Spring 2019

Quantifying Impact of Cyber Actions on Missions or Business Processes: A Multilayer Propagative Approach

Unal Tatar
Old Dominion University, unaltatar@gmail.com

QUANTIFYING IMPACT OF CYBER ACTIONS ON MISSIONS OR BUSINESS PROCESSES: A MULTILAYER PROPAGATIVE APPROACH

by

Unal Tatar
B.S. May 2004, Bilkent University
M.S. September 2009, Middle East Technical University

A Dissertation Submitted to the Faculty of
Old Dominion University in Partial Fulfillment of the
Requirements for the Degree of

DOCTOR OF PHILOSOPHY

ENGINEERING MANAGEMENT AND SYSTEMS ENGINEERING

OLD DOMINION UNIVERSITY
May 2019

Approved by:

Adrian Gheorghe (Director)

C. Ariel Pinto (Member)

Charles B. Daniels (Member)

Hayretdin Bahsi (Member)

ABSTRACT

QUANTIFYING IMPACT OF CYBER ACTIONS ON MISSIONS OR BUSINESS PROCESSES: A MULTILAYER PROPAGATIVE APPROACH

Unal Tatar
Old Dominion University, 2019
Director: Dr. Adrian Gheorghe

Ensuring the security of cyberspace is one of the most significant challenges of the modern world because of its complexity. As the cyber environment is getting more integrated with the real world, the direct impact of cybersecurity problems on actual business frequently occur. Therefore, operational and strategic decision makers in particular need to understand the cyber environment and its potential impact on business. Cyber risk has become a top agenda item for businesses all over the world and is listed as one of the most serious global risks with significant financial implications for businesses.

Risk analysis is one of the primary tools used in this endeavor. Impact assessment, as an integral part of risk analysis, tries to estimate the possible damage of a cyber threat on business. It provides the main insight into risk prioritization as it incorporates business requirements into risk analysis for a better balance of security and usability. Moreover, impact assessment constitutes the main body of information flow between technical people and business leaders. Therefore, it requires the effective synergy of technological and business aspects of cybersecurity for protection against cyber threats.

The purpose of this research is to develop a methodology to quantify the impact of cybersecurity events, incidents, and threats. The developed method addresses the issue of impact quantification from an interdependent system of systems point of view. The objectives of this research are (1) developing a quantitative model to determine the impact propagation within a

layer of an enterprise (i.e., asset, service or business process layer); (2) developing a quantitative model to determine the impact propagation among different layers within an enterprise; (3) developing an approach to estimate the economic cost of a cyber incident or event.

Although there are various studies in cybersecurity risk quantification, only a few studies focus on impact assessment at the business process layer by considering ripple effects at both the horizontal and vertical layers. This research develops an approach that quantifies the economic impact of cyber incidents, events and threats to business processes by considering the horizontal and vertical interdependencies and impact propagation within and among layers.

This dissertation is dedicated to my wife Irem and sons Levent and Bulent.

I also dedicate this work to my parents.

ACKNOWLEDGMENTS

I would like to express my appreciation to my family, advisor, committee members and friends who provided intellectual and motivational support to make this dissertation possible.

My family deserves endless gratitude. They showed great patience for my long periods of study and provided the best and most support.

My advisor, Dr. Gheorghe – *Doctorvater,* has always welcomed my ideas and provided his strong support to realize these ideas in the most efficient manner. My committee members, Dr. Pinto, Dr. Bahsi, and Dr. Daniels offered invaluable feedback on my research design. Dr. Sousa-Poza's guidance and mentorship were also priceless to create my research program.

Whole ERI team and especially my dearest friends, Omer Keskin and Omer Poyraz, were encouraging by exchanging views on the progress of my study and strengthening my motivation.

I would also like to express my deep sense of gratitude and sincere thanks to the Engineering Management and Systems Engineering Department and all its professors, faculty, staff and research assistants. I would not have been able to complete this research without encouraging and constructive environment provided by them.

NOMENCLATURE

A	Availability
AOD	Availability of Data
APT	Advanced Persistent Threat
BOL	Baseline Operability Level
BOLP	Baseline Operability Level of Node P
BP	Business Process
C	Confidentiality
COD	Criticality of Dependency
CODP	Criticality of Dependency of Node P
CAPT	Captain
CIA	Confidentiality, Integrity, Availability
CISO	Chief Information Security Officer
$Cov	Insurance Coverage
$Ctl	Cost of Control
CPM	Critical Path Method
CSES	Cyberspace Security Econometrics System
$Ded	Insurance Deductible
DDNA	Development Dependency Network Analysis
DDoS	Distributed Denial of Service
DNS	Domain Name System
FDNA	Functional Dependency Network Analysis
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FFDF	Failure Flow Decision Function
GNSS	Global Navigation Satellite Systems
I	Integrity
IEC	International Electrotechnical Commission

IEEE	Institute of Electrical and Electronics Engineers
$Imp	Cost of Impact
IOD	Impact of Dependency
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology
MOE	Measure of Effectiveness
MOP	Measure of Performance
NATO	The North Atlantic Treaty Organization
NIST	National Institute of Standards and Technology
OBIMC	Ontology Based Information Management Capability
P	Operability
PC	Personal Computer
PERT	Program Evaluation and Review Technique
PII	Personally Identifiable Information
$Prm	Premium
SE	Self-Efficiency
SME	Subject Matter Experts
SOD	Strength of Dependency
SODA	Stochastic Operational functional Dependency Analysis
SODP	Strength of Dependency of Node P
SoS	System of Systems
SDVF	Single Dimensional Value Function
TTL	Time-to-Live
V	Value
w	Weight

TABLE OF CONTENTS

Page

LIST OF TABLES xv

LIST OF FIGURES xvi

Chapter

1 INTRODUCTION 1

1.1 Overview 1

1.2 Definition of Key Concepts and Variables 3

1.3 Purpose of the Study 6

1.4 Research Questions 6

2 LITERATURE REVIEW 8

2.1 Introduction to Literature Review 8

2.2 Method of Literature Review 10

2.3 Results of Analysis 15

2.3.1 General Results from the Analysis 15

2.3.2 Method of Study 15

2.3.3 Method of Validation 16

2.3.4 Representation of Layers in Impact Assessment 18

2.3.5 Representation of Dependencies Impact Propagation 20

2.3.6 Economics of Cybersecurity Risk and Impact 22

Chapter Page

2.3.7 Knowledge Gap 23

3 METHODOLOGY 27

3.1 Introduction 27

3.2 Expected Results and Criteria for Evaluating Results 30

3.2.1 Functional Dependency Network Analysis (FDNA) 31

3.2.1.1. Overview of FDNA 31

3.2.1.2. Previous Studies on FDNA 34

3.2.1.3. Modifications to FDNA 46

3.2.2 Economics of Cybersecurity and Risk 47

3.3 Generalizability and Validity of the Research 51

3.3.1 Generalizability of Research 51

3.3.2 Validity of Research 52

4 MODEL DEVELOPMENT 55

4.1 Introduction 55

4.2 Multiple Component FDNA Nodes 55

4.3 Applicability of FDNA Concepts into Cybersecurity 59

4.4 Modifications to FDNA to Develop FDNA-Cyber 61

4.5.1. Self-Efficiency of Nodes 62

4.5.2. Integrating *Confidentiality, Integrity* and *Availability* 63

Chapter Page

4.5.3. AND Gate Integration 76

4.5.4. OR Gate Integration 83

4.5 Cost Calculation Model 90

4.5.1. Cost Factors for an Adverse Cyber Event 90

4.5.2. Impact of Time and Duration to Cyber Cost 93

4.5.3. Case Study: Economic Impact of a DDoS Attack Targeting a Higher Education Institute 93

4.5.3.1. Background of Online Learning at Higher Education Institutes 93

4.5.3.2. Research Problem 94

1.5.3.2.1. Model 95

4.5.3.3. Application of the model on distance learning data 98

4.5.3.3.1. Data collection and preparation 98

4.5.3.3.2. Simulation results 103

4.5.3.3.2.1. Risk acceptance 104

4.5.3.3.2.2. Risk control 104

4.5.3.3.2.3. Risk transfer 104

4.5.3.3.2.4. Comparison of risk mitigation strategies 105

4.5.3.4. Limitations 106

4.5.3.5. Conclusions 107

Chapter Page

4.5.4. Formula for Calculating Cost of a Cyber Action 107

5 RESULTS AND ANALYSIS 110

5.1 Introduction 110

5.2 Case 1: Impact Propagation and Cost Calculation 110

5.2.1 Build a simple 3-tier network to compare cost and impact difference as per the attacked asset(s) 110

5.2.2 List effected assets/services/task/business processes 112

5.2.3 Cost graph for B1-4 114

5.2.4 Time/Duration impact 115

5.3 Case 2: Redundancy – Resiliency 117

5.3.1 Most critical asset analysis 117

5.3.1.1 Find most critical asset(s) (i.e. asset(s) having most impact) for each BP 118

5.3.1.1.1 Most critical assets in terms of causing loss of operability 118

5.3.1.1.2 Most critical assets in terms of causing cost of loss 119

5.3.1.2 Scenarios where assets are randomly degraded 120

5.3.2 Assess the impact of adding redundancy on resiliency 121

5.3.2.1 Add a redundant asset (i.e. an asset with the same functionality with OR gate) 121

5.3.2.2 Add to A3 (A3.1 and A3.2) 121

5.3.2.3 Add to A1 (A1.1 and A1.2) 123

Chapter Page

5.3.2.4 Compare the impact of adding a redundant node to A3 and A1 124

5.4 Case 3: Compare impact (cost) of attack and security/infrastructure investment scenarios 126

5.4.1 Change system configuration (add a redundant node) 126

5.4.2 Buy a security tool to prevent attack (Anti-virus, Host Based IDS etc.) 126

5.4.3 Comparison of mitigation strategies 127

5.5 Case 4: Risk Management Decision Making 129

5.5.1 Risk management decision making 129

5.5.1.1 Risk acceptance 129

5.5.1.2 Risk avoidance 130

5.5.1.3 Risk control 130

5.5.1.4 Risk transfer (insurance) 130

5.5.2 Scenarios for risk management strategies 130

5.5.2.1 Risk acceptance 131

5.5.2.2 Risk control 131

5.5.2.3 Risk transfer 132

5.5.2.4 Risk control and risk transfer 133

5.5.3 Comparison of risk management strategies 133

5.6 Sensitivity Analysis 135

Chapter Page

6 CONCLUSION 141

6.1 High Level Summary of Findings 141

6.2 Significance of the Study 141

6.3 Future Research 145

REFERENCES 146

VITA 157

LIST OF TABLES

Table Page

1. Results of Queries in IEEE Xplore and SCOPUS 11

2. Analysis Items 14

3. The detailed analysis of reviewed papers 17

4. Data for domicile, tuition rates, and types of courses 99

5. 12-hour DDoS attack impact 101

6. Risk Mitigation Strategy Costs 104

7. Relation of potential consequences and cost factors 108

8. List of affected nodes when each asset is degraded to zero one by one 113

9. Business Process costs caused by degradation of each asset 119

10. Effect of adding a redundant node for A3 on total cost 123

11. Effect of adding a redundant node for A1 on total cost 124

12. Comparison of risk management strategies for each scenario 135

LIST OF FIGURES

Figure Page

1. Impact Dependency Graph 3

2. A taxonomy of Information security risk assessment approaches 4

3. Horizontal and Vertical Dependency of Layers 20

4. Research methodology 29

5. A Sample 4-Node FDNA Graph Topology 31

6. A 2-Node FDNA Graph 33

7. Capability Portfolio Context Representation of FDNA Graph 34

8. Iterative validation process 53

9. Representation of a constituent node 57

10. Dependency Relations of Constituent Nodes and Single Nodes 58

11. A 2-Node FDNA Graph 63

12. An FDNA-Cyber node 64

13. A 2-node FDNA-Cyber graph 65

14. A 3-node FDNA-Cyber graph 69

15. A 3-node FDNA-Cyber graph 72

16. AND dependency of a 3-node FDNA graph 76

17. A 3-node FDNA-Cyber graph with AND gate dependency 78

18. A 3-node FDNA-Cyber graph with AND gate dependency 80

19. OR dependency of a 3-node FDNA graph 84

20. A 3-node FDNA-Cyber graph with OR gate dependency 85

21. A 3-node FDNA-Cyber graph with OR gate dependency 87

Figure Page

22. Cost factors of an adverse cyber event 92

23. The Mitigation Strategy Selection Algorithm..... 96

24. Total number of distance learning courses for each day..... 98

25. Value of Stream for 15-minute periods for each day..... 100

26. Direct impact of a 12-hour DDoS attack 102

27. Direct impact of a 72-hour DDoS attack 103

28. Cost of Impact and Mitigation Strategies 106

29. Sample 3-tier enterprise network..... 111

30. Total cost caused by each failed asset..... 114

31. Total costs caused by CIA 115

32. Total cost caused by each failed asset with a different time and duration..... 117

33. Cumulative performance degradation of business process nodes…..... 118

34. Total cost caused by each failed group of assets 120

35. Modified network with redundancy added for A3..... 122

36. Modified network with redundancy added for A1..... 123

37. Total cost caused by each failed asset and redundant nodes 125

38. Total cost caused by partially degraded assets in comparison with the full degradation scenarios 127

39. Total cost caused by partially degraded assets in comparison with the redundancy scenarios 128

40. Total cost caused by partially degraded assets in comparison with the redundancy scenarios with regards to CIA values 129

Figure Page

41. Total costs for risk acceptance strategy 131

42. Total costs for risk control strategy 132

43. Comparison of risk management strategies 134

44 Cost of degradation of C-I-A values of Asset 1 to 4..... 136

45 Operability level of C-I-A for Asset 1 136

46 Operability level of C-I-A for Asset 2 137

47 Operability level of C-I-A for Asset 3 138

48 Operability level of C-I-A for Asset 4 138

49 Operability levels of Confidentiality values of Assets A1 to A4..... 139

50 Operability levels of Integrity values of Assets A1 to A4 139

51 Operability levels of Availabilty values of Assets A1 to A4..... 140

CHAPTER 1

1 INTRODUCTION

1.1 Overview

Ensuring the security of cyberspace is one of the biggest challenges the modern world has been come across due to the complexity of the domain. Solutions to cybersecurity problems have to cover all aspects of the problem domain including technical, organizational, and human aspects. All individuals ranging from top-most strategic decision makers to ordinary computer users have particular responsibilities that cannot be delegated to others. Thus, the risk management notion of each individual is the most vital countermeasure to preserve cybersecurity.

As the cyber security environment is getting more integrated with the real world, the direct impact of cybersecurity problems on real business frequently occur. Therefore, operational and strategic decision makers in particular need to understand the cyber environment and its potential impact on business. For instance, cyber infrastructures are heavily used in military operations. Commanders at different rankings must have the capability to figure out the effect of cyber threats to military operations and make decisions accordingly.

Protection against cyber threats requires a holistic approach that should cover technology, business and human aspects of the problem domain. Impact assessment, which highly involves the harmonization of technological findings with business requirements, is a critical analysis task that commonly exists in risk, incident, event, or vulnerability management activities (Bahsi, Udokwu, Tatar, & Norta, 2018).

Impact assessment, as an integral part of risk analysis, tries to estimate the possible damage of a cyber threat on a business or mission. It provides the primary insight into risk prioritization as it incorporates the business or mission requirements into risk analysis for a better balancing of

security and usability. Moreover, this assessment constitutes the main body of information flow between technical people and business leaders. Therefore, it requires effective harmonization of technological and business aspects of cybersecurity (Bahsi, et al., 2018).

To calculate the impact of cyber incidents and events in a way that a senior level decision maker could comprehend, assessing the impact on mission or business processes is a better option than doing it at the asset or service level. The asset layer represents the information systems, the service layer shows the IT or business functions that can be performed by a group of assets, and the mission layer models the ongoing mission or business processes in the target organization(s) (Bahsi, et al., 2018).

Accurate cyber impact assessment requires considering impact propagation at horizontal and vertical layers. The dependencies between the unit components of each layer are called horizontal dependencies. For instance, some studies consider a task as the unit of a mission and define the ordering requirements as horizontal dependencies at the mission layer. Vertical dependencies link the components belonging to different layers. Jakobson (2011) proposes an impact dependency graph as shown in Figure 1.

Although there are many studies in cybersecurity risk quantification, only a few studies focus on mission level impact assessment by considering ripple effects at both horizontal and vertical layers.

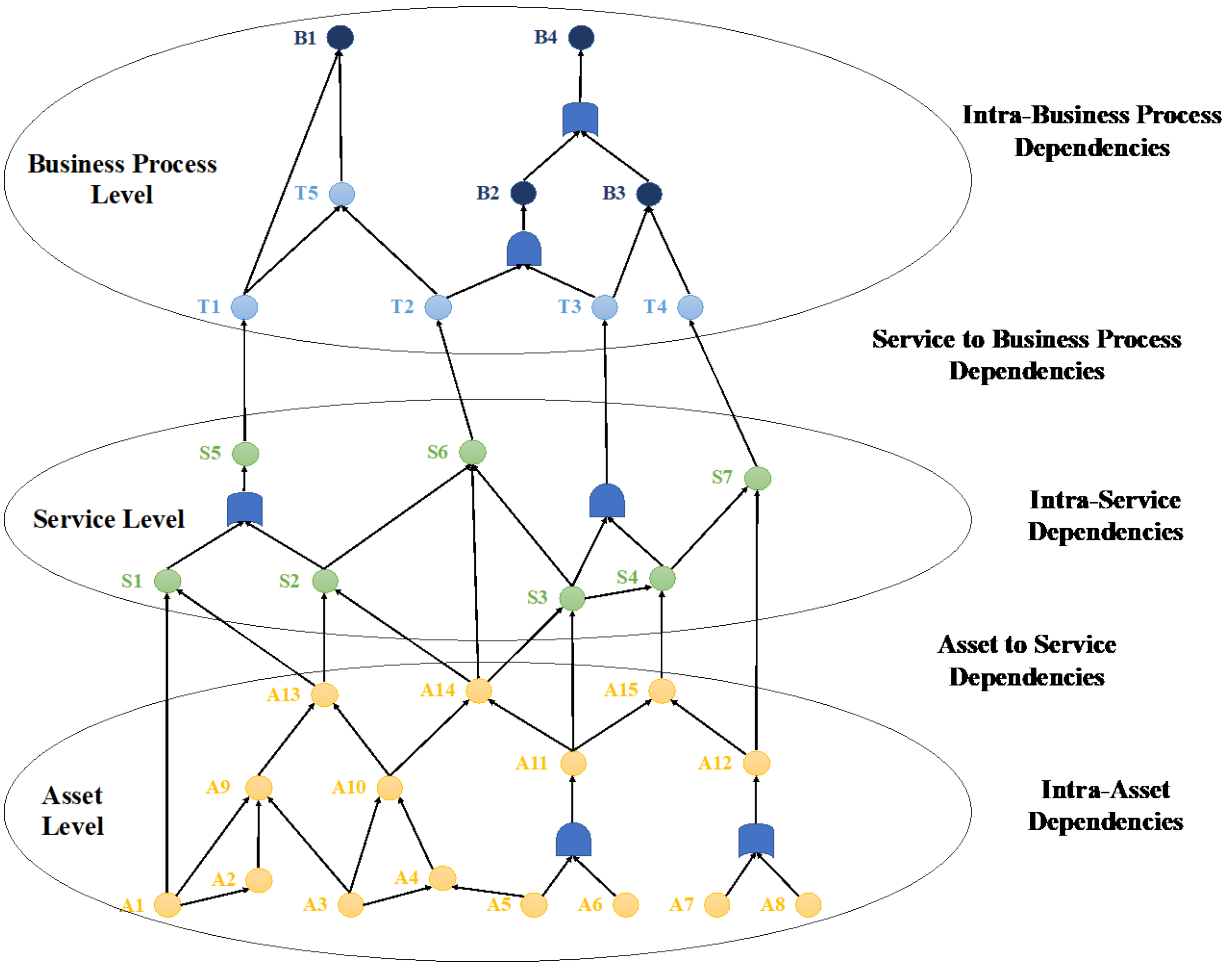


Figure 1. Impact Dependency Graph (adapted from Jakobson 2011)

1.2 Definition of Key Concepts and Variables

In this section, the key concepts used in this proposal are defined. Shameli-Sendi, Aghababaei-Barzegar, and Cheriet created a taxonomy for information security risk assessment methods as depicted in Figure 2 (Shameli-Sendi, Aghababaei-Barzegar, & Cheriet, 2016). Since the perspective (i.e. asset driven, service driven or business driven), resource valuation (i.e. vertical or horizontal) and risk measurement (i.e. non-propagated or propagated) are also used in

quantification of cyber impact on missions or business processes, the definitions of these review papers are used.

