrial or commercial activities, of a competitor"* (e.g. an enterprise attacking a competitor through statements that are false and untrue with relation to the latter's goods or services);

c) who may use "*indications or allegations which may mislead the public as to the nature, the manufacturing process, the characteristics, the suitability for their purpose, or the quantity of the goods"* (e.g. a company publishing false and untrue statements concerning the quality or safety of its own products in connection with promotion or sales advertising).

The concept of illegitimates and of unfair competition also applies to the following:

a) individuals (or group of individuals) who are involved in the act of disclosing or using the secret or confidential information without proper consent of the rightful holder of the information, in a manner contrary to honest commercial practices (e.g.

acts tending to appropriate another's secret information, such as a method of manufacturing a product, through industrial or commercial espionage);

b) individuals (or group of individuals) whose acts or practices that, in the course of industrial or commercial activities, damage the goodwill or reputation of another's enterprise, regardless of the fact whether such acts cause confusion or not (e.g. deliberate and bad faith registration of well known brand names as domain names on Internet).

4.3. Context of Cyber Engagement

Operations in cyberspace acts as an enabler in domains outside cyberspace like critical infrastructure, financial institutions and net-centric warfare in the existing under-water, water, land, air and space domains, while providing a new space where it can deliver effects. The *context of context engagement* (Figure 4-7) is broadly divided into three categories to produce a preferred level of cyber operations, i.e. (a) Protection of interests, (b) Expansion of interests, and (c) Power projections.

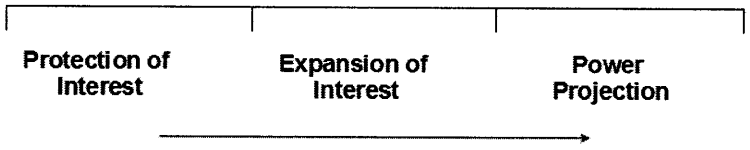


Figure 4-7 : Context of cyber engagement in IPR.

The following sections will attempt to list the activities, related to intellectual property rights domain, in each of the above-mentioned categories:

4.3.1. Protection of Interest

For all intellectual property systems to be functional, they should be supported by a strong judicial system for enabling the award of rights, enforcing rights, and dealing with both civil and criminal offenses. Every effort should be made to make the judicial system accessible and sufficient for fair and expedited dispute resolution procedures. Further, the system should be able to enforce the decisions made by the judicial system to limit and recover the losses caused by the infringement and prevent any future infringement.

In addition to it, an actor should also take proactive actions to protect and manage intellectual property (IP) assets relevant to intellectual property rights. A few of actions related to electronic commerce include (WIPO Academy 2007):

a) Assess IP assets relevant to e-commerce by listing any potential resources and related contracts.

b) Avoid damage to IP rights that may through other's act of infringement, as well as infringing other's IP rights.

c) Uses of great care when disclosing information relating to one's own company as well as that of third parties in an online environment.

d) Preparation for potential private international law issues that arise from international commercial activity by asking consumers to agree to legal clauses, such as arbitration clauses, in advance.

e) Inclusion of IP rights notices and disclaimers on goods and services to protect one's IP rights as well as to avoid getting involved in infringement of any third party's IP rights.

Further, while developing the web services, the following acts may protect one against potential infringement situations by knowing what one owns and what one does not:

a) Perform a trademark check to ensure that the choice of domain names does not abuse existing trademarks in your one's country as well as other countries.

b) Perform a patent check to ensure that processes or technology being used in web-services development does not abuse existing patents.

c) Perform a copyright check to ensure that the content on the website does not abuse anyone else's copyright.

d) If consultant or company is being used to design the web services, provisions in the agreement with them concerning ownership and intellectual property rights should be properly reviewed.

e) Keep abreast of competitor's activities in the markets, where products or services are being offered and if become aware of an apparent infringement seek legal advice from a qualified intellectual property attorney.

4.3.2. Expansion of Interest

For an actor to have a global reach in the cyberspace, it needs access technologies and mechanisms for deploying and positioning friendly cyber assets across the friendly, global commons and adversary networks. As different public entities begin regulating the Internet and formulate electronic commerce policy, following are few measures for increasing an actor's lateral pressure:

a) Technology neutrality (i.e., developing policy, independent of technology being used) is one of the ways to exert lateral pressure for global reach. Formulating technologically neutral policy ensures that excessive policy work is not performed as the latest technological innovations reach the marketplace. For example, if

intellectual property policy is developed for the Internet, it should also be applicable to the wireless Internet.[18]

b) Coordinate with national and international organizations in the formulation of appropriate positions on the issues affecting IP (e.g. validity of electronic contracts and concerns related to physical jurisdiction.) (WIPO Academy 2007).

4.3.3. Power Projection

"The challenges facing the world today will require a much broader conception and application of national power than just military prowess" (Gates 2008). Individuals, governments, businesses, and other institutions often engage in intellectual disciplines to develop tools for a better understanding the needs and gaps in current capabilities for ensuring responsiveness to a dynamic, complex, and evolving environment. To have such a prescriptive and adaptive power, an actor should have tools and technology to (Tenorio 2010):

a) **Predict** expected behavior of cyberspace (social, technological and legal) under a variety of scenarios involving complexity of the system, environment, and human independence.

b) **Emulate** cyberspace behavior factors, (i.e., knowledge /intelligence, sensing and external interaction) at both system and subsystem levels over a continuum of Live-Virtual- Constructive environment.

c) **Prescribe** guidance and considerations for suitable, effective, and survivable Internet and recommendations for an evolving cyberspace.

In order to predict-emulate-prescribe the future actions in cyberspace, tools and technologies employed should be able to (Tenorio 2010):

---

[18] Based on discussions at European Commission "Future of Internet" meeting at MIT. March 18th, 2010.

a) Develop algorithms and models for predicting behavior of the system;

b) Develop test protocols and algorithms to support evaluation of cyberspace management and Internet shutdown;

c) Develop realistic test-bed components, and environments to support the Internet evaluation approaches to unfolding situations;

d) Develop methodologies and metrics to evaluate distributive control and situational awareness and compile ground-truth data to support.