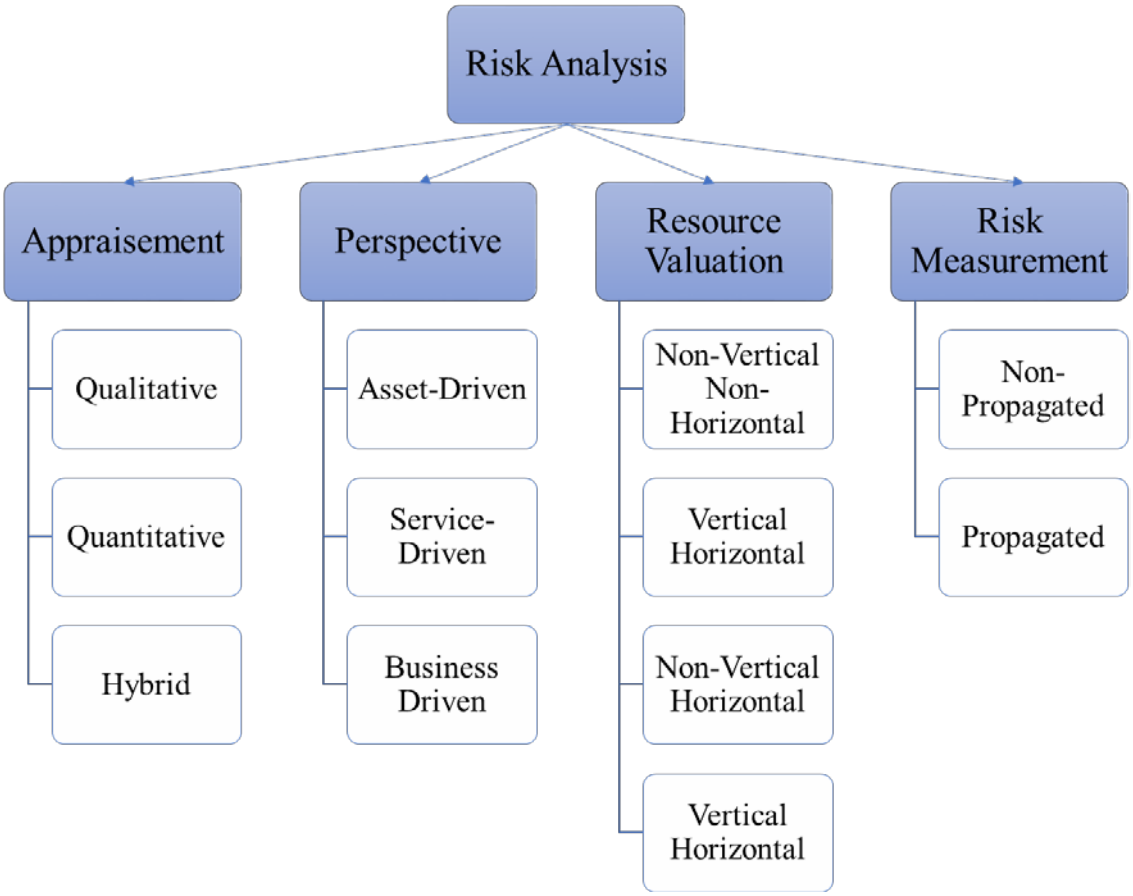


Figure 2. A taxonomy of Information security risk assessment approaches (Shameli-Sendi et al., 2016)

Definition 1: Asset layer is composed of software, hardware, data and people. In the asset driven approach, which is the most common in risk analysis, there are thousands of assets in a medium to large organization to be analyzed and maintained on a regular basis according to various risk scenarios (Jakobson, 2011; Shameli-Sendi et al., 2016).

Definition 2: Service layer is comprised of services that rely on assets to enable tasks and missions. Internet connection, identity management, email and video conferencing are some of the services that can be available in an enterprise (Jakobson, 2011). In the service-driven perspective, “risks are identified and assessed based on their impact on the services” (Shameli-Sendi et al., 2016).

Definition 3: Mission layer is a higher level than asset and service layers. However, it relies on the other two layers. The mission layer is mostly used in military contexts. In the civilian domain, the **business process layer** is used to refer to the mission layer. These two terms are used interchangeably in this study (Jakobson, 2011). In the business process layer perspective, “values are not assigned to assets, but rather to processes that are directly linked to business goals” (Shameli-Sendi et al., 2016).

Definition 4: The **vertical view** is defined as “a bottom-up view and it considers the resources’ contribution degree of a level in the upper level” (Shameli-Sendi et al., 2016) as illustrated in Figure 1.

Definition 5: The **horizontal view** (Jakobson, 2011) is used to refer to “the dependencies between resources at the same level” (Shameli-Sendi et al., 2016).

In a non-propagated model, it is assumed that impact is not propagated to other resources within or among layers. In a propagated model the impact of the attack on the compromised resource propagates to other dependent resources (Jakobson, 2011; Shameli-Sendi et al., 2016).

1.3 Purpose of the Study

The purpose of this study is to develop a methodology to quantify the impact of cybersecurity events, incidents, and threats by considering the dependencies and propagation of impact within and among layers of assets, services, and business processes. The study will address the issue of impact quantification from a system of systems point of view.

The objectives of the research are as follows.

Objective 1: Develop a quantitative model to determine the impact propagation within a layer.

Objective 2: Develop a quantitative model to determine the impact propagation among different layers within an enterprise.

Objective 3: Develop an approach to estimate the economic cost of a cyber incident or event.

1.4 Research Questions

There are many studies and practical solutions to gauge the impact of a cyber incident. However, they are not fully capable of responding to strategic level decision makers' needs especially in calculating the impact on business instead of an impact on targeted assets and assigning an economic value to impact. A novel attempt will be made to improve measurement of the impact of cyber incidents and events. The following questions are identified to frame this study.

1. How can the intra-dependency within a layer (i.e., asset, service, and business process) be modeled?
2. How can the inter-dependency among layers (i.e., asset, service, and business process) be modeled?
3. How can the propagation of impact of cyber actions be modeled?
4. How can the total economic impact of loss be modeled to identify an effective and efficient risk mitigation strategy?

CHAPTER 2

LITERATURE REVIEW

The purpose of this chapter is to review, synthesize, and criticize the literature that describes what is known regarding the impact of cyber incidents and events on missions or business processes. The first section explains the aim of the literature review. In this section the questions explored during the literature review are listed. The second section accounts for the methodology used for a systematic literature review. The third section provides findings from the literature review, particularly the knowledge gap.

Some parts of this chapter have been published in the author et.al.'s (2018) paper entitled "Impact Assessment of Cyber Actions on Missions or Business Processes: A Systematic Literature Review".

2.1 Introduction to Literature Review

The impact assessment is a part of various preventive, detective and corrective cyber-security tasks such as risk assessment, incident handling, or event monitoring. The impact of a threat is a critical analysis item in a risk assessment. The triage phase of an incident handling operation starts with the investigation of the damage caused by the incident. An event generated by security monitoring systems or a finding obtained in a vulnerability analysis is subject to an impact analysis to be adequately validated and prioritized. In this study, event, incident, and threat are covered by the term "cyber actions."

Various academic studies, which can be classified under topics such as situational awareness, dynamic risk analysis, mission impact analysis or cyber battle damage assessment, address the relationship between missions and impacts of cyber actions. In this study, the existing body of literature is reviewed to address the following questions:

(1) Do the current studies represent mission, service and asset (information systems) layers? If so, what models do they use?

(2) Do current studies represent the dependencies of the objects between different layers? Do they handle the dependencies in each layer? If so, what representation methods do they utilize?

(3) What cyber actions trigger the impact assessment?

(4) Do they consider the impact of confidentiality, integrity or availability related cyber actions?

(5) Do they assess mission capability or economic consequences?

(6) What application domains do they cover?

(7) Do they handle multiple processes of one organization?

(8) Do they bring a solution to the processes that involve multiple organizations?

(9) What automation levels do they use for the data collection?

(10) Do they conduct impact assessment during the planning or operational phase of the missions?

(11) What validation methods do they utilize?

(12) Do current studies assess the mission capability or economic consequences?

(13) How is the Functional Dependency Network Analysis method used to model the interdependency of systems?

Additionally, the following research questions are also addressed to deal with research gaps: (1) What research problems should the researchers address? (2) What approaches may provide a promising result for the identified problems?

Franke and Brynielsson (2014) present a comprehensive review of the literature regarding cyber situational awareness. Cherdantseva et al. (2016) review the risk assessment methods that address SCADA systems. However, these studies do not focus on impacts and their relations to missions in a detailed way. Kott, Ludwig and Lange (2017) analyze two studies that conduct mission impact assessment and identify some research challenges in the field. Although it does not include a systematic review of the literature, the discussion about the modeling of attackers and defenders is noteworthy. This literature review is unique as it systematically reviews the relevant literature and profoundly explores impact propagation of cyber actions between IT systems and missions in the analyzed studies.

2.2 Method of Literature Review

The literature review is narrowed to papers that utilize the mission flows as the subject of the impact analysis. Therefore, the studies that establish links between cyber actions and missions and evaluate the propagation of impact and determine the consequences are included. The identification of relevant papers was done in three steps: (a) running keyword queries on academic databases, (b) removing irrelevant papers by manually reviewing the meta-data, (c) selecting the appropriate ones by reading the relevant parts of the papers.

The following keywords are used: mission impact assessment, battle damage assessment, situational awareness and risk management. As the review subject is the impact of cyber actions on missions or business processes, the terms "cyber," "mission," and "business" are added to the search queries as shown in Table 1. The term, “damage assessment” is accompanied by only “cyber” as this term has a specific meaning that does not further clarification. A query is run through all the publications in the IEEE Xplore and journal papers in the SCOPUS databases. Additionally, all the papers published in “Proceedings of the NATO IST128 Workshop Assessing

Mission Impact of Cyberattacks” are included since the scope of the workshop exactly resonates with this review’s subject.

The column of Table 1 called “search result” gives the number of publications identified by the queries that are applied to only metadata such as abstract, title and keywords. After collecting the papers, the abstract of each paper is examined to understand whether it is relevant for further analysis. The column called "manual review result" gives the number of papers obtained after this filtering study. Search queries yielded 773 papers, and the manual reviews of metadata decreased it to 133. The removal of duplications resulted in a set of 76. After scrutinizing all these papers and eliminating those that do not fit the outlined criteria, 22 studies remained for detailed analysis. If one author or the same research team published a more mature paper as a continuation of their previous work, then it is also covered in the analysis.

Table 1. Results of Queries in IEEE Xplore and SCOPUS

Search Query	**IEEE Xplore (all publications)**		**SCOPUS (only journal papers)**	
	Search Result	**Manual Metadata Review Result**	**Search Result**	**Manual Metadata Review Result**
"cyber" + "impact" + "mission"	60	30	10	5
"cyber" + "impact" + "business"	98	16	114	6
"cyber" + "damage assessment"	38	10	4	2
"cyber" + "situational awareness" + "mission"	18	9	8	1
"cyber" + "situational awareness" + "business"	25	6	7	5
"cyber" + "risk" + "mission"	51	20	15	3
"cyber" + "risk" + "business"	157	16	168	4
Total Number	447	107	326	26

Some studies introduce impact assessment based on the value of information- and system assets. If a study does not derive those values by considering the mission, or relevant factors, then it is assumed that the study does not provide a link between cyber actions and missions; thus, it is not included in the analysis. The studies regarding the security of cyber-physical systems that investigate the interactions between cyber- and physical components are reviewed and then the impacts on physical components are related to failures in business functions. Some of the papers quantify the impact of cyber actions in economic terms such as monetary loss without a systematic analysis of business flows. They are also analyzed since the loss is somehow related to the missions.

Table 2 gives the analysis items that are used in this study. A set of categorical values is determined for each item. After reviewing each paper, the relevant value that mostly describes the contribution is selected.

Definition 6: Cyber actions can be a threat, incident or event.

Definition 7: If the expression of the action primarily includes attack vector terms, it is classified as a **threat**.

Definition 8: Incident means that the object of impact assessment is a case that most likely ends up with cybersecurity damage.

Definition 9: The **event** category is assigned to the studies that process the security events generated by monitoring systems or vulnerability scanners. The application domain gives information about the type of organization from which the case studies or examples are selected.

The impact of cyber actions on information system assets is assessed according to the security properties, confidentiality, integrity, and availability whereas the impact on missions is classified by using two categories, mission capability and economic.

Definition 10: Confidentiality is "preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information" (NIST SP 800-122).

Definition 11: Integrity is "the security objective that generates the requirement for protection against either intentional or accidental attempts to violate data integrity (the property that data has not been altered in an unauthorized manner) or system integrity (the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation)" (NIST SP 800-33).

Definition 12: Availability is "ensuring timely and reliable access to and use of information. Note: Mission/business resiliency objectives extend the concept of availability to refer to a point-in-time availability (i.e., the system, component, or device is usable when needed) and the continuity of availability (i.e., the system, component, or device remains usable for the duration of the time it is needed)" (NIST SP 800-160).

Definition 13: Mission capability refers to restrictions imposed on mission resources or outputs due to the occurrence of cyber actions.

Definition 14: Economic impact category labels the studies that measure the consequences according to monetary losses. Assessment layers provide the main framework for the formulation and modeling of impact propagation from the information system assets to missions. The asset layer represents the information systems, the service layer shows the IT or business functions that can be performed by a group of assets, and the mission layer models the

ongoing mission or business processes in target organization(s). The dependencies between the unit components of each layer are called horizontal. For instance, some studies consider a task as the unit of a mission and define the ordering requirements as horizontal dependencies at the mission layer. Vertical dependencies link the components belonging to different layers. Jakobson (2011) proposes an impact dependency graph as shown in Figure 1. This structure is chosen as a reference framework for the evaluation of assessment layers and horizontal/vertical dependencies as it provides a comprehensive view for layers and their dependencies and additionally includes the service layer that may act as a significant facilitator for covering complex IT systems and a multitude of missions belonging to one or more organizations.

Table 2. Analysis Items

Analysis Items	**Categorical Values**
Cyber Actions	Threat, Incident, Event
Application Domain	Military, Enterprise, Cyber-physical Systems, Cloud Computing
Impact on Mission	Mission Capability, Economic Impact
Impact on Information System Assets	Confidentiality, Integrity, and Availability
Assessment Layers	Mission, Service, Asset
Dependency	Horizontal, Vertical
Number of Processes	Multiple, One
Number of Organizations	Multiple, One
Data Collection	Partially Automatic, Manual
Phase of the Mission	Planning, Operational
Method of the Study	No Validation, Simulation, Case Study, Deployment to a Test/Live Environment

The number of organizations and processes handled in the case studies, examples or experiments are also examined. The data collection method is classified as manual if it relies entirely on the extraction of expert knowledge without the help of any automation means. The

method is considered partially automatic when it employs the combination of human intervention and automatic procedures. If the proposed solution operates with the data collected in a real-time, or near real-time manner, then the phase of the mission is acknowledged as operational, otherwise planning. The method of the study is classified as no validation if it does not give any form of validation. Otherwise, it is labeled as a simulation, case study or deployment to a test/live environment.

2.3 Results of Analysis

2.3.1 General Results from the Analysis

45% of the studies occur in the military, 45% in the cyber-physical systems and 9% in the enterprise domain. Main cyber action in 41% is event, 32% threat, and 27% incident. All the papers consider the impact on mission capability to some extent. Only 27% also deal with the economic impact. At the asset layer, availability is the most prevalent impact type at a rate of 82%. The ratios of studies that consider integrity and confidentiality are 68% and 59% respectively. Three studies do not provide precise information about these impact types at all, and one study deals with only integrity attacks. All of the remaining ones address the availability, which shows the most common focus of impact assessment studies. The general overview of the findings are given in Table 3.

2.3.2 Method of Study

50% of the studies employ manual methods that depend on the elicitation of expert knowledge for the identification of dependencies and cyber actions. In the remaining studies, which use partially automated means, the detection of cyber action relies on automatized systems. Extraction of the dependencies, however, is left to manual methods. Thus, practical deployment of such frameworks is not feasible in medium- or large-sized organizations. All studies deal with

missions that belong to only one organization. Though frameworks of most studies handle more than one mission, they do not thoroughly examine the feasibility of the proposed methods in settings having various missions, and Edell (2015) uses a reference architecture with a functional layer that connects asset and business process layers. Garvey and Patel (2014) utilize mission trees, which include the mission elements and main mission functions. Wu, Kang, and Li (2015) describe the impact on assets with some types of damages that are not systematically derived from business processes. Thus, they lack a mission layer but have a service layer. Cam and Mouallem (2013) employ an ordered binary decision diagram for the availability evaluation of services given by the status of assets. Terminal nodes represent the level of mission assurance. Kanoun, Papillon and Dubus (2015) map the terminal node of each attack path to a detrimental event that includes the definition of a security violation in an IT service. As it does not provide a further link with the business process, it is concluded that this study has a service layer but not a business process layer.

2.3.3 Method of Validation

The most frequently preferred validation method is case study, which is 41% although the degree of rigorousness varies significantly. 27% employ simulation whereas 23% demonstrated their contribution at test or live environments and 9% do not provide any validation. 27% of the studies can be applied in operational settings as they obtain real- or near real-time event data. The remaining ones contribute to the planning phase due to the more static nature of the data sources. In this analysis, besides the system monitoring data, vulnerabilities identified during the vulnerability management processes are also categorized as an event. However, as vulnerability identification tasks do not generate continuous real or near real-time data, the mission phase of a study is classified as planning if it only handles vulnerabilities.

Table 3. The detailed analysis of reviewed papers

Paper	Google Scholar Citation	Cyber Actions			Application Domain			Impact on Mission		Impact On Cyber Assets			Assessment Layers			Dependency		Number of Processes	Number of Organizations	Data Collection	Phase of the Mission		Method of the Study			
		Threat	Incident	Event	Military	Enterprise	Cyber-Physical	Mission Capability	Economic Impact	Confidentiality	Integrity	Availability	Mission	Service	Asset	Horizontal	Vertical	1/Multiple	1/Multiple	Manual/Partially Automatic	Planning	Operational	No Validation	Simulation	Case Study	Deployment to a Test/Live Environment
(Jajodia et al. 2011)	71			√	√			√		√	√	√	√		√	√		M	1	P	√				√	
(Jakobson 2011)	65			√	√			√		√	√	√	√	√	√	√	√	M	1	M		√				√
(Abercrombie, Sheldon, and Grimaila 2010), (Sheldon, Abercrombie, and Mili 2009)	8, 32	√					√	√	√	√	√	√	√		√		√	M	1	M	√		√			
(Musman et al. 2011), (Musman and Temin 2015)	16, 4		√		√			√		√	√	√	√		√	√	√	1	1	M	√			√		
(Giani et al. 2012)	12	√					√	√	√		√		√		√			M	1	M	√				√	
(Granadillo et al. 2016)	10	√					√	√	√	√	√	√	√	√	√	√	√	M	1	P	√					√
(Noel at al. 2015)	8	√			√			√		√	√	√	√		√	√	√	1	1	P	√			√		
(Llansó and Klatt 2014) (Llansó, Hamilton, and Silberglitt 2012)	7 5			√			√	√			√	√	√	√	√	√	√	M	1	P	√			√		
(Creese et al. 2013)	7			√		√		√					√		√	√		M	1	P		√			√	
(Garvey and Patel 2014)	6	√			√			√	√	√	√	√	√	√			√	M	1	M	√				√	
(Angelini and Santucci 2015)	5		√				√	√		√	√	√	√		√	√	√	M	1	P		√				√
(Cam and Mouallem 2013)	4	√			√			√		√	√	√	√		√		√	1	1	M	√				√	
(Choobineh, Anderson, and Grimaila 2012)	4		√		√			√					√		√	√	√	1	1	M	√				√	
(Xiang, Wang, and Zhang 2014)	3		√				√	√				√	√		√	√	√	M	1	M	√			√		
(LaVallee, Fix, and Edell 2015)	2			√			√	√					√	√	√		√	M	1	P		√				√
(Lemay, Fernandez, and Knight 2014)	2		√				√	√	√			√	√		√			M	1	P	√			√		
(Heinbockel, Kertzner, and McQuaid 2010)	1			√	√			√				√	√	√	√		√	M	1	M		√				√
(Kanoun, Papillon, and Dubus 2015)	1			√		√		√		√	√	√		√	√	√	√	M	1	P	√				√	
(Lange, Krotofil, and Möller 2015)	1			√			√	√		√	√	√	√		√	√	√	M	1	P		√			√	
(Shaw 2003)	1		√		√			√				√	√		√		√	1	1	M	√			√		
(Wu, Kang, and Li 2015)	1			√			√	√	√	√	√	√		√	√			M	1	P	√				√	
(Lei 2015)	0	√			√			√		√	√	√	√	√	√	√	√	M	1	M	√		√			

2.3.4 Representation of Layers in Impact Assessment

There are three layers in an enterprise to assess the impact of cyber actions. These layers are asset layer, service layer and mission layer (Jakobson, 2011; Shameli-Sendi et al., 2016)

Mission (a.k.a. Business Process)Layer: 91% of the studies establish a mission layer to represent the ongoing mission or business process. A task that may have dependency with other tasks constitutes the unit in this layer. A control-flow idea provides the ordering of tasks, which also forms the primary building block of horizontal dependencies. Choobineh, Anderson and Grimaila (2012), Creese et al. (2013), Musman and Temin (2015), Angelini and Santucci (2015), and Noel at al. (2015) use Business Process Modeling Notation (BPMN) which has constructs for the representation of these dependencies. Granadillo et al. (2016) utilize a probabilistic graphical model, which defines business function nodes and maps them to the business process nodes. However, this model does not reflect the timing and workflow requirements. Shaw (2003) models the workflow of the mission layer as a discrete event system. Some studies that contribute to the cyber-physical domain evaluate the impact of the cyber action using reliability models which also include the representation of physical components (Lemay, Fernandez and Knight 2014; Xiang, Wang and Zhang 2014; Giani et al. 2012; Lange, Krotofil and Möller 2015). As business processes are incorporated into the models, these studies are considered to have a mission layer.

Service Layer: 41% of the studies have a service layer in their frameworks. Lei (2015) and Heinbockel, Kertzner, and McQuaid (2010) explicitly define such a layer that establishes links between asset and mission layers. Other studies illustrate a business/mission function layer that maps assets to function-based categories then to missions. LaVallee, Fix, and Edell (2015) use a reference architecture that has a functional layer that connects asset and business process layers. Garvey and Patel (2014) utilize mission trees, which include the mission elements and main

mission functions. Wu, Kang, and Li (2015) describe the impact on assets with some types of damages, which are not systematically derived from business processes. Thus, it lacks a mission layer but has a service layer. Cam and Mouallem (2013) employ an ordered binary decision diagram for the availability evaluation of services given by the status of assets. Terminal nodes represent the level of mission assurance. Kanoun, Papillon and Dubus (2015) map the terminal node of each attack path to a detrimental event that includes the definition of a security violation in an IT service. As it does not provide a further link with the business process, this study has a service layer but not a business process layer.

Asset Layer: All studies except one included an asset layer. Most of the studies utilize network topology as the representation method for this layer whereas some studies employ models such as attack graphs, which also include the topology information in their formalism (Jajodia et al. 2011; Wu, Kang and Li 2015; Kanoun, Papillon and Dubus 2015; Llansó and Klatt 2014; Noel et al. 2015). Although network connections given in the topology represent the horizontal dependencies, it is important to note that they may help to understand the propagation of the attack but not the impact. Even the attack graph modeling, which is interested in finding the dependencies between vulnerabilities of hosts to identify the attack paths, does not provide an instrument for assessing the impact propagation. In a typical attack scenario, perpetuators infiltrate into the target system, do lateral movements, reach the main target system asset or data and commit the final action such as exfiltration, deletion or modification of the data. The existing horizontal dependencies in the analyzed studies enable us to track and evaluate the possible movements of an attacker until the final act. However, they do not include any data and functional dependency representations, which are required for the impact assessment of the final action and its consequences on other parts of the system. Therefore, they may contribute to the assessment of

the threat but not the impact. Studies in the cyber-physical domain use network topologies that also show the functional dependencies between cyber and physical components that enable the tracing of impact propagation from cyber to physical space (Xiang, Wang and Zhang 2014). Cam and Mouallem (2013) determine the security status of assets by using Time Petri Net models. Shaw (2003) and Choobineh, Anderson and Grimaila (2012) simply handle this layer by a list of cyber-assets. Jakobson (2011) and Lei (2015) utilize graph-based notations.

2.3.5 Representation of Dependencies Impact Propagation

While assessing the impact of cyber actions two types of dependencies could be considered. Vertical view refers to the dependencies between resources of different layers, while the horizontal view refers to the dependencies between resources at the same layer (Shemali-Sendi et al., 2016) (Figure 3).

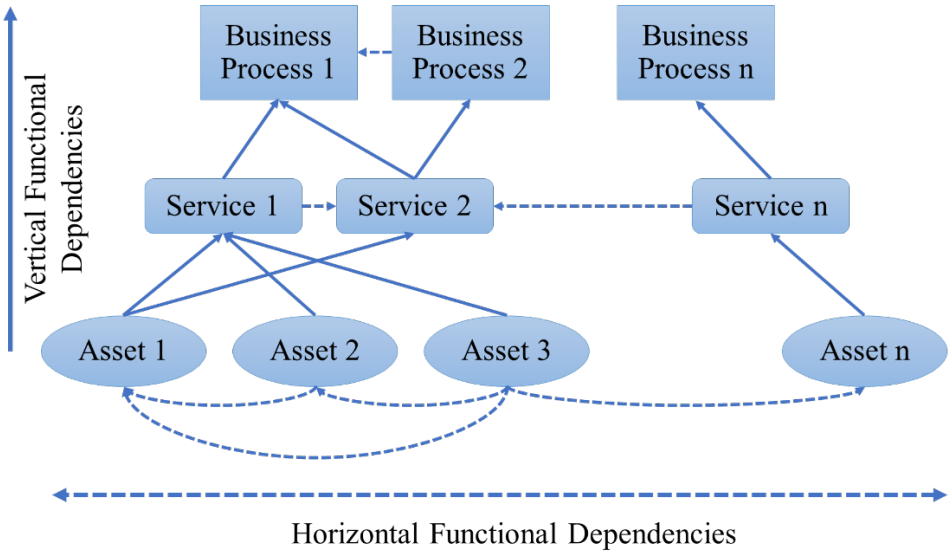


Figure 3. Horizontal and Vertical Dependency of Layers (Shemali-Sendi et al., 2016)

Vertical Dependencies: 77% of the studies define or assume vertical dependencies between assets and mission/service layers. These dependencies establish the socio-technical property by demonstrating the interactions between technology and business processes. The edges between different layers represent vertical dependencies in the dependency graph notation provided in (Jakobson 2011). Musman and Temin (2015) introduce the relevant data- or system assets as resources of tasks defined at the mission layer. Llansó and Klatt (2014) link mission- and service layers via data assets. Granadillo et al. (2016) connect different layers with the edges of a probabilistic graph. Choobineh, Anderson and Grimaila (2012) use a matrix that maps assets to mission tasks. Garvey and Patel (2014) provide the link between mission and service layers by the edges of the mission tree. As the reliability model that represents the physical components acts as a mission layer in some studies of the cyber-physical domain, the association of physical components to a cyber asset forms a vertical dependency (Lemay, Fernandez and Knight 2014; Xiang, Wang and Zhang 2014).

Horizontal Dependencies: Jakobson (2011), Lei (2015), Granadillo et al. (2016), and Llansó and Klatt (2014) utilize a structure that covers all layers, mission, service, asset and all types of dependencies, horizontal and vertical. Jakobson (2011), who also establishes the reference framework in this analysis, employs an impact dependency graph as the main representation of layers and their dependencies. It proposes a method for the analysis of the impacts that propagate over this graph structure. The main contribution of Lei (2015) is not about impact assessment as it utilizes the framework of Jakobson (2011), but it proposes a cyber situational awareness system, which interacts with mission situational management in the physical space to make the continuation of a mission possible in case of a successful cyber attack. Granadillo et al. (2016) provide an impact propagation framework based on a probabilistic graph model for evaluating the

operational and financial consequences of cyber-threats. The study considers that business processes depend on business functions and these functions rely on IT resources. It is assumed that business processes represent the mission layer, business functions correspond to the service layer and IT resources form the asset layer. Horizontal and vertical dependencies are established based on probabilistic models. Llansó and Klatt (2014) estimate the level of attacker efforts and mission impacts. The noteworthy contribution of this study is that it quantifies the impact on a mission by the mission- and system-based effectiveness metrics deduced from the sensor data.

2.3.6 Economics of Cybersecurity Risk and Impact

Quantifying impact of cyber actions in monetary values would help make better decisions while choosing a risk mitigation strategy. There are three focus areas of the papers, which include economic aspects of cyber risk and impact: reliability (Sheldon, Abercrombie and Mili, 2008; Abercrombie, Sheldon, and Mili 2009; Lemay, Fernandez and Knight, 2014), resiliency (Giani, et. al. 2012), and return of investment (Granadillo, et. al. 2016; Garvey and Patel, 2014).

Abercrombie, Sheldon and Grimaila (2010), Wu, Kang and Li (2015), Granadillo et al. (2016), and Garvey and Patel (2014) cover all types of impacts on missions and cyber assets. Abercrombie, Sheldon and Mili (2008) measure the impact of threats on security requirements according to the views of each stakeholder. It evaluates the violation of security requirements with the term, mean failure cost, which is the quantification of the productivity, business, or data losses regarding the financial basis. Abercrombie, Sheldon and Grimaila (2010) discuss the utilization of the same impact measurement idea to a mission-centric analysis rather than a security requirement-centric one. However, it does not provide an example or use case analysis that explores the feasibility of the idea. Wu, Kang, and Li (2015) determine the value of assets according to the economic loss, environmental damage, casualties and repair cost incurred in case of being

attacked. This study does not conclude the descriptions of loss by the analysis of mission flows. Granadillo et al. (2016) evaluate the operational and financial consequences of mitigations to cyber-threats. The financial impact of an attack is determined according to the annual loss expectancy that covers the loss of asset, data, reputation, revenue or customers. The limitation of this study is that it employs the impact propagation constructs for the evaluation of the mitigation actions, not cyber action itself. Garvey and Patel (2014) use utility theory for measuring the performance of organizations and effectiveness of missions. This study determines the economic benefit returns of cybersecurity investments. However, they do not represent the asset layer in their impact propagation framework. In all these studies, the impacts of cyber actions that cause confidentiality, integrity or availability results are covered at the asset layer. As a different approach, Musman and Temin (2015) classify the impact types into six categories, interruption, degradation, interception, modification, fabrication and unauthorized use.

2.3.7 Knowledge Gap

The analyzed papers do not consider the cross-organizational nature of most enterprise and military operations. In enterprise operations, collaborations are experienced in the form of outsourcing while as contractors in military missions. Since assets are shared across all parties involved in a mission (R. Matulevičius et al. 2016), security requirements and controls must be applied on information systems that support the assets across all collaborating parties. Parties involved in the mission have separate goals depending on the role they respectively play. Differences in goals may cause variations in the perception of impacts that may lead to different security requirements and countermeasures. Further investigation of goal-based modeling methods in representing the function-based relationship between collaborating parties should be done. These methods model the processes according to the overall goal of the mission (Sterling and

Taveter 2009). The overall goal is further broken down into functional goals. Tasks required to achieve each functional goal of the mission are assigned to a role and are carried out by a specific party collaborating in the mission.

Almost all analyzed studies have a layer that represents the information-system assets. The typical approach employed in this layer is network- and asset-centric rather than data-centric as the system assets are mapped to the nodes of the service- or mission layers without the consideration of data assets and the identification of relevant data flows. The drawback of this approach is twofold: First, the horizontal dependencies cannot be precisely identified, and impact analysis starts with the incomplete asset set. For instance, a datum can reside in many nodes or be temporarily stored in the network-forwarding nodes, meaning that a confidentiality threat to each of these nodes may have an impact on the mission. Only the tracing of the data flows can reveal the complete set of assets that may cause information leakage. Second, the approach may lead to putting system administrators, not the information asset owners, into the center for the extraction of expert knowledge, although they are the least familiar with business processes. The asset-centric approaches are not enough to cover the risk landscape induced by recent technologies such as cloud computing, mobility, and the Internet of Things (NSS Labs 2013), and the focus of threat modeling has shifted to data-centric approaches (National Institute of Standards and Technology 2016). The ICT process model proposed by Musman and Temin (2015) is an example of a data-flow representation. The integration of data-flow models into the asset layer and establishing vertical dependencies with the other layers over data rather than system assets may improve impact assessment capability.

The horizontal dependency in the asset layer is an important construct to analyze the propagation of the impact caused by a cyber action on an asset to other assets. However, in the

studies, these dependencies are only established for the identification of attack paths. Cyber action finally affects an asset at the end of the path, and then the impact propagates only to the service- or mission layer without considering the further spreading in the same layer. It is essential to identify the data and functional dependencies between different assets to understand the propagation of the impact to the other parts that do not belong to the attack path.

The development of automatic- or semi-automatic methods for the identification of dependencies is a significant issue that requires more interest from the research community. For the extraction of all types of dependencies, the analyzed studies rely on manual methods or do not detail the extraction techniques. Business process mining, extracting process knowledge from the event logs, is utilized as an important approach for the automatic identification of business-process flows in the literature (Van Der Aalst 2012). These methods can find the horizontal dependencies at the mission layer. Automatic methods have been applied to network traffic or host- based data actively or passively for the discovery of dependencies among network services (Chen et al. 2008; Natarajan et al. 2012; Lucian et al. 2009; Zand et al. 2014). These methods can determine the horizontal dependencies at asset and service layers.

The identification of vertical dependencies is an open research area. As event logs may have information about business processes and system activities, the adaptation of business process mining techniques is required for the identification of dependencies between the mission and service layers. The discovery methods applied for network services may explore the mappings between asset or service layers.

The dependency data obtained by expert knowledge elicitation may suffer problems regarding data accuracy as the experts may not know all the details of business processes or information systems. On the other side, some researchers question the relevance of findings

identified by automatic dependency discovery methods whereas it is also shown that these methods determine the dependencies experts do not know (Kott, Ludwig, and Lange 2017). Thus, instead of perceiving the expert knowledge elicitation and automatic extraction methods are complete alternatives to each other, both methods should be utilized for having more accurate dependency data.

The analyzed studies calculate the economic impact based on the cost of loss of production and quality. Granadillo et al. (2016) mention the loss of reputation, legal procedures, loss of revenue from clients or customers, and insurance costs. Likewise, Abercrombie, Sheldon and Grimaila (2010) mention a loss of reputation and liability costs. However, none of the papers develops a method to calculate loss of reputation or liability costs. First, new models that include these losses should be developed to show if they have an impact on the business process or missions. Second, studies ignore the ripple effect caused by a cyber action while gauging the economic value of impact. Ripple effect can be calculated by considering the horizontal and vertical dependencies within and between the layers. Third, assigning a realistic monetary value to the impact of a cyber action is a challenge. Calculating the financial value of a business process rather than an asset or a service may give a more realistic and holistic result since it is easier to determine the strategic value of the business process in an enterprise setting. Fourth, the advanced persistent threat in which the primary motivation is the exfiltration of critical data rather than disrupting the ongoing missions is a significant problem. Although early detection of these threats remains a technical challenge, the incurred economic loss should be quantified to make better decisions during risk management or incident handling. The economic impact of all forms of confidentiality threats should be better addressed in future studies.

CHAPTER 3

METHODOLOGY

3.1 Introduction

The characteristics of the research problem affect the methodology to be used. The research problem is quantifying the impact of cyber actions on missions or business processes. The problem involves advanced technologies, attack methods, complex engineering and business systems, interdependencies within and among the layers of an enterprise, propagation of impact and related uncertainties. The first implication is scarcity of data (Martin Eling & Werner Schnell, 2016). In order to cope with this problem, relying on the work of other researchers who have accessed the data and extending adoption of the theories, approaches, and conclusions of their works are essential.

The second implication of the research problem is the impracticality of experimenting in a real operational environment. It is not achievable to empirically test any hypothesis to make inferences and validate the conclusions in a timely and cost effective manner. To provide a solution to the infeasibility of using a real operational environment, modeling and simulation can be used as an effective tool. If real world experimentation is not attainable or not efficient, simulation models of the real system or the proposed system can be employed for experimentation purposes (Law, 2008). Modeling and simulation is an effective decision support tool for both technical and managerial problems (Tolk, 2013). Theories which can be totally new or based on previous theories, can be represented as models and implemented as simulations (Diallo, Padilla, Bozkurt, & Tolk, 2013).

Credibility of the modeling and simulation method relies on validation. Validation is “the process of determining whether a simulation model is an accurate representation of the system, for

the particular objectives of the study" (Law, 2008). A method of validation is applying solutions to a real system and comparing it with the results of the simulation. However, this is not always possible. There are several factors that make validation of findings of a simulation difficult or even impossible. One of these factors is unavailability or inexistence of the real world system or relevant data regarding the system (Law, 2008). Since modeling and simulation is mostly used for problems with few or no empirical data and even though a complete validation is not possible, there are several techniques to validate the system behavior and define how realistic the model is (Tolk, 2013). Tolk (2013) states, "if all parts and their relations and functional transactions are reasonable – which translates to their following an accepted theory that can be used to describe the problem – we assume the model to be reasonable as well".

An important point that should be recognized for the validation of modeling and simulation based research is to consider that a model developed for a particular objective may not be valid for a different objective. During the research design, validation of a simulation model should be utilized in an iterative and continuous manner up to reaching the final model (Landry, Malouin, & Oral, 1983; Robinson, 2013; Sargent, 2015).

Based on the characteristics of the research problem. Modeling and simulation is used as the main research method. The details of the methodology are given in Figure 4.

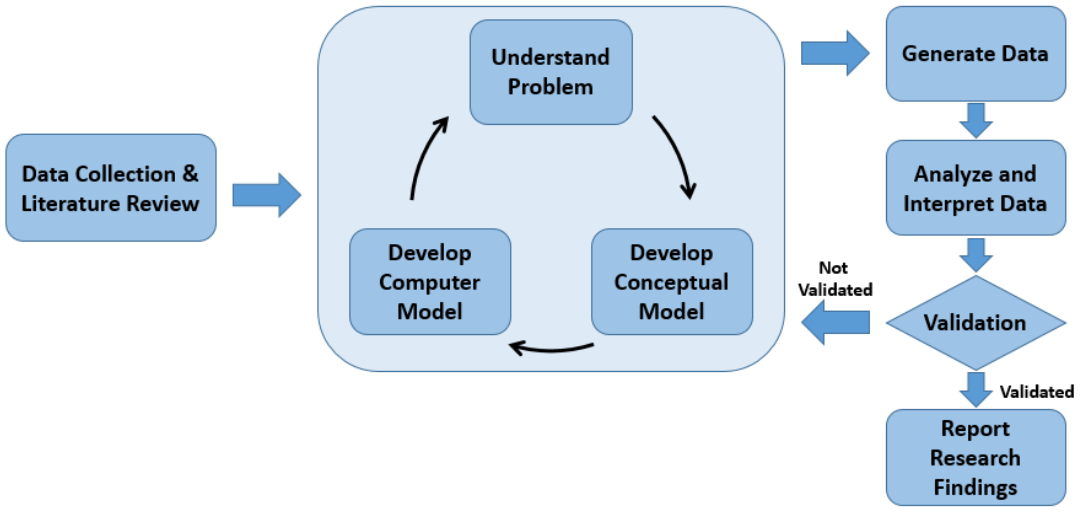


Figure 4. Research methodology

The method of the proposed research is explained below.

1. Review literature to find out valuable approaches and theories which are appropriate for the research problem
2. Model Development
    a. Conceptual Model Development: A conceptual model will be developed based on the theories and approaches being examined. Functional Dependency Network Analysis (FDNA) (Garvey & Pinto, 2009) is the main method, which will be modified to assess the ripple effects. A new approach will also be developed for economic cost estimation.
    b. Develop Computer Model: A computer model will be developed to formalize the conceptual model. A computer model will be improved

thorough iterations to better represent the real world problem to a satisfactory level until reaching an acceptable level.

3. Model Validation: The developed model will be validated through sensitivity analysis. A synthetic network of assets, services and business processes including several types of nodes will be generated in computing environment. The synthetic model will include all types of possible complexities a network may have. The complexities can be interdependencies between nodes within and among layers, different cyber event and incident types, and dependence on time, etc. The model specification and the results of the simulation are validated by sensitivity analysis. Otherwise, the steps in the model development stage will be repeated until a valid model is reached.
4. Reporting: Research findings will be reported.

The model will employ Functional Dependency Network Analysis and methods to calculate economic impact of cyber actions on missions, which are briefly explained in the following sections.

3.2 Expected Results and Criteria for Evaluating Results

The expected results of the developed model are listed in the objectives of the research. These results are listed below.

- A quantitative model to determine the impact propagation within a layer.
- A quantitative model to determine the impact propagation between different layers within an enterprise.
- An approach to estimate the economic cost of a cyber incident or event.

3.2.1 Functional Dependency Network Analysis (FDNA)

3.2.1.1. Overview of FDNA

Functional Dependency Network Analysis (FDNA) is a method "developed to model and measure dependency relationships between suppliers of technologies and providers of services these technologies enable the enterprise to deliver" (Garvey & Pinto, 2009).

Modeling the dependency relations between nodes of a system is important to model and measure the ripple effects of failure or loss of operability of one of the nodes over the other nodes on which it is dependent.

The FDNA employs graph theory to define the dependencies between its nodes (Figure 5).

FDNA can be a used to model the dependencies of a variety of systems, such as "the domains of input-output economics, critical infrastructure risk analysis, and non-stationary, temporal, dependency analysis problems" (Garvey & Pinto, 2009).

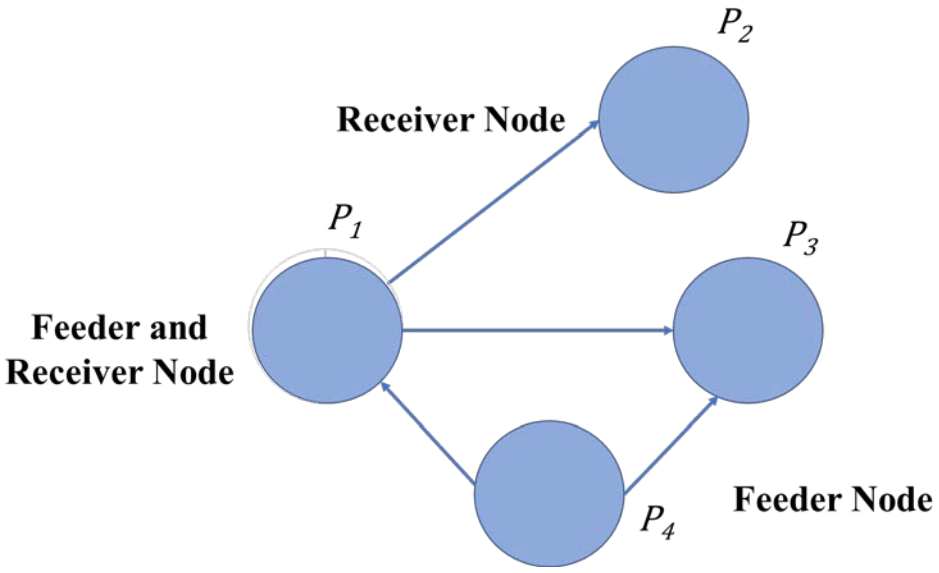


Figure 5. A Sample 4-Node FDNA Graph Topology

The major concepts of FDNA are defined below.

Operational Performance: A measure which is used for stating the realization of a node's output (Garvey & Pinto, 2009).

Operability: "A state where a node is functioning at some level of performance" (Garvey & Pinto, 2009).

Operability Level: "The level of performance achieved by a node" or "the utility it yields" (Garvey & Pinto, 2009).