Further, these resources and tools should have (Tenorio 2010):

a) Extent: Expanse of test scenarios associated with an ever expanding portfolio of cyberspace operations;

b) Variety: The types and categories of test related to a challenging set of missions in complex environments;

c) Ambiguity: Testing emerging technology against the backdrop of traditional, irregular, disruptive, catastrophic environment and testing for suitability, effectiveness, and survivability.

4.4. Instruments and Intensity of Engagement

The intellectual property right system is in constant search for solutions to the new challenges, exceptions, and limitations of the traditional IP rules as they arise due to the digitization of the information. These challenges include online licensing models, digital rights management, and role of the Internet service providers.

This section presents the procedures adopted, maintained and (or) applied at different levels of engagement – coercive to cooperative to affect other's behavior (Figure 4-8). Instruments of engagement at different intensities are listed below:

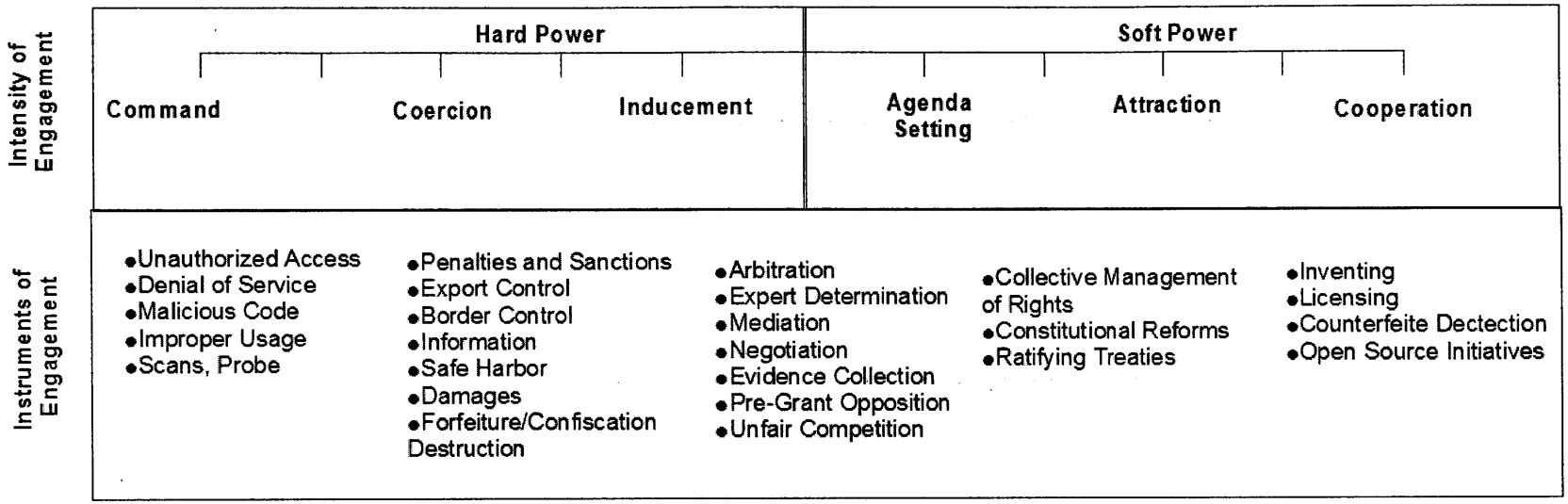


Figure 4-8: Instruments and Intensity of engagement in IPR, adapted from Nye (2004, 8).

a) **Unauthorized access**[19] is an attempt to gain logical or physical access without permission to a network, system, application, data, or other resource.

b) **Unauthorized access**[19] is an attempt to gain logical or physical access without permission to a network, system, application, data, or other resource.

c) **Unauthorized access**[19] is an attempt to gain logical or physical access without permission to a network, system, application, data, or other resource.

d) **Denial of Service** (DoS)[19] is an attack to prevent or impair the normal authorized functionality of networks, systems, or applications by exhausting the resources.

e) **Malicious Code**[19] is an attempt to install a code-based malicious entity (e.g., virus, worm, and Trojan horse etc.) that infects an operating system or application.

f) **Improper Usage**[19] is a violation of acceptable computing use policies by an individual.

g) **Scans, Probes, or Attempted Access**[19] includes any activity that seeks to gain access or to identify open ports, protocols, service, or any combination for later exploitation.

h) **Penalties and Sanctions:** Provision for penalties that include imprisonment, monetary fines, or both that are sufficiently high to deter to future acts of infringement or violation.

i) **Export Control**: Provision for any permanent or temporary restriction on import and export of articles and services primarily governed by state's export control act (e.g. 22 U.S.C. of the Arms Export Control Act in United States (US-ITAR 2010)).

---

[19] (US-CERT)

j) **Border Control:** Provision for any permanent or temporary action to avoid the release of suspected and imported, infringing goods into domestic markets by the designated authorities.

k) **Safe Harbor:** Provision for third parties (e.g. Internet intermediaries) to protect themselves against any risk involved, once they exercise judicial judgment to remove their client's content or disclose their identity to the designated authorities.

l) **Injunction:** Provision for "issuing interlocutory injunction to prevent any imminent infringement of the intellectual property right from occurring" (WIPO 2001).

m) **Seizure:** Provision for authorizing the seizure of suspected counterfeit trademark goods or pirated copyright [or related rights] goods, any related materials and implements used in the commission of the alleged offence.

n) **Damages**: Provision for judicial authorities to order infringer, to pay a monetary compensation including account for profit (i.e. amount earned by the way of unjust enrichment through the infringement) to the right holder.

o) **Forfeiture/Confiscation and Destruction:** Provision for confiscation/forfeiture and (or) destruction of all counterfeit or pirated goods, of materials and implements used in the creation of such goods.

p) **Arbitration**: Provision for submitting a dispute to one or more mutually agreed arbitrator(s) who makes a binding decision on the dispute. In choosing arbitration, the parties opt for a private dispute resolution procedure instead of going to court.

q) **Expert determination**: Provision for submitting a dispute to one or more mutually agreed subject matter expert(s) who makes a determination on the matter referred to them. The determination is binding, unless the parties agreed otherwise.

r) **Mediation:** Provision for a neutral intermediary to help the parties to reach a mutually satisfactory settlement of their dispute. *Mediation is a non-binding procedure controlled by the parties*; however, any settlement is recorded in an enforceable contract.

s) **Negotiation:** An act of persuading an infringer to change his actions to avoid further infringement.

t) **Evidence Collection:** Collecting information or articles that may be used in the court to enable it in determining the truth or issues of the fact.

u) **Unfair Competition :**An act of competition that is contrary to honest practices in industrial or commercial matters by creating confusion, constituting false allegations which may mislead the public as to the nature, the manufacturing process, the characteristics, the suitability for their purpose, or the quantity of the goods.

v) **Collective Management of Rights:** Collective management of a given repertory of works, i.e. collecting royalties, effective licensing and monitoring use of each work, through a single window organization for its members (WIPO Academy 2007).

w) **Pre-grant Opposition**: Provision for formal opposition to the designated authorities before the grant of intellectual property rights to an individual or group of individual.

x) **Constitutional Reform:** Adoption and consideration of series of policies, which may require, for their implementation, amendment of national laws and international treaties.

y) **Ratifying Treaties:** A formal process of approving and sanctioning an international treaty and its provisions within one's boundaries. Treaties in IPR are broadly categorized into following three groups , (WIPO 2001) :

i. The first group of international treaties, related to IPR, is for establishing international protection among the member nations. e.g. the *Paris Convention(WIPO 1998)* , *the Madrid Agreement for the Repression* of False or Deceptive Indications of Source on Goods (WIPO 1996, 2008), and the *Lisbon Agreement* (WIPO 2002) for the Protection of Appellations of Origin and their International Registration.

ii. Treaties in the second group facilitate international protection of intellectual property rights. e.g. the *Patent Cooperation Treaty(WIPO 2009)*, the *Madrid Agreement* Concerning the International Registration of Marks (WIPO 1996, 2008), *the Lisbon Agreement (WIPO 2002)* ,the *Budapest Treaty* on the International Recognition of the Deposit of Microorganisms for the Purposes of Patent Procedure (WIPO 1997)and the *Hague Agreement* Concerning the International Deposit of Industrial Designs (WIPO 2008).

iii. The third group of treaties facilitate in establishing classification systems and procedures for improving and keeping them up to date. e.g. *International Patent Classification* Agreement(WIPO 2006), the *Nice Agreement* Concerning the International Classification of Goods and Services for the Purposes of the Registration of Marks (WIPO 1997),the *Vienna Agreement* Establishing an International Classification of the Figurative Elements of Marks (WIPO 2008) and the *Locarno Agreement* Establishing an International Classification for Industrial Designs (WIPO 1997).

z) **Public Outreach:** All concentrated efforts to reach out to the public and businesses to promote a general understanding of intellectual property rights.

aa) **Overcoming the problem** in a legitimate way by

i. **Inventing** around the already protected intellectual property,

ii. **Licensing or negotiating a contract** in a friendly way to use the intellectual property, and

iii. Assessing the scope and validity of the intellectual property.

iv. **Development and implementation of schemes** that allow for easy identification of original work or products that counterfeiter tries to copy or infringe (e.g. use of holograms, watermarks, meta-data, etc.).

bb) **Open Source Initiative:** Distribution of intellectual property, free of licensing restrictions and encouraging users to use, to copy, to modify and to distribute it freely as long as certain conditions are met, such as creative commons and public documents.

4.5. Summary

This chapter focused on the intersections of tasks 2 to 4 of the research methodology, presented in chapter 1. A test use-case based on the "Intellectual Property Rights (IPR)" domain was developed. The CSSD framework was then adapted to test its applicability to the use-case.

The IPR based test use-case proved to be a robust, comprehensive, and coherent use-case covering all the modalities of **socio-economic-technological-political system.** It provided both the legal understanding and legislative efforts at international level, in as collaborative, effective and uniform manner as possible, to protect the rights of intellectual property owners and to avoid future conflicts. It helped in the continuous evaluation and upgradation of the CSSD framework in the context of cyber-international relations.

5. CONCLUSION

This chapter discusses the contributions and the limitations of *Cyber System for Strategic Decisions* (CSSD) framework, and presents recommendations for future work.

5.1. Addressing the Research Question

The following research question was posed in Chapter : What cyberspace **"is made of"** and **"who gets what, when, and how ?"** (Lasswell 1950). Two challenges related to explorations of cyber-international relations were discussed:

1) Lack of holistic approach to explore the intersection of social, economic, technical and legal disciplines related to cyberspace and international relations[20], and
2) Need to ensure that the number of actors and stakeholders who participate in the articulation of propositions, and propositions themselves are accurately represented[21].

Challenge (1) is addressed by articulating the rules of mapping the knowledge in the emerging field of cyber-international relations to ensure a consistency in the representation of the content. The Cyber System for Strategic Decisions (CSSD) framework, developed to map the international relations in cyberspace, thus, acts as the foundation for developing a coherent understanding of the knowledge content bearing on the specific aspects of cyberspace of interest in any situation. It provides the fundamentals for thinking about, searching for, retrieving and analyzing to enhance both content and the value of the knowledge.

---

[20] Refer p 18.

[21] Refer p 23.

The research initiative has also developed the foundations for an internally consistent and articulate representation of cyber-international relations space in terms of a*ctors- individuals and group of individuals*, *layers of the Internet* and the *extent of engagement* that form the basis of the CSSD framework. This approach can be applied to diverse domains to build scenarios and model different facets of both the real world and cyberspace according to the practical needs. *The instruments and intensity of engagement* and *the extent of time of engagement* are the two dependencies that map the interactions among the different entities.