Baseline Operability Level (BOL): "The operability level of the receiver node when the feeder is completely inoperable" (Garvey & Pinto, 2009).

Feeder Node: A node which contributes to the operability of one or more other nodes (i.e. receiver nodes) (Garvey & Pinto, 2009).

Receiver Node: A node which receives contribution from one or more other nodes (i.e. feeder nodes) to have some level of operability (Garvey & Pinto, 2009).

Strength of Dependency (SOD): "The strength with which a receiver node's operability level relies on the operability level of feeder nodes. SOD captures the effects of relationships that increase the performance as addition to BOL" (Garvey & Pinto, 2009).

Criticality of Dependency (COD): "The criticality of feeder node contributions to a receiver node for it to achieve its operability level objectives. COD governs how the performance of the receiver node will decrease below the BOL in time and possible become inoperable eventually" (Garvey & Pinto, 2009).

The general equation of FDNA algebra for the graph in Figure 6 is given below.

$$P_j = f\left(P_i, \alpha_{ij}, \beta_{ij}\right), 0 \leq P_i, P_j \leq 100\ , 0 < \alpha_{ij} \leq 1\ , 0 \leq \beta_{ij} \leq 100$$

where, P_j is operability level of the receiver node,

P_i is operability level of the feeder node,

α_{ij} is Strength of Dependency (SOD) constraint and ($0 < \alpha_{ij} \leq 1$),

$\beta_{ij}$is Criticality of Dependency (COD) constraint and ($0 \leq \beta_{ij} \leq 100$)

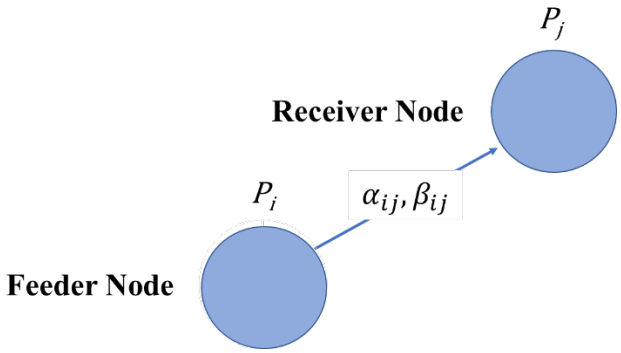


Figure 6. A 2-Node FDNA Graph

FDNA is very instrumental to model the ripple effects of any loss of operability in feeder node(s) to analyze not just operability but also business continuity of an enterprise. As depicted in Figure 7, capability portfolio of an enterprise including internal and external portfolio dependency node(s), and capabilities can be represented by FDNA to calculate the loss of enterprise capability in case of a loss of functionality of any node.

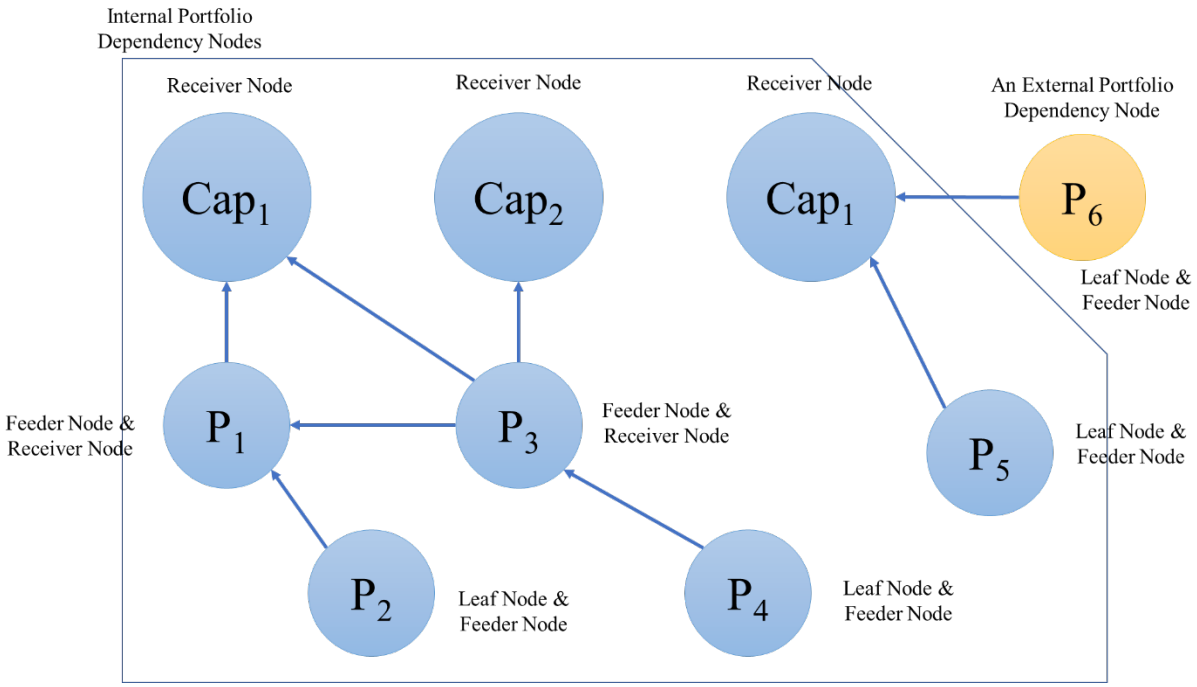


Figure 7. Capability Portfolio Context Representation of FDNA Graph

3.2.1.2. Previous Studies on FDNA

FDNA is used in its first traditional form or after modified for particular settings for various aims. In this section, relevant previous studies are analyzed.

The purpose of a study by Drabble (2011) is to understand the effects of decisions made in one system on dependent systems and make the collaboration meaningful without much effort. The approach presented in the study helps determine the information dependency among the systems. The information mentioned in this study includes people, locations, resources, and concepts from different origins. This helps decision makers within interdependent systems to perceive the possible constraints and restraints that others' decisions provide and also will help determine how compatible their decisions are with the other systems.

The authors propose an ontology based information management capability (OBIMC) to help information sharing collaboration that is not dependent on any constituent system or any user

within these systems. This approach is intended to solve information collaboration issues among systems that don't have an agreed purpose.

On the other hand, this approach differs from FDNA, which focuses on calculating the risk among interdependent systems. OBIMC focuses on the dependencies to provide better link semantics, providing redundancy by alternative feeder and receiver nodes. Another feature of this technique is to provide reasoning over groups of feeder and receiver nodes by making sub-networks. The study shows the process of how OBIMC works with an example in a healthcare network.

Another study by Drabble (2012) aims to solve the collaboration issue within interdependent networks where there is a need to understand which information is essential to be communicated and how to pass this information within the network. The study describes a dependency based network model that makes both qualitative and quantitative information flow channel through the interdependent network of people, organizations, locations, resources, and concepts. This model is required for the emergency response networks where there is a lack of information, and anything can be crucial for understanding the situation.

The approach presented in this study analyzes the network and provides Plan Models that outline the required adjustments within the nodes to deliver the intended outcome from the network. The Plan Models indicate the required changes for the nodes directly, or indirectly through the nodes on which they have a dependency.

The method presented in this study, Athena, analyzes the capabilities, dependencies, and vulnerabilities of the nodes to predict the potential impact of the changes in one node at the others. This study has similarities with FDNA but doesn't focus on calculating the risk of interdependent

systems and the risk mitigation strategies for them. However, it uses some of the terms as same as FDNA, such as SOD, COD, BOLP, MOE, and MOP.

The study applies the model in a counter insurgency example to show the advantages of it.

The aim of this study (Guariniello & DeLaurentis, 2013a) is to assess dependencies in the System of Systems (SoS). Their objectives are assessing the operability, reliability, and resilience of SoS architectures, specifically in two kinds of networks: operational and development. This study adapts the FDNA in order to assess the operability of the operational system based on the strength and criticality of the functional dependencies among the constituent systems and capabilities of SoS. Additionally, this study presents Development Dependency Network Analysis in order to assess how a network of constituent systems and delays within the network affect the capabilities and the time required for development.

One novelty of the study is adding a term to FDNA, degraded functioning, meaning that a component of the system may operate with a degraded level due to its malfunctions that may affect the other nodes of the network.

Additionally, this study presents a test of stochastic analysis with FDNA. The authors conducted an analysis for the operability of the constituent systems of SoS. The analysis includes a probability distribution for the operability of such systems.

The last contribution of the study is the Development Dependency Network Analysis (DDNA). The purpose of this technique is to evaluate how network topology and delays affect the development time and capabilities of the SoS. This technique uses the FDNA concepts and represents them as done in Program Evaluation and Review Technique (PERT) and Critical Path Method (CPM).

Guariniello & DeLaurentis (2013b) studied the effects of dependencies within systems of systems in the space operations and development research activities. They applied the previously modified FDNA and DDNA approaches in their previous study (Guariniello & DeLaurentis, 2013a) into the space systems operations and development.

From the methodological perspective, this study does not add more to FDNA than the previous one. Similarly, it employs FDNA to calculate the dependencies within an operational system of systems by adding the *malfunction* term. For example, it helps to analyze how the Mars mission equipment depends on the orbital communication satellites. For DDNA, it borrows SOD and COD from FDNA and builds a new technique also borrowing concepts from PERT and CPM methods. DDNA is used to analyze developmental dependencies. It helps to plan parallel development of space systems to shorten time to conduct enough research and prototypes for each technology new space systems requires. The study applies these two techniques on hypothetical space missions. The results provide important outcomes that show the dependency analysis in both operation and development. The results show the scalability of the methods and their power to analyze the dependencies within the space infrastructure.

Guariniello & DeLaurentis (2013c) applied the same modified FDNA approach to a new field, servicing for on-orbit satellites. The modified and stochastic FDNA methodology is borrowed from the authors' previous study (Guariniello & DeLaurentis, 2013a). In this study, they model the satellites as a two-level system of systems. The lower level considers the modular satellite systems and analyzes the functional dependencies among the systems within a satellite, such as power supply, communication, navigation, and computing. At the higher level, they analyze the functional interdependencies among different types of satellites, such as communication, observation, experimental, and servicing satellites. They also take the satellite

groups at different orbit levels into consideration. The authors apply the approach to a hypothetical case of satellites and discuss the importance of the analysis of dependencies and how to improve the susceptibility of the satellites. The results compare the satellite life lengths with or without the operation of servicing satellites. They also provide insights into the applicability of the method on similar problems within and outside of space infrastructure field.

The objective of the article by Guariniello and DeLaurentis (2014a) is quantifying the impact of cyber attacks targeting communications and information flows on the operability of the component systems. The authors also "aim to evaluate and compare different architectures with respect to their reliability and robustness under attack" (Guariniello & DeLaurentis, 2014a). The whole impact is much more than the impact on a single attacked component of communication and information systems. For a holistic impact assessment, ripple effects on the behavior of whole system-of-systems caused by interdependencies should be considered. In the original FDNA, SOD and COD values can be identified through expert judgment and evaluation or may come from the result of simulations and experiments. The analysis can be a deterministic evaluation of a single instance of the SoS (i.e., internal health status or Self-Effectiveness), or a stochastic quantification of the overall SoS behavior. The authors apply the modified FDNA methodology they developed (Guariniello & DeLaurentis, 2013a) and applied to other fields (Guariniello & DeLaurentis, 2013b; 2013c) in their previous studies. Guariniello and DeLaurentis propose a modification to Functional Dependency Network Analysis (FDNA) tool to analyze operability of the communication architectures when they are exposed to cyber-attacks, from a system of systems view. In the modified version of FDNA, internal (primary and secondary) and external (tertiary) effects are taken into account because of the nature of the impact of cyber attacks. Internal effects are already modeled by Self-Effectiveness. Guariniello and DeLaurentis add weight on each dependency link,

called Availability of Data (AOD), to model the effect of specific communication and data loss on a single interdependency as well as to represent partially compromised communication and data. The results also show that the architecture of the systems can be modified to improve its resilience to cyber attacks.

The purpose of this study by Guariniello and DeLaurentis (2014b) is to assess the effects of interdependencies among a system of systems on the metrics that show the properties of SoS, which are known as *ilities*. The authors apply the modified FDNA methodology they developed (Guariniello & DeLaurentis, 2013a) in their previous study. They provide a hypothetical case to apply and discuss the validity of their approach. They applied the methods to a marine combat SoS that includes ships, helicopters, Unmanned Aerial Vehicles, Unmanned Surface Vehicles, mines, and submarines. The results show that a trade-off among *ilities* exists. The decision makers can adjust the resilience, reliability, and flexibility of the SoS according to the mission's requirements, resources, and objectives. The results are preliminary and need to be improved by further studies, especially cost analysis.

The purpose of the study by Wang, Zhang, and Li (2014) is to analyze the security of Global Navigation Satellite Systems (GNSS). The authors employ FDNA to solve this issue by calculating the impact of threats to the service performance. The results imply that the FDNA provides stable results and it is convergent. The increasing amount of iterations starts to does not change the results significantly after a number of iteration achieved. According to the results, the success rate of the current GNSS is almost 5%, which means that it is highly probable that it will fail against the threats. Based on the authors' results, FDNA is an appropriate and beneficial tool to fulfill the purpose of the study.

The purpose of this study (Cole, 2017) is to evaluate the impacts of messy data in System of Systems (SoS). In other words, how does data quality in one constituent system affect the dependent systems within a SoS? The authors present and implement a new quantitative approach called Data Dependency Network Analysis (DDNA) to assess the effects of data in SoS and provide mitigation strategies. DDNA adapts the Functional Dependency Network Analysis (FDNA) by adding new parameters including Output Data Quality Level, Incoming Data Cleansing Effectiveness, Data Governance Effectiveness, Operability Strength, Strength of Data Dependency, and Contextual Alignment Factor. The authors present an Agent-Based Model using NetLogo. During each iteration of the simulation, receiver nodes' states are updated based on the state of data providers, node's parameters and system self effectiveness parameters. DDNA can be used for three purposes:

Identification of Bad Actors: Identifying the nodes affecting the SoS negatively.

Improvement of Data Cleansing: Identifying the data degradation mitigation strategies.

Improvement of Data Governance: Finding the optimum strategy to minimize data degradation.

Servi and Garvey (2017) aim to develop new methods based on FDNA to answer the following questions to achieve resiliency of the enterprise system.

"What is the effect on the ability of an enterprise to operate if one or more elements or element dependency chains degrade, fail, or are eliminated due to exploited vulnerabilities?

How much operational degradation occurs, where does it ripple across its elements, and does it breach minimum levels of performance?

Which nodes or elements are most critical to achieving performance objectives?" (Servi & Garvey, 2017).

The purpose of the study by Short, Lai, and Bossuyt (2018) is to model how to disable non-critical subcomponents of a system when the system fails in order to avoid the failure of the critical subcomponents. The authors propose a methodology, failure flow decision function (FFDF) methodology, to achieve this. It helps to model the failure flow so that it would be possible to direct the failure to the non-critical subsystems instead of critical ones. The paper provides a case study of the proposed FFDF methodology on a Mars exploration platform.

The importance of this methodology increases when the system at hand is not in a serviceable location or situation due to certain reasons, such as high cost and lack of resources. The methodology helps decision makers best before the architectural design of the system to be produced.

FFDF has differences from FDNA. FDNA is a unidirectional functional dependency analysis method that depends on the input-output relationship. SODA (Guariniello & DeLaurentis, 2017) is a tool that is a modified version of FDNA for stochastic operational functional dependency analysis. FFDF, unlike FDNA and SODA, can analyze backward failure flow since it is not unidirectional. However, a disadvantage of FFDF is that its analyses are based on binary failure, meaning that there is no degraded operational state for the nodes while FDNA and SODA have this option. On the other hand, the lack of this option is not an issue of FFDF according to the authors, since it is not intended to analyze systems that are repairable due to their location or situation.

According to the results of the case study in this article, FFDF is beneficial and helps improve the survival of the test equipment by directing the failure to a non-critical subcomponent instead of a critical one. FFDF helps system designers during the conceptual phase of design.

Garvey discussed how FDNA could be used to answer questions similar to the ones below (Garvey, 2018).

"What is the effect on the ability of a system of system to operate effectively if one or more entities or feeder-receiver chains degrade, fail, or are eliminated due to adverse events or situations?

How much operational degradation occurs, and does it breach the system of system's minimum acceptable level of performance?" (Garvey, 2018).

In the FDNA context, resilience is defined as "the ability of a system to absorb the effects of nodal degradation while maintaining an acceptable level of operational effectiveness" (Garvey, 2018). The article asserts that FDNA is a useful tool to model and measure the resilience of a system being engineered to interoperate with other interacting systems and elements (Garvey, 2018). Garvey offers to use FDNA for a resilient system design or measuring the resilience of a system to system failures or exploitations. Measurement of resilience enables decision makers and planners to determine optimal investment levels to maintain a system of systems operational effectiveness.

Pinto, Garvey, and Santos proposed research to apply FDNA on the cyber layer of an enterprise to address resiliency of the system (Pinto, Garvey, & Santos, n.d.). The cyber layer of an enterprise system is getting more important since most of the functions rely on the cyber layer. Both malicious and non-malicious failures of the cyber layer cause a failure to deliver those functionalities. Pinto, Garvey, and Santos list the following steps to apply FDNA to the cyber layer of any enterprise system.

"*Develop a functional dependency model of an enterprise of concern*

Identify the functions that are delivered by/through the cyber subsystem

Highlight these functions as the cyber layer of the enterprise

Perform FDNA on this cyber layer, particularly highlighting the resilience (and its proxy measures)

Applying FDNA in the cyber layer of an enterprise system is valuable since system engineers, managers, and administrators may be able to answer the following questions.

What functions does the cyber layer provide, whether by design or by emergence?

How to decompose a cyber layer into functional performance objectives?

How to establish measures of performance (MOP) for these functional objectives?

How to translate various and disparate MOP's unto comparable and algebraically manageable measures of effectiveness (MOE).

How to describe robustness and rapidity of the cyber layer and each of its subcomponents?

How to establish recovery objectives for the cyber layer and each of its subcomponents?

How to describe resilience of the cyber layer and each of its sub-components?"

Garrido-Pelaz, González-Manzano, and Pastrana (2016) aim to develop a model for cybersecurity information sharing among dependent organizations being impacted by different cyber attacks (Garrido-Pelaz, González-Manzano, & Pastrana, 2016). The model has two stages: propagation of cyber-attacks and information sharing. The authors used FDNA to simulate propagation of cyber-attacks and game theory to make decisions on information sharing. The developed model uses several variables to decide on cyber attack information sharing.

Costa, McShane, and Pinto (2015) aim to apply FDNA on interbank lending to build a model to answer the following questions.

"What causes a problem in one sector of the economy to spread through the rest of it?

What are the channels for financial contagion?

Suppose a bank becomes insolvent and fails. What is the effect on other banks in the system?

How can we measure the spread of risk in a system as interconnected as the banking sector?" Costa, McShane, and Pinto (2015)

Costa, McShane, and Pinto first make a literature review to find out the methods to study financial contagion (Costa, McShane, & Pinto, 2015). The authors employ a system-of-systems approach and a method of network analysis. FDNA is modified to simulate the impact of the collapse of a bank on other financial institutions. In the developed model, the FDNA concepts of baseline operability level and strength of dependency apply themselves well to a financial contagion model. However, there is difficulty in applying the concept of criticality of dependency on this model. This particular aspect of FDNA does not describe this interbank lending system well (Costa et al., 2015).

The goal of Guariniello and DeLaurentis is to develop a framework to support decision in systems design and architecture. The article introduces the system operational dependency analysis (SODA) methodology. SODA is a useful tool to support design decision making (Guariniello & DeLaurentis, 2017). Guariniello & DeLaurentis (2017) propose a parametric model of the behavior of the system. SODA method can be used for various aims. SODA supports:

SODA is based on Leontief-based Input/Output method originally proposed by Haimes, and the FDNA method. One of its innovations is adding Impact of Dependency (IOD) as a third parameter alongside SOD and COD. IOD "ranges between 1 and 100 and is defined as 100 divided by the slope of the COD dependent" (Guariniello & DeLaurentis, 2017). IOD enables SODA to model dependencies better than FDNA, particularly the dependencies that exhibit an input/output behavior similar to a step function (Guariniello & DeLaurentis, 2017). The authors also provide

approaches to use SODA in a deterministic or a probabilistic manner. They modify FDNA to support a resilient system design or measure the resilience of a system to system failures or exploitations. Measurement of resilience enables decision makers and planners to determine optimal investment levels to maintain a system of systems operational effectiveness.

In their study, DeLaurentis et al.(2012) compares existing system of systems analysis methods. They modified FDNA to analyze the SoS deterministically and stochastically. They added a self-effectiveness term for each node as different from the original FDNA that gives self-effectiveness (operability/measure of effectiveness) values only to the feeder nodes. This value indicates the nodes' own performance regardless of any dependency on the other nodes.

They analyze a sample five-node SoS network deterministically. Firstly, they give reduced self-effectiveness values to each node while keeping the rest of the nodes' self-effectiveness at 100 and analyze the operability values of the other nodes. Then they give the reduced values to pairs of nodes and further investigate the effects. They also conducted the same analysis on a more complex network and compared deterministic results for different cases, such as node or link removal, and different architecture.

DeLaurentis et al. (2012) also analyzed the same five-node network stochastically by conducting a Monte Carlo simulation. The simulation gives all the possible initial values to each node and computes the operability values. At the end, it comes up with a probability density function for each node's operability value. The study lacks detailed explanation of this process and results. By this demonstration, they show that FDNA is useful to analyze the critical nodes of a SoS network and assess resiliency of each node.