Challenge (2) is addressed by developing connectivity logic and weaving it into the framework. The complete framework system is integrated through connectivity logic, which defines how the different pieces of the framework are linked. This logic serves as a mechanism to (a) developing a content-based indexing system and (b) linking the constituent elements of a system in a nested hierarchical manner.

Finally, to test the logic of the framework, a robust, comprehensive, and coherent test use-case was developed. The use-case was based on "Intellectual Property Rights (IPR)" domain. IPR proved to be a strong test use-case because it is a well established and provides both the legal understanding and legislative efforts at international level, in as collaborative, effective and uniform manner as possible, to protect the rights of intellectual property owners, and to avoid future conflicts.

5.1.1. Value of Mapping Cyberspace

Having presented the logic as well as the design principle, structure and architecture, this section summarizes the value added by this thesis on following parameters:

Conceptually, it is a step in the direction for reducing the ambiguities between the different forms of human activities, and providing a coherent understanding of various

knowledge content, social as well as technical, which are central to matters of 'cyberspace". It also enables in ensuring that the number of "voices" who participate in the articulation of propositions, and propositions themselves are accurately represented.

Strategically, mapping the knowledge domain for cyberspace will help in organizing the multidisciplinary knowledge, in all forms, comprehensively, thus, making it more easily accessible to the policy makers and business strategists.

Operationally, the research provides a way of organizing knowledge about cyberspace that is operational as well as replicable. It also provides clarity of information and an alert when a solution to a problem becomes source of new problem. Further, it can be developed in the lingua franca of different communities based on the use of common terms. This will help in interjecting a degree of precision in understanding, even when actors and communities can interpret terms and subject differently.

Functionally, the entire initiative provides the foundations for the design of web-based analytic decision making tools for knowledge management, networking and sharing, related to cyber-international relations. Such web-based analytic decision making tools include:

a) **Coupled-DSM** for end-to-end representation and dependence modeling of the complex world as shown in chapter 2.

b) **Real Options Analysis** for identification of options-type and mechanisms to manage the "perplexities," where a mechanism is an enabler of the option and type represents the type of flexibility provided by the option. Mun (2002, 2003) presents real options analysis tools and techniques for valuing strategic investments and decisions.

c) **System Dynamics Modeling** for understanding the both temporal and spatial nature of social-technical- legal changes when a particular element(s)of the of the model

are modified over a range. This may help in the identifying the performance envelope of the model. Sterman (2000) presents a detailed analysis of system dynamics and its application in modeling the complex systems.

5.2. Limitations

Looking in retrospect, the results of this thesis are based on the foundations of knowledge representation found in the legal arena. The key five principles of such represenation are (Koepsell 2000, 33-38):

a) Categorization scheme for the constituent elements of a system when created may be crude, but nonetheless it forms a framework.

b) A correct framework should be logical and follow the law.

c) Existing system may or may not comprise robust and accurate framework.

d) When existing framework does not provide correct system representation, certain practical problems and inefficiencies may arise.

e) When the system consists of robust framework, the problems associated with weak frameworks may be avoided.

Figure 5-1 reviews the research methodology used in this thesis for both developing and testing the framework used for mapping the cyberspace domain. This research work began by first designing a framework (Task 1) for mapping the knowledge domain of the subject of interest. Design of test mechanisms (Task 2) followed the task one. The test mechanism should follow a logic and the laws of transitivity (von Winterfeldt 1989).

A representative use-case based on the intellectual property rights was developed for actual testing of the framework in the next task. IPR has been selected as the test use-case because it provided both the legal understanding and legislative efforts at international level, in

as collaborative, effective and uniform manner as possible, to protect the rights of intellectual property owners and to avoid future conflicts. Task 3 helped in identifying the practical problems and inefficiencies in the existing framework. Finally, task 4 involved in determining whether by altering the logic of the framework would overcome the shortcoming, identified in task 3. These shortfalls are addressed in the next iteration of the research methodology. The complete framework is presented in Chapter 2 and 3. Chapter 4 presents IPR based test use-case.

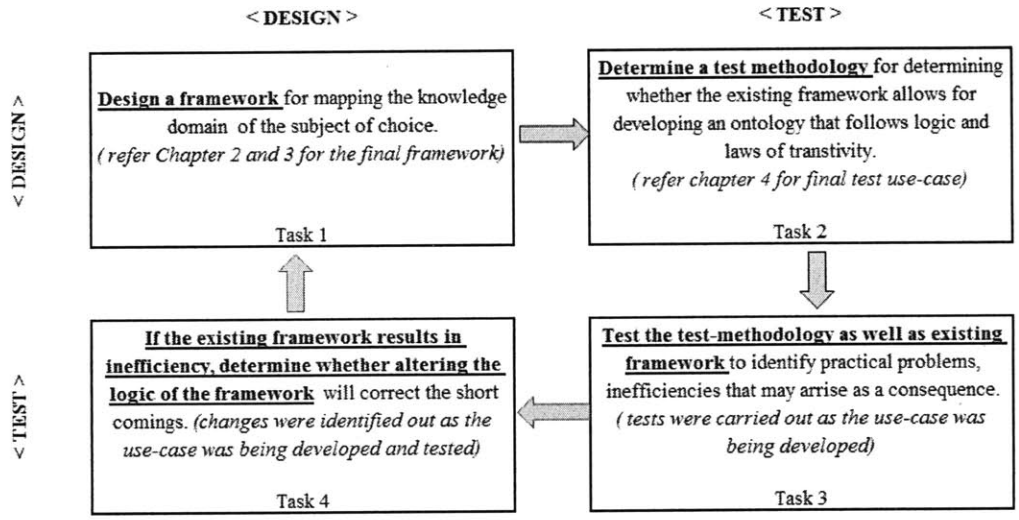


Figure 5-1: Expanded methodology: Guide to current and future work[22].

The first iteration of the research methodology revealed that the knowledge in the "Intellectual Property Rights (IPR)" domain in the context of the cyber-international relations is still at its infancy and terminology used is continually changing. Further, the claims made in this work are based on the current acceptance of the use of common terms that refer to the objects,

[22] Based on author's joint work with Dr. Tsoline Mikaelian for PATFrame research project at Lean Advancement Initiative, MIT, Cambridge, 02139. Fall 2009.

and relations that may exist between those objects/terms, as applied to the phenomenon of cyberspace today. The approach is further complicated if the domain (i.e. intellectual property rights) is not only based on the cumulative past developments but is also continually evolving.

A thorough investigation of such subjects, thus, require more than one iterations of the research methodology but also continual upgradation of the framework over time to reflect both the spatial and temporal developments taking place in field of cyber-international relations. This thesis only provides an adaptive framework to map such interactions and its applicability to only one of the many important domains of cyberspace, i.e. Intellectual Property Rights (IPR).

5.3. Recommendations for Future Work

This section presents recommendations for future work, to address the limitations in the scope of the research.

a) **Use-Case Scenarios:** This research has developed a framework for mapping cyberspace and identified a few dimensions and variables. These variables may be used within a different perspective view of the cyberspace to identify their relative importance. Future research can expand this initial study to develop a comprehensive knowledge base that can be used for explorations in cyber-international relations in the context of US Government priorities.

b) **Logic Development and Implementation:** The next step for the applicability of coupled Dependency Matrix, introduced in Chapter 2, is embedding logic in it and identifying the metrics for the measuring the different "illities" as identified in (Ross, Rhodes, and Hastings 2007).

c) **Automation and software implementation:** Future work can also investigate methods to automate the application of the logical framework for different use-cases/ scenarios.

d) **Extensions of the framework**: Work can also be done in extending the framework for probabilistic modeling to capture the uncertainty in the cyberspace and to develop logical analysis.

This page is intentionally left blank.

REFERENCES

Akao, Yoji. 1990. *Quality Function Deployment : Integrating Customer Requirements into Product Design*. Cambridge, Mass.: Productivity Press.

Avgerou, Chrisanthi, and Kathy McGrath. 2007. Power, Rationality, and the Art of Living Through Socio- Technical Change. *MIS Quarterly* 31 (2):295-315.

Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, and Stephen Wolff. 2010. A Brief History of the Internet. *Internet Society*.

Bartolomei, C.Y. 2007. Qualitative Knowledge Construction for Engineering Systems : Extending the Design Structure Matrix Methodlogy in Scope and Procedure, Engineering Systems Division, Massachusetts Institute of Technology, Cambridge, MA 02139.

Benkler, Yochai. 2006. *The Wealth of Networks : How Social Production Transforms Markets and Freedom*. New Haven [Conn.]: Yale University Press.

Berg, P. 2008. Global Vigilance, Reach, and Power. *Air & Space Power Journal* (4).

Berners-Lee, Tim, and Mark Fischetti. 1999. *Weaving the Web : The Original Design and Ultimate Destiny of the World Wide Web by its Inventor*. San Francisco: Harper

Brooks, Andrew G., and Cynthia Breazeal. 2006. Working with Robots and Objects: Revisiting Deictic Reference for Achieving Spatial Common Ground. In

Proceedings of the 1st ACM SIGCHI/SIGART Conference on Human-Robot Interaction. Salt Lake City, Utah, USA: ACM.

Brown, Ian, Simon Forge, Karen Guevara, Lara Srivastava, Colin Blackman, Jonathan Cave, and Rafael Popper. 2010. Towards a Future Internet: Interrelation between Technological, Social and Economic Trends. Oxford Internet Institute, Oxford University, UK

Browning, T. R. 1999. The Design Structure Matrix. In *The Technology Management Handbook*, edited by R. C. Dorf. Boca Raton, FL: CRC Press.

———. 2001. Applying the Design Structure Matrix to System Decomposition and Integration Problems: A Review and New Directions. *Engineering Management, IEEE Transactions on* 48 (3):292-306.

Carr, Edward Hallett. 1981. *The Twenty Years' Crisis, 1919-1939 : An Introduction to the Study of International Relations*. London: Macmillan.

Chalaby, J. K. . 2000. New Media, New Freedoms, New Threats. *Gazette* 62 (1).

Choucri, Nazli. 2007. *Mapping Sustainability : Logic and Framework*. Edited by J. M. Kauffman. Vol. 11, *Mapping Sustainability : Knowledge e-Networking and the Value Chain*. Dordrecht: Springer Verlag.

———. *Explorations in Cyber International Relations* 2009 [cited April , 27, 2010. Available from http://web.mit.edu/ecir/about.html.

Choucri, Nazli, and Robert Carver North. 1975. *Nations in Conflict : National Growth and International Violence*. San Francisco: W.H. Freeman.

Clark, David D. 2009. Tools of Engagement. edited by D. D. Clark. Cambridge, MA: MIT Computer Science and Artificial Intelligence Laboratory

———. 2010. Characterizing Cyberspace: Past, Present and Future. In *MIT CSAIL Working Paper*. Cambridge MA 02139: Massachusetts Institute of Technology.

———. 2010. Tools of Engagement: Mapping theTussles in Cyberspace. In *MIT CSAIL Working Paper*. Cambridge MA 02139: Massachusetts Institute of Technology.

Clausewitz, Carl von, Michael Howard, Peter Paret, and Beatrice Heuser. 2006. *On War*. New York: Oxford University Press.

Danilovic, Mike, and Tyson R. Browning. 2007. Managing complex product development projects with design structure matrices and domain mapping matrices. *International Journal of Project Management* 25 (3):300-314.

Department of Defense. 2006. Joint Publication 3-13 : Information Operations: http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf.

———. 2009. Dictionary of Military and Associated Terms.

———. *The DoDAF Architecture Framework Version 2.0* 2009. Available from http://cio-nii.defense.gov/sites/dodaf20/index.html.