Another approach developed by DeLaurentis et al. (2012) is the Development Dependency Network Analysis (DDNA). This method borrows concepts from FDNA, Critical Path Method

(CPM), and Program Evaluation and Review Technique (PERT). The purpose of this method is to find the most critical events of a network (series) of systems to be developed in time where some of the systems could be started developing before or after the preceding systems are developed. It is a more realistic way of assessing the development time based on the dependencies between the system than PERT and CPM.

3.2.1.3. Modifications to FDNA

There are several aspects that can be used when identifying the characteristics of dependencies within a layer and among layers. These are explained below.

Confidentiality, Integrity and Availability Aspects: Value and impact of dependencies can be defined as a vector of confidentiality, integrity and availability values. Some attacks just target one or a few of these properties of information. Most of the valuation is based on availability value. However, for some missions, confidentiality is also vital. So, to assess the impact more accurately and simulate the propagation in horizontal and vertical layers, these three properties of the information could be used for valuation.

Self-Efficiency: FDNA assumes that the loss of operability of a node is possible only at least one of its feeder nodes' operability level degrades. However, there are also cases in which a node might fail even if all of its feeder nodes are at full operability level. Therefore, a new parameter will be introduced to FDNA algebra to cover this kind of situations..

Nature of Dependencies: The dependency relation types of traditional FDNA are not sufficient to address the dependencies in cyberspace. For instance, the traditional FDNA is shortcoming in two cases which are pretty common in cyber system architectures: (i) Functionality of one node is dependent on the operability of more than one node simultaneously, and (ii)

Functionality of one node is dependent on the operability of any of more than one nodes. New dependency operators will be introduced to tackle these issues.

Time-Dependency in Mission Modeling: Time is an important factor to calculate the impact of a cyber action on business processes or missions. The impact varies according to the state of the business process.

From a mission monitoring viewpoint at each particular time, a mission step could be in one of the three different states: (a) it could be already completed, (b) it could be in progress, or (c) it could be in a state of a planned execution. The overall state of the mission depends on the states of the mission tasks: the mission is in a planned state when none of its tasks have been started, the mission is an execution state if at least one of its task is an execution state, and finally, completion of all mission tasks brings the whole mission into the completed state (Jakobson, 2011).

For example, assume that, for Old Dominion University, asset layer includes network equipment, cables and computers etc. Service layer includes email service, identity management service, internet connection service etc. Mission layer includes delivering online courses. If an asset (i.e. router) is degraded because of a cyber attack, then internet connection service fails along with some others. This might also cause degradation of the mission, degradation of online courses. However, if this cyber incident occurs during a holiday, a time period in which no online courses are delivered, it has no impact on the mission. Therefore, time is an important factor that should be considered while defining the dependencies.

3.2.2 Economics of Cybersecurity and Risk

Economics of information security and cybersecurity investment have been studied for a long time. However, in recent years, the number of publications has been increasing due to

escalating expenditures and loss from security breach apart from the technical problems. Scholars suggest different methods to help decision-makers decide how to invest in cybersecurity to protect operational excellence and intellectual property. Specific prominent studies to increase the efficiency in cybersecurity risk management are reviewed below. Parts of this section have been previously published in (Keskin, Tatar, Poyraz, Pinto, & Gheorghe, 2018).

One relevant study was presented by CAPT Erickson (2016), a cybersecurity figure of merit. Erickson states that "The Navy is unable to measure and express cyber program of record wholeness, platform cyber readiness, and the impact of programmatic and budgetary decisions on cyber readiness, or to quantify the value of specific cybersecurity standards or controls. Without an accepted means of holistically scoring risk within a system of systems construct, the Navy cannot consistently shape cybersecurity investment priorities to optimize value in a resource constrained environment." The main research problem of Erickson is "how to optimize complex cybersecurity investment combinations to provide the maximum value in terms of operational risk reduction in resource-constrained environments." Morse and Drake (2012) developed a methodology to cope with acquisition risk. In order to have more realistic and objective risk assessment, they proposed a methodology to quantify acquisition risks through data-driven monetization. Cybersecurity is not within the scope of their study, but the core is calculating risk in monetary values as in this research.

Shultz and Wydler (2015) studied the integration of cybersecurity into acquisition life-cycle, a shift from bolt-on security to built-in security. Shultz and Wydler described how the government is moving from compliance-based requirements to a risk-based cybersecurity management framework to integrate cybersecurity into program acquisition and execution support. Kaestner, Arndt, and Dillon-Merrill (2016) focused on embedding cybersecurity during the

acquisition process to reduce the product life-cycle costs because of the reduced need to fix vulnerabilities in the systems later. To attain this goal, the acquisition community must be aware of cyber threats and have an understanding of risk assessment. In the recommendations section of their article, Kaestner et al. (2016) state that "Risk management experts agree that the first step to take is to assess the financial risk of a security breach. This requires a detailed inventory of the organization's assets at risk that will be used to assess the financial risk." The recommendation of Kaestner et al. (2016) is the goal of this study.

There have been studies to compare different methods to determine the optimal amount to invest in cybersecurity. There are comparisons of the economics of cybersecurity, such as game theory, optimization theory, use of real data, and security controls selection. Cavusoglu et al. (2008) and Fielder et al. (2016) utilized game theory and optimization to compare the two for benchmarking efficiency of cybersecurity investments.

Economics of cybersecurity studies employs optimization methods to address several types of problems. For example, an earlier work (Gordon and Loeb 2002) utilized optimization to calculate the optimal amount to invest in cybersecurity, and it showed that a small fractional amount of the expected loss would be enough to invest in cybersecurity.

Arora et al. (2004) suggest taking a risk management approach to evaluate information security solutions. They indicate that security managers should consider risk-based Return on Investment method to decide how to invest in cybersecurity due to so many uncertainties in the cyber domain.

Research on the topics of the economics of cyber risk and cyber insurance –the primary method of risk transference– has grown exponentially since 2010. This highlights the increasing relevance of the topic, from both a practical and an academic perspective (Eling & Schnell, 2016).

Sheldon, Abercrombie and Mili (2009) developed the Cyberspace Security Econometrics System (CSES). The CSES provides “a measure (i.e., a quantitative indication) of reliability, performance and/or safety of a system that accounts for the criticality of each requirement as a function of one or more stakeholders’ interests in that requirement. For a given stakeholder, CSES accounts for the variance that may exist among the stakes one attaches to meeting each requirement”. The stakeholders, with assistance from subject matter experts, define the criteria of a quantitative value of an asset. Financial basis (e.g. cost of operational downtime, hardware and software costs etc.), standards and regulations such as FISMA, NIST 800-60 and/or FIPS 199/200, and stakeholder defined requirements are the quantitative valuation criteria used in the CSES method (Abercrombire, Sheldon, & Grimaila, 2010).

Current methods commonly put more emphasis on technology and less on people, process and socio-economic risk factors (Spears, 2005; Tatar, Bahsi and Gheorghe, 2016). Major risk assessment approaches, such as ISO/IEC 27001 and 27002 standards, are designed based on security control domains and focus more on an asset’s security posture while ignoring its preparedness towards a set of high-risk loss scenarios (Ruan, 2017). One of the major problems of actuaries working in the insurance sector or enterprise risk management is the quantification of cyber risk. Almost all the security companies keep incident and loss data as proprietary to have a competitive advantage (Ruan, 2017). Subsequently, there is not enough data to employ statistical methods and mathematical models for appropriate calculations and predictions. This scarcity of data leads analysts to rely on scenario approaches rather than the use of the classical stochastic modeling (Lloyd’s, 2015). For Rakes, Deane, and Rees (2012) employing expert judgment to define worst-case scenarios and estimate their likelihood for high-impact IT security breaches is a

more efficient approach. Even more so, fast-changing technology environment requires a modeling approach, which dynamically measures risk (Eling & Schnell, 2016).

3.3 Generalizability and Validity of the Research

3.3.1 Generalizability of Research

Generalizability (also referred as external validity) of a research defines the effectiveness and usefulness of the research. According to (Polit & Beck, 2010), generalizability is “an act of reasoning that involves drawing broad inferences from particular observations”.

In system engineering research, behavior of the systems is dependent on the system’s context. It is always possible to apply the findings of a research to another system context. Therefore, attaining generalizability of the research in systems engineering field is difficult. Valerdi and Davidz suggested utilizing adequate sampling, random sampling, replicating the results in various settings with different methods and using field research to mitigate the generalizability problem (Valerdi & Davidz, 2009).

There are several types of external validity: a) population, b) setting, c) task/stimulus, and d) temporal/social. Population component of external validity deals with “Will the results generalize to other persons or animals?” Setting component of external validity deals with “Will the findings apply to other settings, situations or locations?” Task Stimuli component of external validity deals with “Will the results generalize to other tasks or stimuli?” Societal/temporal component of external validity deals with “Will the findings continue to apply as society changes over the years?” (Garbin, n.d.). According to Firestone, there are three forms of external validity: (1) Statistical generalization, (2) Analytic generalization, (3) Case-to-case transfer of findings (Firestone, 1993). Statistical generalization is extrapolation of findings from a sample to a population. For attaining Statistical generalizability, the sample should be representative of the

population (i.e. random sampling). Analytic generalization is constructing a theory or concept from certain findings of the research. Transferability is concerned with the extent to which the findings of one study can be applied to other situations. Case-to-case transfer of findings, transferability, is applying findings of a research to a similar situation by the readers or users of the research. Since the readers of the research transfer the findings of a research to another situation by comparing the specifics of the research environment and specifics of the other situation, the researcher should provide detailed descriptions of the research environment (Polit and Beck, 2010).

This research aims to develop an approach to calculate the impact of cyber action by considering ripple effects and propagation. First, scarcity of available data is an issue for this study. To achieve generalizability, "selecting" the sample data to represent the greater population is not possible. Data in the previously published documents will be used. Since the goal of this study is to develop an approach, the analytic generalization is more proper for the generalizability of the research findings.

3.3.2 Validity of Research

Validity of modeling and simulation based research consists of conceptual model validation, computerized model verification, operational validation, and data validity (Sargent, 2015). *Conceptual model validation* is defined as "determining that the theories and assumptions underlying the conceptual model are correct and that the model representation of the problem entity is "reasonable" for the intended purpose of the model" (Sargent, 2009). *Computerized model verification* is defined as "assuring that the computer programming and implementation of the conceptual model is correct" (Sargent, 2009). *Operational validation* is defined as "determining that the model's output behavior has sufficient accuracy for the model's intended purpose over the

domain of the model's intended applicability" (Sargent, 2009). *Data validation* is defined as "ensuring that the data necessary for model building, model evaluation and testing, and conducting the model experiments to solve the problem are adequate and correct" Sargent, 2009).

Validation during model development is an iterative process. Sargent defines this iterative process as depicted in Figure 8. Sargent states that conceptual model validation, computerized model verification, operational validation and data validation are the required steps of the iterative validation process (Sargent, 2015).

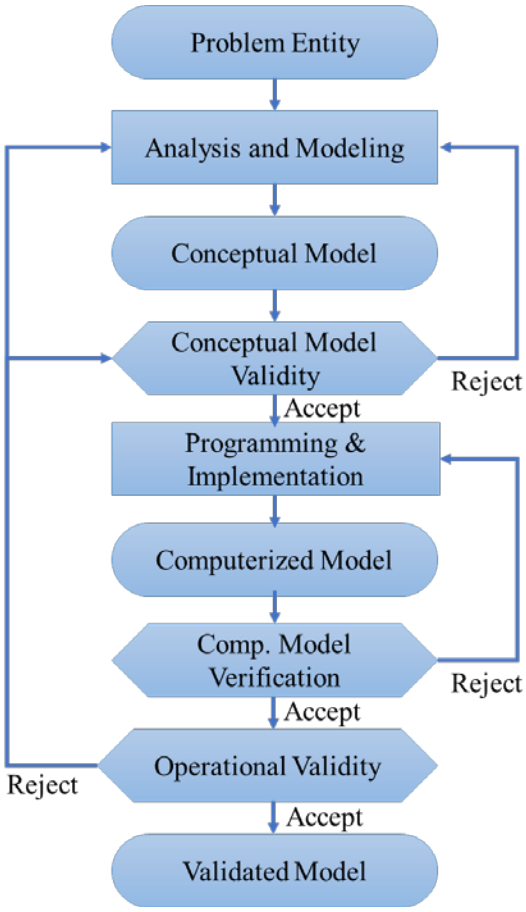


Figure 8. Iterative validation process (Sargent, 2015)

There are several validation techniques and tests to validate and verify the model. Sensitivity analysis will be used as the primary validation technique.

Sensitivity analysis (parameter validity) is changing the values of parameters; the effect on the output parameters should be checked for representation of the reality (Landry et al., 1983; Law, 2006; Sargent, 2013). The outputs and the structure can be compared with other models as well (Landry et al., 1983).

CHAPTER 4

MODEL DEVELOPMENT

4.1 Introduction

This study aims to modify FDNA to develop FDNA-Cyber, which is a new quantitative method to (1) determine the cyber impact propagation within a layer (i.e., Asset layer, Service layer or Business Process layer), (2) determine the impact propagation among different layers within an enterprise, and (3) estimate the economic cost of a cyber incident or event. .

In this chapter, firstly, complex features of FDNA (i.e., constitutional nodes) ,which are mandatory to develop FDNA-Cyber, are explained. Then, modifications to FDNA, such as integration of *Confidentiality*, *Integrity*, and *Availability* concepts, *Self Efficiency* of nodes, and new dependency relations (AND and OR dependencies) are explained. Finally, for the calculation of economic cost, cost factors and impact of time on economic consequences are explained.

4.2 Multiple Component FDNA Nodes

FDNA is a useful graph theory method to address the following questions.

> *"How risk-dependent are capabilities so threats to them can be discovered before contributing programs (e.g., suppliers) degrade, fail, or are eliminated?*
>
> *and*
>
> *What is the effect on the operability of capability if, due to the realization of risks, one or more contributing programs or supplier-provider chains degrade, fail, or are eliminated."* (Garvey, 2009)

The major formulas of FDNA are explained in Chapter 3. According to Garvey's original definition (Garvey, 2009), the fundamental equation of FDNA for the operability level of node P_y that is dependent on the operability levels of h other nodes $P_1, P_2, P_3, \ldots, P_h$ is given by

$$0 \leq P_y = Min\left(SODP_y, CODP_y\right) \leq 100$$

$$SODP_y = Average\left(SODP_{y1}, SODP_{y2}, SODP_{y3}, \dots, SODP_{yh}\right)$$

$$SODP_{yl} = \alpha_{ly} P_l + 100\left(1 - \alpha_{ly}\right), 0 \leq P_l, P_y \leq 100, 0 < \alpha_{ly} \leq 1, l = 1,2,3, \dots, h$$

$$CODP_y = Min\left(CODP_{y1}, CODP_{y2}, CODP_{y3}, \dots CODP_{yh}\right)$$

$$CODP_{yl} = P_l + \beta_{ly}, 0 \leq \beta_{ly} \leq 100\ (1 - \alpha_{ly})$$

where

$SODP_y$: Strength of Dependency (SOD) equation of P_y on feeder nodes $P_1, P_2, P_3, \dots, P_h$

$CODP_y$: Criticality of Dependency (COD) equation of P_y on feeder nodes $P_1, P_2, P_3, \dots, P_h$

α_{ly}: Strength of dependency fraction of P_y on feeder nodes P_l

β_{ly}: The operability level that a receiver node decreases to without its feeder node contribution

Hitherto, FDNA analytics include single component node cases. However, FDNA is also a convenient tool where a node is composed of multiple components. Garvey & Pinto (2009) describes *single component* node as the "one that is defined by one and only one component." A multi component node, which is called *constituent node*, is a special "a node characterized by two or more components." It is always possible to split up a constituent node into at least two distinct components. For example, a computer which is composed of memory, storage, processing unit, input unit, and output unit– a total of five components – is an example of a constituent node. The graphical representation of a constituent node – the computer example – is given in Figure 9.

A constituent node can be a feeder or receiver node. There are several possible dependency relations in which a constituent node can take place. The possible dependency relations of a constituent node or its components are (a) dependency of a constituent node with a single node,

(b) dependency of a constituent node with another constituent node, (c) dependency of a component of a constituent node with another component in another constituent node, (d) dependency of a component of a constituent node with a component in the same constituent node, (e) dependency of a component of a constituent node with another constituent node (as a whole), and (f) dependency of a component of a constituent node with a single node (as a whole) (Figure 9).

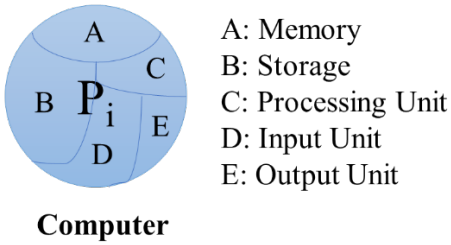
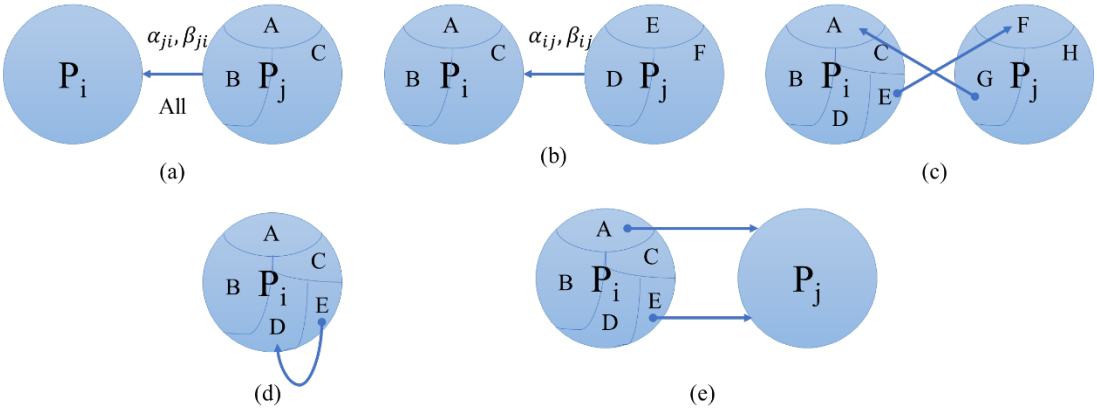


Figure 9. Representation of a constituent node (Garvey & Pinto, 2012)

Operability level of a constituent node is different from a single node's, which can be represented by a single dimensional value function (SDVF). The operability level of constituent node is a function of operability levels of its components. As for the single node, operability level of each component of a constituent node is represented by its own SDVF. A classical form of Keeney-Raiffa additive value function is used to calculate the overall operability of a constituent node (Keeney & Raiffa, 1976). That means, "the overall operability function of the constituent node is a linear additive sum of the component SDVFs" (Garvey, 2009).

Operability level of a constituent node is different from a single node's, which can be represented by a single dimensional value function (SDVF). The operability level of the constituent node is a function of operability levels of its components. As for the single node,

operability level of each component of a constituent node is represented by its own SDVF. A classical form of Keeney-Raiffa additive value function is used to calculate the overall operability of a constituent node (Keeney & Raiffa, 1976). That means, "the overall operability function of the constituent node is a linear additive sum of the component SDVFs" (Garvey, 2009).



(a) Single node: Constituent node dependency
(b) Constituent node: Constituent node dependency
(c) Constituent node component: Another constituent node component dependency
(d) Constituent node component: Constituent node's another component dependency
(e) Constituent node component: Single node dependency

Figure 10. Dependency Relations of Constituent Nodes and Single Nodes (Garvey & Pinto, 2012)

For the computer example in Figure 10, operability functions of A, B, C, D, and E are represented by SDVFs $V_A(x_A), V_B(x_B), V_C(x_C), V_D(x_D), and\ V_E(x_E)$. The operability of function of P_i is as follows.

$$P_i = w_A V_A(x_A) + w_B V_B(x_B) + w_C V_C(x_C) + w_D V_D(x_D) + w_E V_E(x_E)$$

where

$$w_A + w_b + w_C + w_D + w_E = 1\ and\ 0 \leq P_i, V_A(x_A), V_B(x_B), V_C(x_C), V_D(x_D), V_E(x_E) \leq 100$$

A general representation of the operability function of a constituent node P_y with k components is

$$P_y = \sum_{i=1}^{k} w_i V_{A_i}(x_i)$$

where

$$w_1 + w_2 + w_3 + \cdots + w_k = 1 \; and \; 0 \leq P_i, V_{A_i}(x_i), \leq 100$$

4.3 Applicability of FDNA Concepts into Cybersecurity

FDNA is developed to "enable management to study and anticipate the ripple effects of losses in supplier-program contributions on dependent capabilities before risks that threaten these suppliers are realized" (Garvey, 2009). FDNA is not developed for a specific application domain such as cyber, transportation or electricity; however, it can be applied to model functional dependency of any domain. A practitioner who wants to apply FDNA to a domain such as cyber security, needs to translate the concepts of FDNA into the concepts of the application domain. In this section of the study, major concepts of FDNA will be explained from a cybersecurity point of view.

Strength of Dependency (SOD) and *Criticality of Dependency* (COD) are the fundamental concepts of FDNA. Garvey (2009) defines SOD as "the operability level a receiver node relies on receiving from a feeder node for the receiver node to continually increase its baseline operability level and ensure the receiver node is wholly operable when its feeder node is wholly operable." From its definition, applicability of SOD into cybersecurity is straightforward. For example, assume that there are a PC and a router, components of an IT system that has many other components. The PC is used for web browsing. The router is a networking device that forwards data packets between computer networks. In this case, the router is a vital component for the PC's internet connection. If the router's bandwidth decreases (i.e., the operability level of the router) because of a system failure or a cyber-attack (i.e., distributed denial of service attack), this causes

a decrease in the quality of the PC's Internet connection (i.e. operability level of PC). In this example, if the feeder node's operability level (i.e., the bandwidth of the router) becomes zero, then the operability of the receiver node (i.e., the Internet connection of PC) also becomes zero (i.e., baseline operability level).