Dodder, R. S. , J. M. Sussman, and J. B. McConnell. 2004. The concept of the "CLIOS process": Integrating the Study of Physical and Policy Systems using Mexico City as an Example.

Drew, Katherine F., and David Scheidt. 2004. Distributed Machine Intelligence for Automated Survivability. In *ASNE Engineering the Total Ship*. Gaithersburg, Maryland.

Easterbrook, Frank H. 1996. Cyberspace and the Law of the Horse. University of Chicago Legal Forum.

Endsley, Mica R. 1995. Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors: The Journal of the Human Factors and Ergonomics Society* 37 (1):33.

Eppinger, Steven D., and Vesa Salminen. 2001. Patterns of Product Development Interactions. Paper read at International Conference on Engineering Design, at Glasgow, UK.

Gates, Robert M. . 2008. Association of American Universities. *Department of Defense, Speech 1228.*

Gray, Colin S. 1999. *Modern Strategy*. New York: Oxford University Press.

Heeks, Richard, and Carolyne Stanforth. 2007. Understanding e-Government Project Trajectories from an Actor-Network Perspective. *European Journal of Information Systems* 16 (2):*165-177.*

Heim, Michael. 1993. *The metaphysics of virtual reality*. New York: Oxford University Press.

Hill, J. D. , and J. N. Warfield. 1972. Unified Program Planning. *IEEE Transactions on Systems, Man and Cybernetics* 2:610-621.

Horton, Keith S, and Trevor A Wood-Harper. 2006. The Shaping of IT Trajectories: Evidence from the U.K. Public Sector. *European Journal of Information Systems* 15 (2):214-224.

Howard, Michael. 1979. The Forgotten Dimensions of Strategy. *Foreign Affairs* 57 (5):975-986.

Jabbour, Kamal. 2009. The Impact of Cyberspace on Strategy. *High Frontier* 5 (3):11-15.

Kalathil, Shanthi , and Taylor Boas. 2006. Open networks closed regimes: The impact of the Internet on authoritarian rule. *Journal of Communication* 56 (1):218-219.

Koepsell, David R. 2000. *The Ontology of Cyberspace : Philosophy, Law, and the Future of Intellectual Property*. Chicago, Ill.: Open Court.

Kollock, Peter. 1998. *Communities in Cyberspace*. Edited by S. Mark: Routledge.

Kuehl, Daniel T. . 2009. From Cyberspace to Cyberpower: Defining the Problem. In *Cyberpower and National Security*, edited by F. D. Kramer, S. H. Starr and L. K. Wentz. Washington, D C: Center for Technology and National Security Policy ; National Defense University Press : Potomac Books.

Lasswell, Harold Dwight. 1950. *Politics, Who Gets What When and How*. New York: Peter Cmith.

Ledet, W. P. , and D. M. Himmelblau. 1970. Decomposition Procedures for the Solving of Large Scale Systems. In *Advances in chemical engineering. Vol.8*, edited by T. B. Drew. New York; London: Academic Press.

Lessig, Lawrence. 1998. The New Chicago School. *The Journal of Legal Studies* 27 (2):661-691.

———. 2002. *Code : and Other Laws of Cyberspace*. New York: The Perseus Books Group.

Levin, Harvey J. 1966. New Technology and the Old Regulation in Radio Spectrum Management. *The American Economic Review* 56 (1/2):339-349.

Lonsdale, David J. 2009. The Impact of Cyberspace on Strategy. *High Frontier* 5 (3):21-25.

Mikaelian, Tsoline. 2009. An Integrated Real options Framework for Model-Based Identification and Valuation of Options Under Uncertainty, Dept. of Aeronautics and Astronautics, Massachusetts Institute of Technology, Cambridge, MA 02139.

Mun, Johnathan. *Real Options Analysis Tools and Techniques for Valuing Strategic Investments and Decisions*. John Wiley & Sons 2002. Available from http://www.netlibrary.com/urlapi.asp?action=summary&v=1&bookid=79080.

———. *Real Options Analysis Course Business Cases and Software Applications*. John Wiley 2003. Available from http://www.netlibrary.com/urlapi.asp?action=summary&v=1&bookid=82745.

Murray, Andrew D. 2007. *The Regulation of Cyberspace : Control in the Online Environment*. Milton Park, Abingdon [UK]; New York, NY: Routledge-Cavendish.

Nye, Joseph S. 2004. *Soft power : the means to success in world politics*. New York: Public Affairs.

———. 2010. Cyber Power. In *ECIR Worling paper dated February 15, 2010*. Cambridge, MA Harvard Kennedy School.

Obama, Barack. 2008. Remarks of the Senetor. West Lafayette, IN 47907: Purdue University.

Pimmler, T.U., and Steven D. Eppinger. 1994. Integration Analysis of Product Decompositions. Paper read at ASME 6th Int. Conf. on Design Theory and Methodilogy, at Minneapolis, MN.

Porter, Michael E., and Claas van der Linde. 1995. Toward a New Conception of the Environment-Competitiveness Relationship. *The Journal of Economic Perspectives* 9 (4):97-118.

Postel, Jon. 2010. *RFC 1591 - Domain Name System Structure and Delegation.* Network Working Group, The Internet Engineering Task Force 1996 [cited May 3, 2010 2010]. Available from http://tools.ietf.org/html/rfc1591#section-4.

Pouloudi, A., and E. Whitley. 2000. Representing Human and Non-Human Stakeholders: On Speaking with Authority. In *Organizational and Social Perspectives on Information Technology : IFIP TC8 WG8.2 International Working Conference on the Social and Organizational Perspective on Research and Practice in Information Technology, June 9-11, 2000, Aalborg, Denmark*, edited by R. Baskerville. Boston, Mass. : Kluwer Acad. Publ.

Protocols.com. 2010. Internet Protocols.

Quayle, Tony. 2009. Lecture 3. *ESD.33 Systems Engineering, MIT, Cambridge, MA.*

Rattray, Gregory J. 2001. *Strategic Warfare in Cyberspace.* Cambridge, Mass. [u.a.: MIT Press.