Garvey (2009) defines COD as "the operability level a receiver node degrades to from its baseline operability level without receiving its feeder node's contribution." The presence of a SOD between a receiver and a feeder node does not imply a COD exists between them. A COD is present between a receiver node and a feeder node only when the receiver degrades from its baseline operability level without receiving it feeder node's contribution. COD does not exist in all dependency relations between receiver nodes and feeder nodes in cybersecurity. However, there are some cases for which the COD concept is useful to explain the functional dependency between a receiver node and a feeder node. For instance, Domain Name System (DNS) is good example to explain the COD concept in cybersecurity domain. The DNS is a service which maps domain names such as www.google.com to the IP address(es) of corresponding machine(s) (Shaikh, Tewari, & Agrawal, 2001). DNS is a kind of phone book for the Internet, a phone book that keeps the domain names and corresponding IP, addresses instead of persons' names and their phone numbers. There is a hierarchy in the DNS. Each IT asset uses its assigned DNS server to resolve the IP address of the system, which it wants to connect. If its own DNS server does not know the IP address, the DNS server asks another DNS server, which is at an upper level in the hierarchy. Once it resolves the IP address of the destination, then it gives this information to the IT asset, which requested first. The DNS server at the bottom level keeps this record for a certain period to respond quickly if there is another IP resolution request for the same address.

DNS servers have an associated time-to-live (TTL) field for each record to limit how long the record can be cached by other name servers in the system. TTL values are, typically, on the order of days (Barr, 1996). A small TTL value reduces the propagation time through the hierarchical DNS servers (i.e., better to have updated records) but increases the load on the name server. COD can be used to model the impact of TTL value on the operability level of a DNS server. For example, a PC wants to connect a server, www.google.com. First, it queries the IP address of www.google.com to its assigned DNS server. If the DNS server has this record in its cache, it does not ask any other DNS server and replies to PC with IP information in its cache. If the connection of the assigned DNS server with other DNS servers at upper levels of hierarchy is lost, it can still reply to IP resolution queries from its cache. However, after a period of TTL value, the record will be removed from the cache of the DNS server. After that, DNS server cannot reply to any IP resolution requests from its clients if it does not have connection to another DNS server. This case can be translated into FDNA concepts as follows. The PC which queries the IP address of www.google.com is a receiver node. The PC's associated DNS server (let's call it DNS-A) is its feeder node to the PC. The other DNS server at the upper level of the hierarchy (let's call it DNS -B) is the feeder node for DNS-A. If DNS –A loses its connection DNS-B, DNS-A is still operational for the records it has in its cache. This level is the baseline operability level of DNS-A. However, after a period of TTL, operability level of DNS-A will be degraded from its baseline operability level. This level is called COD for the dependency of DNS-A to DNS-B.

4.4 Modifications to FDNA to Develop FDNA-Cyber

This study introduces FDNA-Cyber, a new method based on FDNA to respond to the limitations of FDNA in cybersecurity risk analysis. This section explains the rationale behind the modifications and new FDNA-Cyber algebra. There are three major modifications to traditional

FDNA: (a) *Self-Efficiency* of nodes, (b) Integrating *Confidentiality, Integrity* and *Availability* values to nodes, (c) New dependency relations (AND and OR dependencies).

4.5.1. Self-Efficiency of Nodes

FDNA is instrumental in modeling the ripple effects between functionally dependent nodes. FDNA assumes that the loss of operability of a node is possible only at least one of its feeder nodes' operability level degrades. Although this condition holds in cyberspace, there are other possibilities, which might cause degradation of operability of a receiver node while all of its feeder nodes are fully operational. For example, for the PC and router example in Section 4.3, the PC might fail because of a system error or a cyber-attack even though the router is fully operational. The operability level of the PC might degrade because of the failure. Therefore, a new parameter should be introduced to FDNA algebra to cover this kind of situation.

A new parameter, *Self-Efficiency,* is developed to enhance FDNA for covering situations in which the receiver node's operability degrades while all of the feeder nodes are fully operational. *Self-Efficiency* of a node is a multiplier to its operability level based on SOD and COD dependencies with its feeders. The new FDNA equations for a 2-node graph (Figure 12) are given below. This self-efficiency formula is different than the *self effectiveness* formula developed by (Guariniello & DeLaurentis, 2014a).

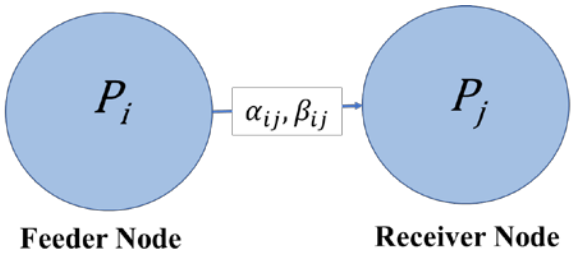


Figure 11. A 2-Node FDNA Graph

$$P_j = SE_j\ (Min(SODP_j, CODP_j)) = SE_j(Min(\alpha_{ij}P_i + 100(1-\alpha_{ij}), P_I + \beta_{ij}))$$

where SE_j is self-efficiency of P_j and $0 \leq SE \leq 1$

α_{ij} is the strength of dependency fraction between P_i and P_j and $0 \leq \alpha_{ij} \leq 1$

β_{ij} is the criticality of dependency between P_i and P_j and $0 \leq \beta_{ij} \leq 100(1-\alpha_{ij})$

$$0 \leq P_i, P_j \leq 100$$

4.5.2. Integrating *Confidentiality, Integrity* and *Availability*

Like many others, NIST standards require valuation of assets in terms of their *Confidentiality, Integrity* and *Availability* values. This three dimensional valuation enables differentiating each type of attack and its respective impact. In FDNA-Cyber model, value and impact of dependencies is defined as a vector of confidentiality, integrity and availability values.

Each node (i.e., an asset, service or business process) of FDNA-Cyber graph has its own *Confidentiality, Integrity* and *Availability* values. Constitutional node representation of FDNA is instrumental to defining FDNA-Cyber nodes (Figure 12).

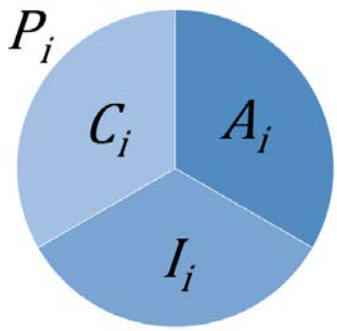


Figure 12. An FDNA-Cyber node

Similar to the classical form of the Keeney-Raiffa additive value function which is used to calculate the overall operability of a constituent node (Keeney & Raiffa, 1976), operability level of a FDNA-Cyber node is a function of operability levels of its components – *Confidentiality, Integrity* and *Availability* values. That means the overall operability function of a FDNA-Cyber node is a linear additive sum of the single dimensional value functions of *Confidentiality, Integrity* and *Availability*.

For the example in Figure 12, operability functions of C_i, I_i, and A_i are represented by SDVFs $V_{C_i}(x_{C_i}), V_{I_i}(x_{I_i}),\ and\ V_{A_i}(x_{A_i})$. The operability function of P_i is as follows.

$$P_i = w_{Ci}V_{Ci} + w_{Ii}V_{Ii} + w_{Ai}V_{Ai}$$

where

$$w_{Ci} + w_{Ii} + w_{Ai} = 1$$

$$V_{Ci} = V_{Ci}(X_{Ci}), V_{Ii} = V_{Ii}(X_{Ii}), V_{Ai} = V_{Ai}(X_{Ai})$$

$$0 \leq V_{Ci}, V_{Ii}, V_{Ai} \leq 100$$

To define the FDNA-Cyber algebra, several FDNA-Cyber dependency equations are developed based on examples.

Example 1: Formulate the FDNA equations for the graph in Figure 13

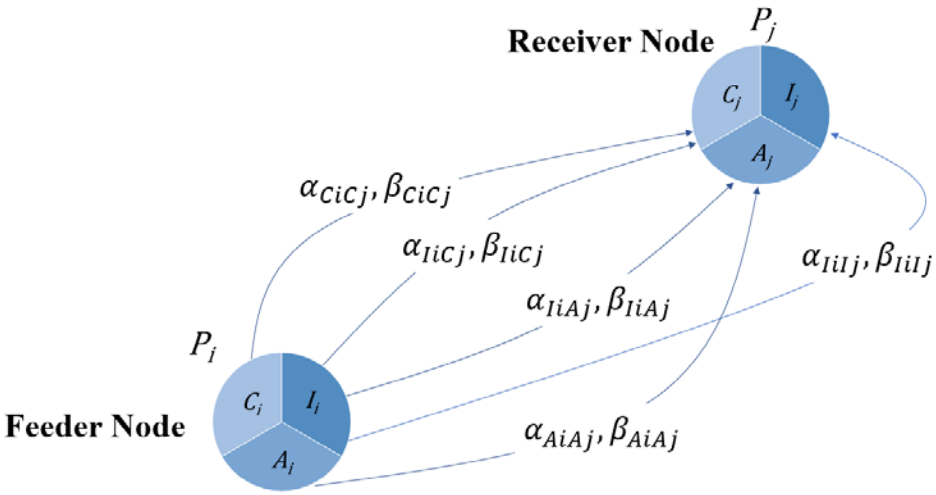


Figure 13. A 2-node FDNA-Cyber graph

The FDNA-Cyber graph in Figure 13 consists of two nodes P_i , *and* P_j.. The equations for operability level of each single node – P_i , *and* P_j – without considering the dependencies are as follows.

$$P_i = w_{Ci}V_{Ci} + w_{Ii}V_{Ii} + w_{Ai}V_{Ai}$$

$$P_j = w_{Cj}V_{Cj} + w_{Ij}V_{Ij} + w_{Aj}V_{Aj}$$

$$w_{Ci} + w_{Ii} + w_{Ai} = 1$$

$$w_{Cj} + w_{Ij} + w_{Aj} = 1$$

$$V_{Ci} = V_{Ci}(X_{Ci}), V_{Ii} = V_{Ii}(X_{Ii}), V_{Ai} = V_{Ai}(X_{Ai}), V_{Cj} = V_{Cj}(X_{Cj}), V_{Ij} = V_{Ij}(X_{Ij}), V_{Aj} = V_{Aj}(X_{Aj})$$

$$0 \leq V_{Ci}, V_{Ii}, V_{Ai}, V_{Cj}, V_{Ij}, V_{Aj} \leq 100$$

$$0 \leq P_i, P_j \leq 100\ ,$$

$$For\ \forall\ X, Y\ \in \{C, I, A\}, 0 < \alpha_{XiYj} \leq 1\ , 0 \leq \beta_{XiYj} \leq 100$$

At first, let's start from a basic scenario. Let's assume that there is only one dependency point. If this dependency is from C_i *to* C_j, then the FDNA-Cyber equation is as follows.

$$V_{Cj} = SE_{Cj}(Min(SODV_{CjCi}, CODV_{CjCi})) = SE_{Cj}(Min(\alpha_{CiCj}V_{Ci} + 100(1 - \alpha_{CiCj}), V_{Ci} + \beta_{CiCj}))$$

where SE_{Cj} is self-efficiency of Confidentiality component of P_j and $0 \leq SE_{Cj} \leq 1$

α_{CiCj} is the strength of dependency fraction between V_{Ci} and V_{Cj} and $0 \leq \alpha_{CiCj} \leq 1$

β_{CiCj} is the criticality of dependency between V_{Ci} and V_{Cj} and $0 \leq \beta_{CiCj} \leq 100(1 - \alpha_{CiCj})$

$$0 \leq V_{Ci}, V_{Cj} \leq 100$$

If this dependency is from I_i *to* I_j, then the FDNA-Cyber equation is as follows.

$$V_{Ij} = SE_{Ij}(Min(SODV_{IjIi}, CODV_{IjIi})) = SE_{Ij}(Min(\alpha_{IiIj}V_{Ii} + 100(1 - \alpha_{IiIj}), V_{Ii} + \beta_{IiIj}))$$

where SE_{Ij} is self-efficiency of Integrity component of P_j and $0 \leq SE_{Ij} \leq 1$

α_{IiIj} is the strength of dependency fraction between V_{Ii} and V_{Ij} and $0 \leq \alpha_{IiIj} \leq 1$

β_{IiIj} is the criticality of dependency between V_{Ii} and V_{Ij} and $0 \leq \beta_{IiIj} \leq 100(1 - \alpha_{IiIj})$

$$0 \leq V_{Ii}, V_{Ij} \leq 100$$

If this dependency is from A_i *to* A_j, then the FDNA-Cyber equation is as follows.

$$V_{Aj} = SE_{Aj}(Min(SODV_{AjAi}, CODV_{AjAi})) = SE_{Aj}(Min(\alpha_{AiAj}V_{Ai} + 100(1 - \alpha_{AiAj}), V_{Ai} + \beta_{AiAj}))$$

where SE_{Aj} is self-efficiency of Availability component of P_j and $0 \leq SE_{Aj} \leq 1$

α_{AiAj} is the strength of dependency fraction between V_{Ai} and V_{Aj} and $0 \leq \alpha_{AiAj} \leq 1$

β_{AiAj} is the criticality of dependency between V_{Ai} and V_{Aj} and $0 \leq \beta_{AiAj} \leq 100(1 - \alpha_{AiAj})$

$$0 \leq V_{Ai}, V_{Aj} \leq 100$$

When we consider all of the five dependency points in Figure 13 (i.e., dependencies from C_i *to* C_j, from I_i *to* I_j, from I_i *to* C_j, from I_i *to* A_j, from A_i *to* A_j), the FDNA-Cyber dependency function for this graph is given by the following equations.

$$V_{Cj} = SE_{Cj}(Min(Ave(SODV_{CjCi}, SODV_{CjIi}), CODV_{CjCi}, CODV_{CjIi}))$$

$$\Rightarrow V_{Cj} = SE_{Cj}(Min\left(Ave(\alpha_{CiCj}V_{Ci} + 100(1 - \alpha_{CiCj}), \alpha_{IiCj}V_{Ii} + 100(1 - \alpha_{IiCj})\right), V_{Ci} + \beta_{CiCj}, V_{Ii} + \beta_{IiCj}))$$

$$V_{Ij} = SE_{Ij}(Min(SODV_{IjIi}, CODV_{IjIi})) = SE_{Ij}(Min(\alpha_{IiIj}V_{Ii} + 100(1 - \alpha_{IiIj}), V_{Ii} + \beta_{IiIj}))$$

$$V_{Aj} = SE_{Aj}(Min(Ave(SODV_{AjAi}, SODV_{AjIi}), CODV_{AjAi}, CODV_{AjIi}))$$

$$\Rightarrow V_{Aj} = SE_{Aj}(Min\left(Ave(\alpha_{AiAj}V_{Ai} + 100(1 - \alpha_{AiAj}), \alpha_{IiAj}V_{Ii} + 100(1 - \alpha_{IiAj})\right), V_{Ai} + \beta_{AiAj}, V_{Ii} + \beta_{IiAj}))$$

where SE_{Cj} is self-efficiency of Confidentiality component of P_j and $0 \leq SE_{Cj} \leq 1$

α_{CiCj} is the strength of dependency fraction between V_{Ci} and V_{Cj} and $0 \leq \alpha_{CiCj} \leq 1$

β_{CiCj} is the criticality of dependency between V_{Ci} and V_{Cj} and $0 \leq \beta_{CiCj} \leq 100(1 - \alpha_{CiCj})$

$$0 \leq V_{Ci}, V_{Cj} \leq 100$$

SE_{Ij} is self-efficiency of Integrity component of P_j and $0 \leq SE_{Ij} \leq 1$

α_{IiIj} is the strength of dependency fraction between V_{Ii} and V_{Ij} and $0 \leq \alpha_{IiIj} \leq 1$

β_{IiIj} is the criticality of dependency between V_{Ii} and V_{Ij} and $0 \leq \beta_{IiIj} \leq 100(1 - \alpha_{IiIj})$

$$0 \leq V_{Ii}, V_{Ij} \leq 100$$

SE_{Aj} is self-efficiency of Availability component of P_j and $0 \leq SE_{Aj} \leq 1$

α_{AiAj} is the strength of dependency fraction between V_{Ai} and V_{Aj} and $0 \leq \alpha_{AiAj} \leq 1$

β_{AiAj} is the criticality of dependency between V_{Ai} and V_{Aj} and $0 \leq \beta_{AiAj} \leq 100(1 - \alpha_{AiAj})$

α_{IiAj} is the strength of dependency fraction between V_{Ii} and V_{Aj} and $0 \leq \alpha_{IiAj} \leq 1$

β_{IiAj} is the criticality of dependency between V_{Ii} and V_{Aj} and $0 \leq \beta_{IiAj} \leq 100(1 - \alpha_{IiAj})$

$$0 \leq V_{Ai}, V_{Aj} \leq 100$$

Example 2: Formulate the FDNA equations for the graph in Figure 14

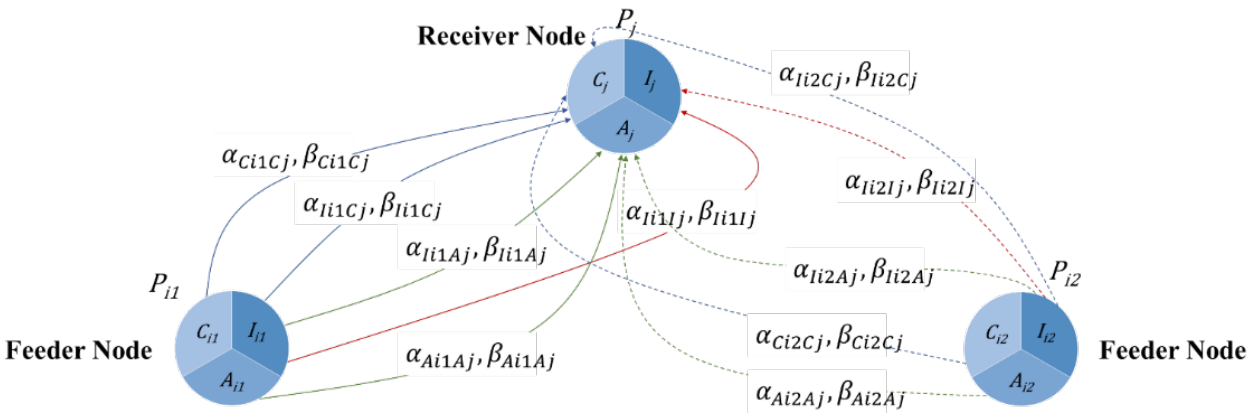


Figure 14. A 3-node FDNA-Cyber graph

The FDNA-Cyber graph in Figure 14 consists of three nodes P_i , $P_{i2,}$ *and* $P_{j..}$ The equations for operability level of each single node – P_{i1} , P_{i2} *and* P_j – without considering the dependencies are as follows.

$$P_{i1} = w_{Ci1}V_{Ci1} + w_{Ii1}V_{Ii1} + w_{Ai1}V_{Ai1}$$

$$P_{i2} = w_{Ci2}V_{Ci2} + w_{Ii2}V_{Ii2} + w_{Ai2}V_{Ai2}$$

$$P_j = w_{Cj}V_{Cj} + w_{Ij}V_{Ij} + w_{Aj}V_{Aj}$$

$$w_{Ci1} + w_{Ii1} + w_{Ai1} = 1$$

$$w_{Ci2} + w_{Ii2} + w_{Ai2} = 1$$

$$w_{Cj} + w_{Ij} + w_{Aj} = 1$$

$$V_{Ci1} = V_{Ci1}(X_{Ci1}), V_{Ii1} = V_{Ii1}(X_{Ii1}), V_{Ai1} = V_{Ai1}(X_{Ai1})$$

$$V_{Ci2} = V_{Ci2}(X_{Ci2}), V_{Ii2} = V_{Ii2}(X_{Ii2}), V_{Ai2} = V_{Ai2}(X_{Ai2}),$$

$$V_{Cj} = V_{Cj}(X_{Cj}), V_{Ij} = V_{Ij}(X_{Ij}), V_{Aj} = V_{Aj}(X_{Aj})$$

$$0 \le V_{Ci1}, V_{Ii1}, V_{Ai1}, V_{Ci2}, V_{Ii2}, V_{Ai2}, V_{Cj}, V_{Ij}, V_{Aj} \le 100$$

$$0 \leq P_{i1}, P_{i2}, P_j \leq 100$$

$$\forall\, X, Y \in \{C, I, A\}: 0 < \alpha_{Xi1Yj}, \alpha_{Xi2Yj} \leq 1\,, 0 \leq \beta_{Xi1Yj,}\beta_{Xi2Yj} \leq 100$$

The FDNA-Cyber dependency function for the graph in Figure 14 is given by the following equations.

$$V_{Cj} = SE_{Cj}(Min\begin{pmatrix} Ave(SODV_{CjCi1}, SODV_{CjCi2}, SODV_{CjIi1}, SODV_{CjIi2}), \\ CODV_{CjCi1}, CODV_{CjCi2}, CODV_{CjIi1}, CODV_{CjIi2} \end{pmatrix})$$

$$\Rightarrow V_{Cj} = SE_{Cj}(Min\Big(Ave(\alpha_{Ci1Cj}V_{Ci1} + 100(1-\alpha_{Ci1Cj}), \alpha_{Ci2Cj}V_{Ci2} + 100(1-\alpha_{Ci2Cj}), \alpha_{Ii1Cj}V_{Ii1} + 100(1-\alpha_{Ii1Cj}), \alpha_{Ii2Cj}V_{Ii2} + 100(1-\alpha_{Ii2Cj})\Big), V_{Ci1} + \beta_{Ci1Cj}, V_{Ci2} + \beta_{Ci2Cj,}V_{Ii1} + \beta_{Ii1Cj}, V_{Ii2} + \beta_{Ii2Cj}))$$

$$V_{Ij} = SE_{Ij}(Min(Ave(SODV_{IjIi1}, SODV_{IjIi2}), CODV_{IjIi1}, CODV_{IjIi2}))$$

$$\Rightarrow V_{Ij} = SE_{Ij}(Min(Ave\Big(\alpha_{Ii1Ij}V_{Ii1} + 100(1-\alpha_{Ii1Ij}), \alpha_{Ii2Ij}V_{Ii2} + 100(1-\alpha_{Ii2Ij})\Big), V_{Ii1} + \beta_{Ii1Ij}, V_{Ii2} + \beta_{Ii2Ij}))$$

$$V_{Aj} = SE_{Aj}(Min\begin{pmatrix} Ave(SODV_{AjAi1}, SODV_{AjAi2}, SODV_{AjIi1}, SODV_{AjIi2}), \\ CODV_{AjAi1}, CODV_{AjAi2}, CODV_{AjIi1}, CODV_{AjIi2} \end{pmatrix})$$

$$\Rightarrow V_{Aj} = SE_{Aj}(Min\Big(Ave(\alpha_{Ai1Aj}V_{Ai1} + 100(1-\alpha_{Ai1Aj}), \alpha_{Ai2Aj}V_{Ai2} + 100(1-\alpha_{Ai2Aj}), \alpha_{Ii1Aj}V_{Ii1} + 100(1-\alpha_{Ii1Aj}), \alpha_{Ii2Aj}V_{Ii2} + 100(1-\alpha_{Ii2Aj})\Big), V_{Ai1} + \beta_{Ai1Aj}, V_{Ai2} + \beta_{Ai2Aj,}V_{Ii1} + \beta_{Ii1Aj}, V_{Ii2} + \beta_{Ii2Aj}))$$

where SE_{Cj} is self-efficiency of Confidentiality component of P_j and $0 \leq SE_{Cj} \leq 1$

α_{Ci1Cj} is the strength of dependency fraction between V_{Ci1} and V_{Cj} and $0 \leq \alpha_{Ci1Cj} \leq 1$

β_{Ci1Cj} is the criticality of dependency between V_{Ci1} and V_{Cj} and $0 \leq \beta_{Ci1Cj} \leq 100(1 - \alpha_{Ci1Cj})$

α_{Ci2Cj} is the strength of dependency fraction between V_{Ci2} and V_{Cj} and $0 \leq \alpha_{Ci2Cj} \leq 1$

β_{Ci2Cj} is the criticality of dependency between V_{Ci2} and V_{Cj} and $0 \leq \beta_{Ci2Cj} \leq 100(1 - \alpha_{Ci2Cj})$

α_{Ii1Cj} is the strength of dependency fraction between V_{Ii1} and V_{Cj} and $0 \leq \alpha_{Ii1Cj} \leq 1$

β_{Ii1Cj} is the criticality of dependency between V_{Ii1} and V_{Cj} and $0 \leq \beta_{Ii1Cj} \leq 100(1 - \alpha_{Ii1Cj})$

α_{Ii2Cj} is the strength of dependency fraction between V_{Ii2} and V_{Cj} and $0 \leq \alpha_{Ii2Cj} \leq 1$

β_{Ii2Cj} is the criticality of dependency between V_{Ii2} and V_{Cj} and $0 \leq \beta_{Ii2Cj} \leq 100(1 - \alpha_{Ii2Cj})$

$$0 \leq V_{Ci1}, V_{Ci2}, V_{Cj} \leq 100$$

SE_{Ij} is self-efficiency of Integrity component of P_j and $0 \leq SE_{Ij} \leq 1$

α_{Ii1Ij} is the strength of dependency fraction between V_{Ii1} and V_{Ij} and $0 \leq \alpha_{Ii1Ij} \leq 1$

β_{Ii1Ij} is the criticality of dependency between V_{Ii1} and V_{Ij} and $0 \leq \beta_{Ii1Ij} \leq 100(1 - \alpha_{Ii1Ij})$

α_{Ii2Cj} is the strength of dependency fraction between V_{Ii2} and V_{Cj} and $0 \leq \alpha_{Ii2Cj} \leq 1$

β_{Ii2Cj} is the criticality of dependency between V_{Ii2} and V_{Cj} and $0 \leq \beta_{Ii2Cj} \leq 100(1 - \alpha_{Ii2Cj})$

$$0 \leq V_{Ii1}, V_{Ii2}, V_{Ij} \leq 100$$

SE_{Aj} is self-efficiency of Availability component of P_j and $0 \leq SE_{Aj} \leq 1$

α_{Ai1Aj} is the strength of dependency fraction between V_{Ai1} and V_{Aj} and $0 \leq \alpha_{Ai1Aj} \leq 1$

β_{Ai1Aj} is the criticality of dependency between V_{Ai1} and V_{Aj} and $0 \leq \beta_{Ai1Aj} \leq 100(1 - \alpha_{Ai1Aj})$

α_{Ai2Aj} is the strength of dependency fraction between V_{Ai2} and V_{Aj} and $0 \leq \alpha_{Ai2Aj} \leq 1$

β_{Ai2Aj} is the criticality of dependency between V_{Ai2} and V_{Aj} and $0 \leq \beta_{Ai2Aj} \leq 100(1 - \alpha_{Ai2Aj})$

α_{Ii1Aj} is the strength of dependency fraction between V_{Ii1} and V_{Aj} and $0 \leq \alpha_{Ii1Aj} \leq 1$

β_{Ii1Aj} is the criticality of dependency between V_{Ii1} and V_{Aj} and $0 \leq \beta_{Ii1Aj} \leq 100(1 - \alpha_{Ii1Aj})$

α_{Ii2Aj} is the strength of dependency fraction between V_{Ii2} and V_{Aj} and $0 \leq \alpha_{Ii2Aj} \leq 1$

β_{Ii2Aj} is the criticality of dependency between V_{Ii2} and V_{Aj} and $0 \leq \beta_{Ii2Aj} \leq 100(1 - \alpha_{Ii2Aj})$

$$0 \leq V_{Ai1}, V_{Ai2}, V_{Aj} \leq 100$$

Example 3: Formulate the FDNA equations for the graph in Figure 15

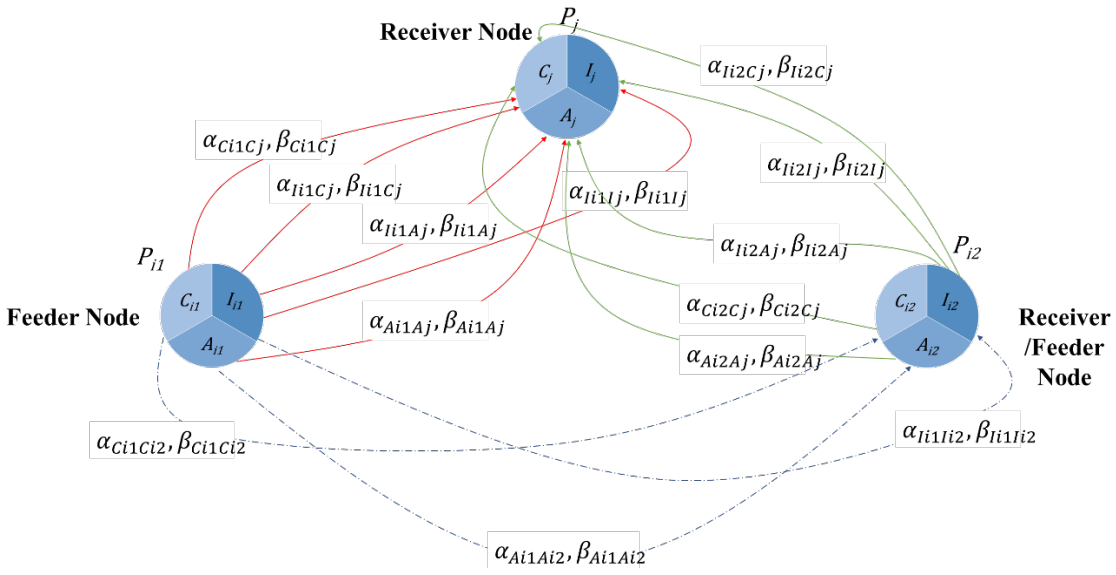


Figure 15. A 3-node FDNA-Cyber graph

The FDNA-Cyber graph in Figure 15 consists of three nodes P_i , $P_{i2,}$ *and* $P_{j.}$ The equations for operability level of each single node – P_{i1} , P_{i2} *and* P_j – without considering the dependencies are as follows.

$$P_{i1} = w_{Ci1}V_{Ci1} + w_{Ii1}V_{Ii1} + w_{Ai1}V_{Ai1}$$

$$P_{i2} = w_{Ci2}V_{Ci2} + w_{Ii2}V_{Ii2} + w_{Ai2}V_{Ai2}$$

$$P_j = w_{Cj}V_{Cj} + w_{Ij}V_{Ij} + w_{Aj}V_{Aj}$$

$$w_{Ci1} + w_{Ii1} + w_{Ai1} = 1$$

$$w_{Ci2} + w_{Ii2} + w_{Ai2} = 1$$

$$w_{Cj} + w_{Ij} + w_{Aj} = 1$$

$$V_{Ci1} = V_{Ci1}(X_{Ci1}), V_{Ii1} = V_{Ii1}(X_{Ii1}), V_{Ai1} = V_{Ai1}(X_{Ai1})$$

$$V_{Ci2} = V_{Ci2}(X_{Ci2}), V_{Ii2} = V_{Ii2}(X_{Ii2}), V_{Ai2} = V_{Ai2}(X_{Ai2}),$$

$$V_{Cj} = V_{Cj}(X_{Cj}), V_{Ij} = V_{Ij}(X_{Ij}), V_{Aj} = V_{Aj}(X_{Aj})$$

$$0 \leq V_{Ci1}, V_{Ii1}, V_{Ai1}, V_{Ci2}, V_{Ii2}, V_{Ai2}, V_{Cj}, V_{Ij}, V_{Aj} \leq 100$$

$$0 \leq P_{i1}, P_{i2}, P_j \leq 100$$

$$\forall\, X, Y \in \{C, I, A\}: 0 < \alpha_{Xi1Yj}, \alpha_{Xi2Yj}, \alpha_{Xi1Yi2}, \leq 1\,, 0 \leq \beta_{Xi1Yj}, \beta_{Xi2Yj}, \beta_{Xi1Yi2} \leq 100$$

The FDNA-Cyber dependency function for the graph in Figure 15 is given by the following equations.

$$V_{Ci2} = SE_{Ci2}(Min(SODV_{Ci2Ci1}, CODV_{Ci2Ci1})$$

$$\Rightarrow\ V_{Ci2} = SE_{Ci2}(Min(\alpha_{Ci1Ci2}V_{Ci1} + 100(1 - \alpha_{Ci1Ci2}), V_{Ci1} + \beta_{Ci1Ci2}))$$

$$V_{Ii2} = SE_{Ii2}(Min(SODV_{Ii2Ii1}, CODV_{Ii2Ii1})$$

$$\Rightarrow\ V_{Ii2} = SE_{Ii2}(Min(\alpha_{Ii1Ii2}V_{Ii1} + 100(1 - \alpha_{Ii1Ii2}), V_{Ii1} + \beta_{Ii1Ii2}))$$

$$V_{Ai2} = SE_{Ai2}(Min(SODV_{Ai2Ai1}, CODV_{Ai2Ai1})$$

$$\Rightarrow\ V_{Ai2} = SE_{Ai2}(Min(\alpha_{Ai1Ai2}V_{Ai1} + 100(1 - \alpha_{Ai1Ai2}), V_{Ai1} + \beta_{Ai1Ai2}))$$

$$V_{Cj} = SE_{Cj}(Min\begin{pmatrix} Ave(SODV_{CjCi1}, SODV_{CjCi2}, SODV_{CjIi1}, SODV_{CjIi2}), \\ CODV_{CjCi1}, CODV_{CjCi2}, CODV_{CjIi1}, CODV_{CjIi2} \end{pmatrix})$$

$$\Rightarrow V_{Cj} = SE_{Cj}(Min\Big(Ave(\alpha_{Ci1Cj}V_{Ci1} + 100(1-\alpha_{Ci1Cj}), \alpha_{Ci2Cj}V_{Ci2} + 100(1-\alpha_{Ci2Cj}), \alpha_{Ii1Cj}V_{Ii1} + 100(1-\alpha_{Ii1Cj}), \alpha_{Ii2Cj}V_{Ii2} + 100(1-\alpha_{Ii2Cj})\Big), V_{Ci1} + \beta_{Ci1Cj}, V_{Ci2} + \beta_{Ci2Cj,}V_{Ii1} + \beta_{Ii1Cj}, V_{Ii2} + \beta_{Ii2Cj}))$$

$$V_{Ij} = SE_{Ij}(Min(Ave(SODV_{IjIi1}, SODV_{IjIi2}), CODV_{IjIi1}, CODV_{IjIi2}))$$

$$\Rightarrow V_{Ij} = SE_{ij}(Min(Ave\Big(\alpha_{Ii1Ij}V_{Ii1} + 100(1-\alpha_{Ii1Ij}), \alpha_{Ii2Ij}V_{Ii2} + 100(1-\alpha_{Ii2Ij})\Big), V_{Ii1} + \beta_{Ii1Ij}, V_{Ii2} + \beta_{Ii2Ij}))$$

$$V_{Aj} = SE_{Aj}(Min\begin{pmatrix} Ave(SODV_{AjAi1}, SODV_{AjAi2}, SODV_{AjIi1}, SODV_{AjIi2}), \\ CODV_{AjAi1}, CODV_{AjAi2}, CODV_{AjIi1}, CODV_{AjIi2} \end{pmatrix})$$

$$\Rightarrow V_{Aj} = SE_{Aj}(Min\Big(Ave(\alpha_{Ai1Aj}V_{Ai1} + 100(1-\alpha_{Ai1Aj}), \alpha_{Ai2Aj}V_{Ai2} + 100(1-\alpha_{Ai2Aj}), \alpha_{Ii1AJ}V_{Ii1} + 100(1-\alpha_{Ii1Aj}), \alpha_{Ii2Aj}V_{Ii2} + 100(1-\alpha_{Ii2Aj})\Big), V_{Ai1} + \beta_{Ai1Aj}, V_{Ai2} + \beta_{Ai2Aj,}V_{Ii1} + \beta_{Ii1Aj}, V_{Ii2} + \beta_{Ii2Aj}))$$

where SE_{Ci2} is self-efficiency of Confidentiality component of P_{i2} and $0 \leq SE_{i2} \leq 1$

α_{Ci1Ci2} is the strength of dependency fraction between V_{Ci1} and V_{Ci2} and $0 \leq \alpha_{Ci1Ci2} \leq 1$

β_{Ci1Ci2} is the criticality of dependency between V_{Ci1} and V_{Ci2} and $0 \leq \beta_{Ci1Ci2} \leq 100(1-\alpha_{Ci1Ci2})$

α_{Ii1Ii2} is the strength of dependency fraction between V_{Ii1} and V_{Ii2} and $0 \leq \alpha_{Ii1Ii2} \leq 1$

β_{Ii1Ii2} is the criticality of dependency between V_{Ii1} and V_{Ii2} and $0 \leq \beta_{Ii1Ii2} \leq 100(1-\alpha_{Ii1Ii2})$

α_{Ai1Ai2} is the strength of dependency fraction between V_{Ai1} and V_{Ai2} and $0 \leq \alpha_{Ai1Ai2} \leq 1$

β_{Ai1Ai2} is the criticality of dependency between V_{Ai1} and V_{Ai2} and $0 \leq \beta_{Ai1Ai2} \leq 100(1 - \alpha_{Ai1Ai2})$

$$\forall\, X \in \{i1, i2, j\}\colon 0 \leq V_{CX}, V_{IX}, V_{AX} \leq 100$$

SE_{Cj} is self-efficiency of Confidentiality component of P_j and $0 \leq SE_{Cj} \leq 1$

α_{Ci1Cj} is the strength of dependency fraction between V_{Ci1} and V_{Cj} and $0 \leq \alpha_{Ci1Cj} \leq 1$

β_{Ci1Cj} is the criticality of dependency between V_{Ci1} and V_{Cj} and $0 \leq \beta_{Ci1Cj} \leq 100(1 - \alpha_{Ci1Cj})$

α_{Ci2Cj} is the strength of dependency fraction between V_{Ci2} and V_{Cj} and $0 \leq \alpha_{Ci2Cj} \leq 1$

β_{Ci2Cj} is the criticality of dependency between V_{Ci2} and V_{Cj} and $0 \leq \beta_{Ci2Cj} \leq 100(1 - \alpha_{Ci2Cj})$

α_{Ii1Cj} is the strength of dependency fraction between V_{Ii1} and V_{Cj} and $0 \leq \alpha_{Ii1Cj} \leq 1$

β_{Ii1Cj} is the criticality of dependency between V_{Ii1} and V_{Cj} and $0 \leq \beta_{Ii1Cj} \leq 100(1 - \alpha_{Ii1Cj})$

α_{Ii2Cj} is the strength of dependency fraction between V_{Ii2} and V_{Cj} and $0 \leq \alpha_{Ii2Cj} \leq 1$

β_{Ii2Cj} is the criticality of dependency between V_{Ii2} and V_{Cj} and $0 \leq \beta_{Ii2Cj} \leq 100(1 - \alpha_{Ii2Cj})$

SE_{Ij} is self-efficiency of Integrity component of P_j and $0 \leq SE_{Ij} \leq 1$

α_{Ii1Ij} is the strength of dependency fraction between V_{Ii1} and V_{Ij} and $0 \leq \alpha_{Ii1Ij} \leq 1$

β_{Ii1Ij} is the criticality of dependency between V_{Ii1} and V_{Ij} and $0 \leq \beta_{Ii1Ij} \leq 100(1 - \alpha_{Ii1Ij})$

α_{Ii2Cj} is the strength of dependency fraction between V_{Ii2} and V_{Cj} and $0 \leq \alpha_{Ii2Cj} \leq 1$

β_{Ii2Cj} is the criticality of dependency between V_{Ii2} and V_{Cj} and $0 \leq \beta_{Ii2Cj} \leq 100(1 - \alpha_{Ii2Cj})$

SE_{Aj} is self-efficiency of Availability component of P_j and $0 \leq SE_{Aj} \leq 1$

α_{Ai1Aj} is the strength of dependency fraction between V_{Ai1} and V_{Aj} and $0 \leq \alpha_{Ai1Aj} \leq 1$

β_{Ai1Aj} is the criticality of dependency between V_{Ai1} and V_{Aj} and $0 \leq \beta_{Ai1Aj} \leq 100(1 - \alpha_{Ai1Aj})$

α_{Ai2Aj} is the strength of dependency fraction between V_{Ai2} and V_{Aj} and $0 \leq \alpha_{Ai2Aj} \leq 1$

β_{Ai2Aj} is the criticality of dependency between V_{Ai2} and V_{Aj} and $0 \leq \beta_{Ai2Aj} \leq 100(1 - \alpha_{Ai2Aj})$

α_{Ii1Aj} is the strength of dependency fraction between V_{Ii1} and V_{Aj} and $0 \leq \alpha_{Ii1Aj} \leq 1$

β_{Ii1Aj} is the criticality of dependency between V_{Ii1} and V_{Aj} and $0 \leq \beta_{Ii1Aj} \leq 100(1 - \alpha_{Ii1Aj})$

α_{Ii2Aj} is the strength of dependency fraction between V_{Ii2} and V_{Aj} and $0 \leq \alpha_{Ii2Aj} \leq 1$

β_{Ii2Aj} is the criticality of dependency between V_{Ii2} and V_{Aj} and $0 \leq \beta_{Ii2Aj} \leq 100(1 - \alpha_{Ii2Aj})$

4.5.3. AND Gate Integration

In cyberspace, dependency relationships of classical FDNA are not sufficient to model the types of dependencies of some FDNA-Cyber nodes (i.e., assets, services or business processes). For instance, if there are two databases in a system and an application server needs to query both of them concurrently (e.g. querying user's social security number from one database and user's date of birth from another database) to respond to a request coming from a web server (i.e., a user's social security number and date of birth), the dependencies of the application server to database servers cannot be modeled by two feeder one receiver node dependency of classical FDNA algebra. A new concept – AND gate – is developed to expand the classical FDNA algebra to cover such situations (Figure 16).