Richards, Matthew G., Adam M. Ross, Daniel E. Hastings, and Donna H. Rhodes. 2008. Empirical Validation of Design Principles for Survivable System Architecture. In *2nd Annual IEEE Systems Conference*. Montreal, Canada.

Ross, A.M., D.H. Rhodes, and D.E. Hastings. 2007. Defining Changeability: Reconciling Flexibility, Adaptability, Scalability and Robustness for Maintaining Lifecycle Value. Paper read at INCOSE International Symposium 2007, at San Diego, CA.

Shannon, Cloud E. 1948. A Mathematical Theory of Communication. *The Bell System Technical Journal* 27:379-423 , 623-656.

Sharman, David M., and Ali A. Yassine. 2007. Architectural Valuation using The Design Structure Matrix and Real Options Theory. *Concurrent Engineering : Reseach and Applications* 14 (2):157-173.

Sommerdagger, Joseph H. 2000. Against Cyberlaw. *Berkeley Technology Law Journal* 15 (3):1145.

Sosa, Manuel E. , Steven D. Eppinger, and Craig M. Rowles. 2004. The Misalignment of Product Architecture and Organizational Structure in Complex Product Development. *Management Science* 50 (12):1674-1689.

Sterman, John. 2000. *Business Dynamics : Systems Thinking and Modeling for a Complex World*. Boston: Irwin/McGraw-Hill.

Steward, Donald V. 1962. On an Approach to Techniques for the Analysis of the Structure of Large Systems of Equations. *SIAM Review* 4 (4):321-342.

Suh, Nam P. 1998. Axiomatic Design Theory for Systems *Research in Engineering Design* 10 (4):189-209.

Tenorio, Thomas. 2010. Meeting the Challenges of Unmanned and Autonomous System Test and Evaluation. Paper read at Annual Research Review, Center for Systems and Software Engineering ,University of Southern California, at Los Angeles, CA

The White House. 2009. Cyberspace Policy Review: Assuring a Trusted and Resilient Information andCommunications Infrastructure.

US-CERT. *Federal Incident Reporting Guidelines*. Department of Homeland Securty, April 28, 2010. Available from http://www.us-cert.gov/federal/reportingRequirements.html.

US-ITAR. *The Arms Export Control Act (CFR 22 U.S.C. 2778)*. U.S. Department of State, April 28, 2010 2010. Available from http://www.pmddtc.state.gov/regulations_laws/aeca.html.

von Winterfeldt, D. . 1989. A Re-examination of the Normative-Descriptive Distinction in Decision Analysis. *Annals of Operations Research* 19 (499-502).

Weck, Olivier de 2009. Design Structure Matrix (DSM) Paper read at ESD 36 : System Project Management, Lecture 9, at MIT , Cambridge, MA.

Whitley, E. 2009. Perceptions of Govemment Technology, Surveillance and Privacy: the U.K. Identity Cards Scheme In *New directions in Surveillance and Privacy*, edited by B. J. Goold and D. Neyland. Cullompton, Devon, U.K.; Portland, Or.: Willan Pub.

Whitley, E., and I. Hosein. 2008. Doing the Politics of Technological Decision Making: Due Process and the Debate About Identity Cards in the U.K. 17 (6):668-677.

WIPO. 1994. *Trademark Law Treaty and regulations : done at Geneva on October 27, 1994, WIPO publication, no. 225.* Geneva: World Intellectual Property Organization.

———. 1995. *Berne Convention for the Protection of Literary and Artistic Works : Paris Act of July 24, 1971, as amended on September 28, 1979, WIPO Publication No. 287 (E).* Geneva: World Intellectual Property Organization.

———. 1996. *Madrid Agreement for the Repression of False or Deceptive Indications of Source on Goods, of April 14, 1891, WIPO Publication, No. 261.* Geneva: World Intellectual Property Organization.

———. 1997. *Budapest Treaty on the International Recognition of the Deposit of Microorganisms for the Purposes of Patent Procedure and Regulations : Done at Budapest on April 28, 1977, and Amended on September 26, 1980* Geneva: World Intellectual Property Organization.

———. 1997. *Locarno Agreement Establishing an International Classification for Industrial Designs : Signed at Locarno on October 8, 1968, as Amended on September 28, 1979, WIPO Publication, No. 271.* Geneva: World Intellectual Property Organization.

———. 1997. *Nice Agreement Concerning the International Classification of Goods and Services for the Purposes of the Registration of Marks of June 15, 1957, as Revised at Stockholm on July 14, 1967, and at Geneva on May 13, 1977, and*

Amended on September 28, 1979. Geneva: World Intellectual Property Organization.

———. 1998. *Paris Convention for the Protection of Industrial Property of March 20, 1883 : as revised at Brussels on December 14, 1900, at Washington on June 2, 1911, at the Hague on November 6, 1925, at London on June 2, 1934, at Lisbon on October 31, 1958, and at Stockholm on July 14, 1967, and as amended on October 2, 1979, WIPO Publication, No. 201 (E)*. Geneva: World Intellectual Property Organization.

———. 2001. *WIPO Intellectual Property Handbook : Policy, Law and Use, WIPO Publication No. 489*. Geneva: WIPO.

———. 2002. *Lisbon Agreement for the Protection of Appellations of Origin and their International Registration : of October 31, 1958, as Revised at Stockholm on July 14, 1967, and as Amended on September 28, 1979 ; and, Regulations (as in force on April 1, 2002), WIPO Publication, No. 264*. Geneva: World Intellectual Property Organization.

———. 2002. *WIPO Performances and Phonograms Treaty (WPPT) (1996) : with the Agreed Statements of the Diplomatic Conference that Adopted the Treaty, and the Provisions of the Berne Convention (1971) and of the Rome Convention (1961) Referred to in the Treaty, WIPO Publication, No. 227*. Geneva: World Intellectual Property Organization.

———. 2003. *Convention Establishing the World Intellectual Property Organization : Signed at Stockholm on July 14, 1967 and as Amended on September 28, 1979.* Geneva: WIPO.

———. 2006. *Strasbourg Agreement Concerning the International Patent Classification of March 24, 1971, as Amended on September 28, 1979, WIPO Publication, No. 275(E).* Geneva: World Intellectual Property Organization.

———. 2008. *Hague Agreement Concerning the International Registration of Industrial Designs, WIPO Publication, No. 269.* Geneva: World Intellectual Property Organization.

———. 2008. *Madrid Agreement Concerning the International Registration of Marks of April 14, 1891, as Revised at Brussels on December 14, 1900, at Washington on June 2, 1911, at The Hague on November 6, 1925, at London on June 2, 1934, at Nice on June 15, 1957, and at Stockholm on July 14, 1967, and as Amended on September 28, 1979 : Protocol Relating to the Madrid Agreement Concerning the International Registration of Marks Adopted at Madrid on June 27, 1989, and as Amended on October 3, 2006, and on November 12, 2007 : Regulations (as in force on September 1, 2009) and : Administrative instructions (as in force on January 1, 2008), WIPO Publication, No. 204(E).* Geneva: World Intellectual Property Organization.

———. 2008. *Vienna Agreement Establishing an International Classification of the Figurative Elements of Marks : Done at Vienna on June 12, 1973, as Amended*

on October 1, 1985, WIPO Publication, No. 266(E). Geneva: World Intellectual Property Organization.

———. 2009. *Patent Cooperation Treaty (PCT) Done at Washington on June 19, 1970, Amended on September 28, 1979, and Modified on February 3, 1984 and on October 3, 2001: and Regulations Under the PCT (as in force from July 1, 2009)*. Geneva: World Intellectual Property Organization.

WIPO Academy. 2007. Module 1: The Concept of Copyright, the Historical and the International Framework. In *Course :DL-201E Copyright and Related Rights*. Geneva, Switzerland: World Intellectual Property Organisation.

———. 2007. Module 2: The Berne Convention- Principles and Notions of Works. In *Course :DL-201E Copyright and Related Rights*. Geneva, Switzerland: World Intellectual Property Organisation.

———. 2007. Module 2:Internet Domains and Trademarks. In *Course :Electronic Commerce and Intellectual Property*. Geneva, Switzerland: World Intellectual Property Organisation.

———. 2007. Module 3: Electronic Business and Patents. In *Course :Electronic Commerce and Intellectual Property*. Geneva, Switzerland: World Intellectual Property Organisation.

———. 2007. Module 3: The Berne Convention- Convention of Protection: Rights and Limitations. In *Course :DL-201E Copyright and Related Rights*. Geneva, Switzerland: World Intellectual Property Organisation.

———. 2007. Module 5: Managing Intellectual Propety Online. In *Course :Electronic Commerce and Intellectual Property*. Geneva, Switzerland: World Intellectual Property Organisation.

———. 2007. Module 6: International Implications and Enforcement. In *Course :Electronic Commerce and Intellectual Property*. Geneva, Switzerland: World Intellectual Property Organisation.

———. 2007. Module 6: Related Rights. In *Course :DL-201E Copyright and Related Rights*. Geneva, Switzerland: World Intellectual Property Organisation.

———. 2007. Module 9: Collective Management of Rights. In *Course :DL-201E Copyright and Related Rights*. Geneva, Switzerland: World Intellectual Property Organisation.

Wylie, J. C. 1967. *Military Strategy: A General Theory of Power Control*. New Brunswick, N.J.: Rutgers University Press.

Zimmermann, H. 1980. OSI Reference Model -The ISO Model of Architecture for Open Systems Interconnection. *Communications, IEEE Transactions on* 28 (4):425-432.

Zittrain, Jonathan. 2008. *The future of the Internet and how to stop it*. New Haven [Conn.]: Yale University Press.

APPENDIX A

BIOGRAPHY OF:

Nazli Choucri is a professor at MIT Department of Political Science. She works in international relations and international political economy with a special focus on conflict, connectivity, and the global environment. Her current research is on the power of knowledge in the global economy, and the political and strategic implications of e-development, e-knowledge, and e-politics.

David Clark is a Senior Research Scientist at the MIT Computer Science and Artificial Intelligence Laboratory. Since the mid 70s, Dr. Clark has been leading the development of the Internet; from 1981-1989 he acted as Chief Protocol Architect in this development, and chaired the Internet Activities Board. In the 1990, he developed extensions to the Internet to support real-time traffic, which involved pricing and related economic issues. His work has increasingly emphasized the interplay of technical and policy factors, looking at specific problems including broadband deployment and network security. Current activities focus on an NSF project to look at architecture for an Internet looking 15 years in the future. He is former chairman of the Computer Science and Telecommunications Board of the National Research Council.

APPENDIX B

BINARY MATRIX MULTIPLICATION[23]

For the calculation of DSM^2 and higher orders of DSM (DSM^3...), following operators are used.

Boolean multiplication-If x, y, z ... are propositions, their logical product (x • y • z •...) in any order is the new proposition "All of x, y, z ... are true." i.e., truth-value of (x • y • z •...) is 1 if that of every factor is 1 but it is 0 if that of any factor is 0.

$$x \cdot y \cdot z = \min[x, y, z]$$

Boolean union-If x, y, z ... are propositions, their Boolean union or logical sum (x ∪y ∪z ...) is the new proposition "At least one of x, y, z, ... is true." Thus, the truth-value of (x ∪ y ∪ z ∪ ...) is 0 if that of every addend is 0, but it is 1 if that of any addend is 1. Briefly,

$$x \cup y \cup z = \max\ [x, y, z]$$

Further, Boolean multiplication is distributive with respect to Boolean union; that is,

$$x \bullet (y \cup z) = (x \bullet y) \cup (x \bullet z)$$

and, the elements c_{ij} of the matrix C= A · B are found

$$c_{ij} = \bigcup_{k=1}^{n} a_{ik} \cdot b_{kj}$$

---

[23] (Ledet and Himmelblau 1970)