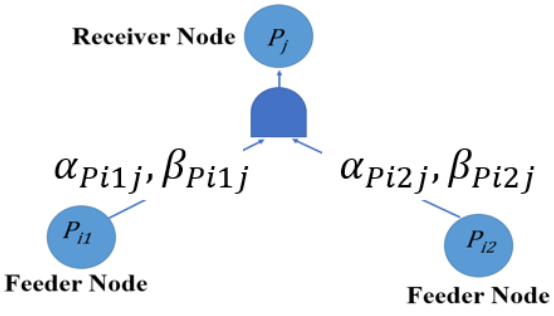


Figure 16. AND dependency of a 3-node FDNA graph

The FDNA-Cyber graph in Figure 16 consists of three nodes P_i , $P_{i2,}$ *and* $P_{j..}$ The equations for operability level of the receiver node –P_j – as follows.

$$P_j = SE_j(Min\left(Min\left(SODP_{ji1}, CODP_{ji1}\right), Min\left(SODP_{ji2}, CODP_{ji2}\right)\right))$$

⇨ $P_j = SE_j(Min\left(SODP_{ji1}, SODP_{ji2}, CODP_{ji1}, CODP_{ji2}\right))$

⇨ $P_j = SE_j(Min\left(\alpha_{P_{i1j}}P_{i1} + 100\left(1 - \alpha_{P_{i1j}}\right), \alpha_{P_{i2j}}P_{i2} + 100\left(1 - \alpha_{P_{i2j}}\right), P_{i1} + \beta_{P_{i1j}}, P_{i2} + \beta_{P_{i2j}}\right))$

where SE_j is self-efficiency of of P_j and $0 \leq SE_j \leq 1$

α_{Pi1j} is the strength of dependency fraction between P_{i1} and P_j and $0 \leq \alpha_{Pi1j} \leq 1$

β_{Pi1j} is the criticality of dependency between P_{i1} and P_j and $0 \leq \beta_{Pi1j} \leq 100(1 - \alpha_{Pi1j})$

α_{Pi2j} is the strength of dependency fraction between P_{i2} and P_j and $0 \leq \alpha_{Pi2j} \leq 1$

β_{Pi2j} is the criticality of dependency between P_{i2} and P_j and $0 \leq \beta_{Pi2j} \leq 100(1 - \alpha_{Pi2j})$

To define the FDNA-Cyber algebra with AND gate, several FDNA-Cyber dependency equations are developed based on examples.

Example 4: Formulate the FDNA equations for the graph in Figure 17

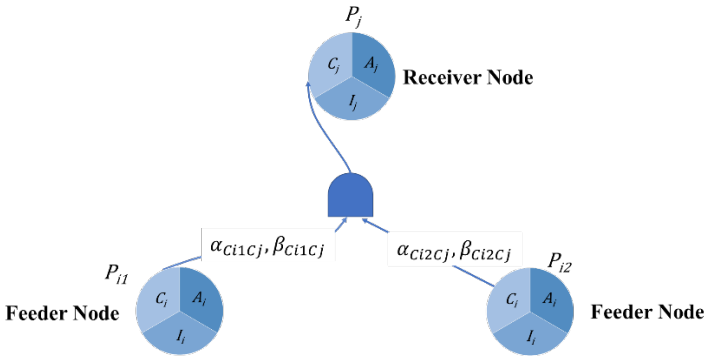


Figure 17. A 3-node FDNA-Cyber graph with AND gate dependency

The FDNA-Cyber graph in Figure 17 consists of three nodes P_{i1}, $P_{i2,}$ *and* $P_{j..}$ The equations for operability level of each single node – P_{i1}, P_{i2} *and* P_j – without considering the dependencies are as follows.

$$P_{i1} = w_{Ci1}V_{Ci1} + w_{Ii1}V_{Ii1} + w_{Ai1}V_{Ai1}$$

$$P_{i2} = w_{Ci2}V_{Ci2} + w_{Ii2}V_{Ii2} + w_{Ai2}V_{Ai2}$$

$$P_j = w_{Cj}V_{Cj} + w_{Ij}V_{Ij} + w_{Aj}V_{Aj}$$

$$w_{Ci1} + w_{Ii1} + w_{Ai1} = 1$$

$$w_{Ci2} + w_{Ii2} + w_{Ai2} = 1$$

$$w_{Cj} + w_{Ij} + w_{Aj} = 1$$

$$V_{Ci1} = V_{Ci1}(X_{Ci1}), V_{Ii1} = V_{Ii1}(X_{Ii1}), V_{Ai1} = V_{Ai1}(X_{Ai1})$$

$$V_{Ci2} = V_{Ci2}(X_{Ci2}), V_{Ii2} = V_{Ii2}(X_{Ii2}), V_{Ai2} = V_{Ai2}(X_{Ai2}),$$

$$V_{Cj} = V_{Cj}(X_{Cj}), V_{Ij} = V_{Ij}(X_{Ij}), V_{Aj} = V_{Aj}(X_{Aj})$$

$$0 \le V_{Ci1}, V_{Ii1}, V_{Ai1}, V_{Ci2}, V_{Ii2}, V_{Ai2}, V_{Cj}, V_{Ij}, V_{Aj} \le 100$$

$$0 \le P_{i1}, P_{i2}, P_j \le 100$$

$$\forall\, X, Y\ \in \{C, I, A\}: 0 < \alpha_{Xi1Yj}, \alpha_{Xi2Yj}, \alpha_{Xi1Yi2}, \leq 1\ , 0 \leq \beta_{Xi1Yj}, \beta_{Xi2Yj}, \beta_{Xi1Yi2} \leq 100$$

The FDNA-Cyber dependency function for the graph in Figure 17 is given by the following equations.

$$V_{Cj} = SE_{Cj}(Min\left(Min\left(SODV_{CjCi1}, CODV_{CjCi1}\right), Min\left(SODV_{CjCi2}, CODV_{CjCi2}\right)\right))$$

$$\Rightarrow\ V_{Cj} = SE_{Cj}(Min\left(SODV_{CjCi1}, CODV_{CjCi1}, SODV_{CjCi2}, CODV_{CjCi2}\right))$$

$$\Rightarrow\ V_{Cj} = SE_{Cj}(Min\left(\alpha_{Ci1Cj}V_{Ci1} + 100\left(1 - \alpha_{Ci1Cj}\right), \alpha_{Ci2Cj}V_{Ci2} + 100\left(1 - \alpha_{Ci2Cj}\right), V_{Ci1} + \beta_{Ci1Cj}, V_{Ci2} + \beta_{Ci2Cj}\right))$$

Where SE_{Cj} is self-efficiency of Confidentiality component of P_j and $0 \leq SE_{Cj} \leq 1$

α_{Ci1Cj} is the strength of dependency fraction between V_{Ci1} and V_{Cj} and $0 \leq \alpha_{Ci1Cj} \leq 1$

β_{Ci1Cj} is the criticality of dependency between V_{Ci1} and V_{Cj} and $0 \leq \beta_{Ci1Cj} \leq 100(1 - \alpha_{Ci1Cj})$

α_{Ci2Cj} is the strength of dependency fraction between V_{Ci2} and V_{Cj} and $0 \leq \alpha_{Ci2Cj} \leq 1$

β_{Ci2Cj} is the criticality of dependency between V_{Ci2} and V_{Cj} and $0 \leq \beta_{Ci2Cj} \leq 100(1 - \alpha_{Ci2Cj})$

$$0 \leq V_{Ci1}, V_{Ci2}, V_{Cj} \leq 100$$

Example 5: Formulate the FDNA equations for the graph in Figure 18

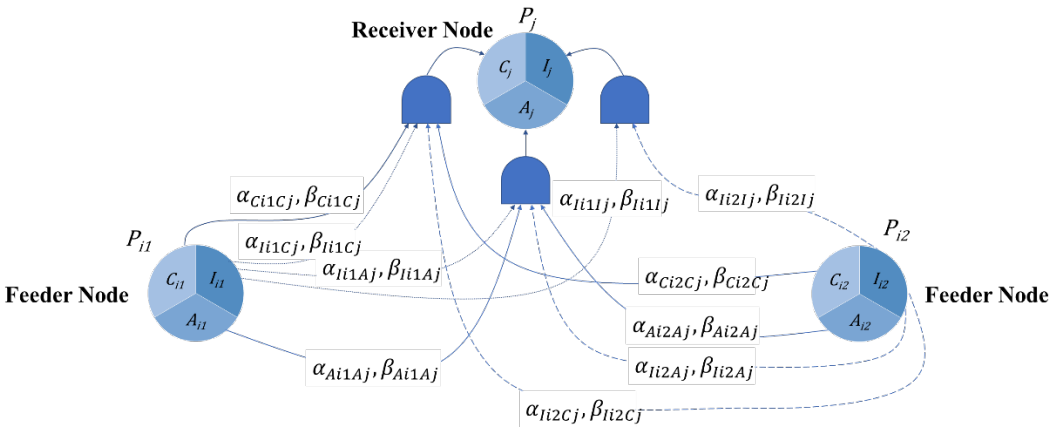


Figure 18. A 3-node FDNA-Cyber graph with AND gate dependency

The FDNA-Cyber graph in Figure 18 consists of three nodes P_i , $P_{i2,}$ *and* $P_{j..}$ The equations for operability level of each single node – P_{i1} , P_{i2} *and* P_j – without considering the dependencies are as follows.

$$P_{i1} = w_{Ci1}V_{Ci1} + w_{Ii1}V_{Ii1} + w_{Ai1}V_{Ai1}$$

$$P_{i2} = w_{Ci2}V_{Ci2} + w_{Ii2}V_{Ii2} + w_{Ai2}V_{Ai2}$$

$$P_j = w_{Cj}V_{Cj} + w_{Ij}V_{Ij} + w_{Aj}V_{Aj}$$

$$w_{Ci1} + w_{Ii1} + w_{Ai1} = 1$$

$$w_{Ci2} + w_{Ii2} + w_{Ai2} = 1$$

$$w_{Cj} + w_{Ij} + w_{Aj} = 1$$

$$V_{Ci1} = V_{Ci1}(X_{Ci1}), V_{Ii1} = V_{Ii1}(X_{Ii1}), V_{Ai1} = V_{Ai1}(X_{Ai1})$$

$$V_{Ci2} = V_{Ci2}(X_{Ci2}), V_{Ii2} = V_{Ii2}(X_{Ii2}), V_{Ai2} = V_{Ai2}(X_{Ai2}),$$

$$V_{Cj} = V_{Cj}(X_{Cj}), V_{Ij} = V_{Ij}(X_{Ij}), V_{Aj} = V_{Aj}(X_{Aj})$$

$$0 \le V_{Ci1}, V_{Ii1}, V_{Ai1}, V_{Ci2}, V_{Ii2}, V_{Ai2}, V_{Cj}, V_{Ij}, V_{Aj} \le 100$$

$$0 \leq P_{i1}, P_{i2}, P_j \leq 100$$

$$\forall\, X, Y \in \{C, I, A\}: 0 < \alpha_{Xi1Yj}, \alpha_{Xi2Yj} \leq 1\,, 0 \leq \beta_{Xi1Yj,}\beta_{Xi2Yj} \leq 100$$

The FDNA-Cyber dependency function for the graph in Figure 18 is given by the following equations.

$$V_{Cj} = SE_{Cj}(Min\begin{pmatrix} Min(SODV_{CjCi1}, CODV_{CjCi1}), \\ Min(SODV_{CjIi1}, CODV_{CjIi1}), \\ Min(SODV_{CjCi2}, CODV_{CjCi2}), \\ Min(SODV_{CjIi2}, CODV_{CjIi2}) \end{pmatrix})$$

$$\Rightarrow V_{Cj} = SE_{Cj}(Min\Big(Min\big(\alpha_{Ci1Cj}V_{Ci1} + 100(1-\alpha_{Ci1Cj}), V_{Ci1} + \beta_{Ci1Cj}\big), Min\big(\alpha_{Ii1Cj}V_{Ii1} + 100(1-\alpha_{Ii1Cj}), V_{Ii1} + \beta_{Ii1Cj}\big), Min\big(\alpha_{Ci2Cj}V_{Ci2} + 100(1-\alpha_{Ci2Cj}), V_{Ci2} + \beta_{Ci2Cj}\big), Min\big(\alpha_{Ii2Cj}V_{Ii2} + 100(1-\alpha_{Ii2Ij}), V_{Ii2} + \beta_{Ii2Cj}\big)\Big)$$

$$\Rightarrow V_{Cj} = SE_{Cj}(Min\big(\alpha_{Ci1Cj}V_{Ci1} + 100(1-\alpha_{Ci1Cj}), V_{Ci1} + \beta_{Ci1Cj}, \alpha_{Ii1Cj}V_{Ii1} + 100(1-\alpha_{Ii1Cj}), V_{Ii1} + \beta_{Ii1Cj,}\alpha_{Ci2Cj}V_{Ci2} + 100(1-\alpha_{Ci2Cj}), V_{Ci2} + \beta_{Ci2Cj}, \alpha_{Ii2Cj}V_{Ii2} + 100(1-\alpha_{Ii2Cj}), V_{Ii2} + \beta_{Ii2Cj}\,))$$

$$V_{Ij} = SE_{Ij}(Max\Big(Min\big(SODV_{IjIi1}, CODV_{IjIi1}\big), Min\big(SODV_{IjIi2}, CODV_{IjIi2}\big)\Big))$$

$$\Rightarrow V_{Ij} = SE_{Ij}(Min\Big(Min\big(\alpha_{Ii1Ij}V_{Ii1} + 100(1-\alpha_{Ii1Ij}), V_{Ii1} + \beta_{Ii1Ij}\big), Min\big(\alpha_{Ii2Ij}V_{Ii2} + 100(1-\alpha_{Ii2Ij}), V_{Ii2} + \beta_{Ii2Ij}\big)\Big))$$

⇨ $V_{Ij} = SE_{Ij}(Min(\alpha_{Ii1Ij}V_{Ii1} + 100(1 - \alpha_{Ii1Ij}), V_{Ii1} + \beta_{Ii1Ij}, \alpha_{Ii2Ij}V_{Ii2} + 100(1 - \alpha_{Ii2Ij}), V_{Ii2} + \beta_{Ii2Ij}))$

$$V_{Aj} = Min\begin{pmatrix} Min(SODV_{AjAi1}, CODV_{AjAi1}), \\ Min(SODV_{AjIi1}, CODV_{AjIi1}), \\ Min(SODV_{AjAi2}, CODV_{AjAi2}), \\ Min(SODV_{AjIi2}, CODV_{AjIi2}) \end{pmatrix}$$

⇨ $V_{Aj} = SE_{Aj}(Min\left(Min(\alpha_{Ai1Aj}V_{Ai1} + 100(1 - \alpha_{Ai1Aj}), V_{Ai1} + \beta_{Ai1Aj}), Min(\alpha_{Ii1Aj}V_{Ii1} + 100(1 - \alpha_{Ii1Aj}), V_{Ii1} + \beta_{Ii1Aj}), Min(\alpha_{Ai2Aj}V_{Ai2} + 100(1 - \alpha_{Ai2Aj}), V_{Ai2} + \beta_{Ai2Aj}), Min(\alpha_{Ii2Aj}V_{Ii2} + 100(1 - \alpha_{Ii2Aj}), V_{Ii2} + \beta_{Ii2Aj})\right))$

⇨ $V_{Aj} = SE_{Aj}(Min(\alpha_{Ai1Aj}V_{Ai1} + 100(1 - \alpha_{Ai1Aj}), V_{Ai1} + \beta_{Ai1Aj}, \alpha_{Ii1Aj}V_{Ii1} + 100(1 - \alpha_{Ii1Aj}), V_{Ii1} + \beta_{Ii1Aj}, \alpha_{Ai2Aj}V_{Ai2} + 100(1 - \alpha_{Ai2Aj}), V_{Ai2} + \beta_{Ai2Aj}, \alpha_{Ii2Aj}V_{Ii2} + 100(1 - \alpha_{Ii2Aj}), V_{Ii2} + \beta_{Ii2Aj}\ ))$

Where SE_{Cj} is self-efficiency of Confidentiality component of P_j and $0 \leq SE_{Cj} \leq 1$

α_{Ci1Cj} is the strength of dependency fraction between V_{Ci1} and V_{Cj} and $0 \leq \alpha_{Ci1Cj} \leq 1$

β_{Ci1Cj} is the criticality of dependency between V_{Ci1} and V_{Cj} and $0 \leq \beta_{Ci1Cj} \leq 100(1 - \alpha_{Ci1Cj})$

α_{Ci2Cj} is the strength of dependency fraction between V_{Ci2} and V_{Cj} and $0 \leq \alpha_{Ci2Cj} \leq 1$

β_{Ci2Cj} is the criticality of dependency between V_{Ci2} and V_{Cj} and $0 \leq \beta_{Ci2Cj} \leq 100(1 - \alpha_{Ci2Cj})$

α_{Ii1Cj} is the strength of dependency fraction between V_{Ii1} and V_{Cj} and $0 \leq \alpha_{Ii1Cj} \leq 1$

β_{Ii1Cj} is the criticality of dependency between V_{Ii1} and V_{Cj} and $0 \leq \beta_{Ii1Cj} \leq 100(1 - \alpha_{Ii1Cj})$

α_{Ii2Cj} is the strength of dependency fraction between V_{Ii2} and V_{Cj} and $0 \leq \alpha_{Ii2Cj} \leq 1$

β_{Ii2Cj} is the criticality of dependency between V_{Ii2} and V_{Cj} and $0 \leq \beta_{Ii2Cj} \leq 100(1 - \alpha_{Ii2Cj})$

$$0 \leq V_{Ci1}, V_{Ci2}, V_{Cj} \leq 100$$

SE_{Ij} is self-efficiency of Integrity component of P_j and $0 \leq SE_{Ij} \leq 1$

α_{Ii1Ij} is the strength of dependency fraction between V_{Ii1} and V_{Ij} and $0 \leq \alpha_{Ii1Ij} \leq 1$

β_{Ii1Ij} is the criticality of dependency between V_{Ii1} and V_{Ij} and $0 \leq \beta_{Ii1Ij} \leq 100(1 - \alpha_{Ii1Ij})$

α_{Ii2Cj} is the strength of dependency fraction between V_{Ii2} and V_{Cj} and $0 \leq \alpha_{Ii2Cj} \leq 1$

β_{Ii2Cj} is the criticality of dependency between V_{Ii2} and V_{Cj} and $0 \leq \beta_{Ii2Cj} \leq 100(1 - \alpha_{Ii2Cj})$

$$0 \leq V_{Ii1}, V_{Ii2}, V_{Ij} \leq 100$$

SE_{Aj} is self-efficiency of Availability component of P_j and $0 \leq SE_{Aj} \leq 1$

α_{Ai1Aj} is the strength of dependency fraction between V_{Ai1} and V_{Aj} and $0 \leq \alpha_{Ai1Aj} \leq 1$

β_{Ai1Aj} is the criticality of dependency between V_{Ai1} and V_{Aj} and $0 \leq \beta_{Ai1Aj} \leq 100(1 - \alpha_{Ai1Aj})$

α_{Ai2Aj} is the strength of dependency fraction between V_{Ai2} and V_{Aj} and $0 \leq \alpha_{Ai2Aj} \leq 1$

β_{Ai2Aj} is the criticality of dependency between V_{Ai2} and V_{Aj} and $0 \leq \beta_{Ai2Aj} \leq 100(1 - \alpha_{Ai2Aj})$

α_{Ii1Aj} is the strength of dependency fraction between V_{Ii1} and V_{Aj} and $0 \leq \alpha_{Ii1Aj} \leq 1$

β_{Ii1Aj} is the criticality of dependency between V_{Ii1} and V_{Aj} and $0 \leq \beta_{Ii1Aj} \leq 100(1 - \alpha_{Ii1Aj})$

α_{Ii2Aj} is the strength of dependency fraction between V_{Ii2} and V_{Aj} and $0 \leq \alpha_{Ii2Aj} \leq 1$

β_{Ii2Aj} is the criticality of dependency between V_{Ii2} and V_{Aj} and $0 \leq \beta_{Ii2Aj} \leq 100(1 - \alpha_{Ii2Aj})$

$$0 \leq V_{Ai1}, V_{Ai2}, V_{Aj} \leq 100$$

4.5.4. OR Gate Integration

To increase resiliency of a critical cyber system, adding redundant components to the system is an established practice. A redundant server is a replica of the primary server with the

same (or sometimes similar) computing power, storage capacity, applications, etc. A redundant server is not active until the primary server fails. Once the primary server loses its operability, the redundant server becomes active and takes the responsibilities of the primary server to prevent system failure or downtime.

Dependency relationships of classical FDNA are not sufficient to model redundant nodes. A new concept – OR gate – is developed to expand the classical FDNA algebra to cover such situations (Figure 19).

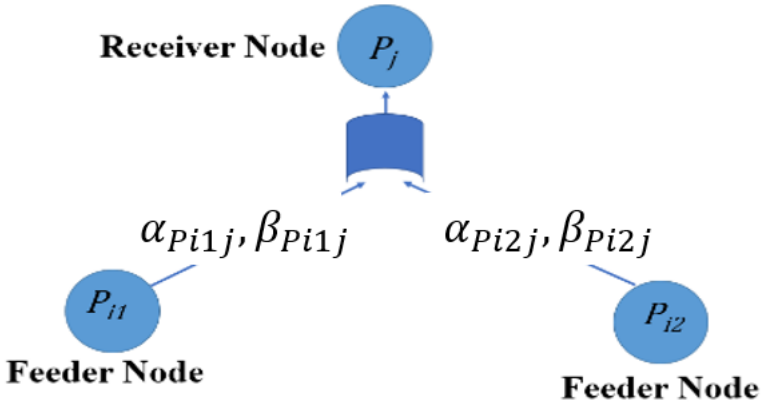


Figure 19. OR dependency of a 3-node FDNA graph

The FDNA-Cyber graph in Figure 19 consists of three nodes P_{i1}, $P_{i2,}$ *and* $P_{j.}$ The equations for operability level of the receiver node –P_j – are as follows.

$$P_j = SE_J(Max\left(Min\left(SODP_{ji1}, CODP_{ji1}\right), Min\left(SODP_{ji2}, CODP_{ji2}\right)\right))$$

$$\Rightarrow P_j = SE_j(Max\left(Min\left(\alpha_{P_{i1j}}P_{i1} + 100\left(1 - \alpha_{P_{i1j}}\right), P_{i1} + \beta_{P_{i1j}}\right), Min\left(\alpha_{P_{i2j}}P_{i2} + 100\left(1 - \alpha_{P_{i2j}}\right), P_{i2} + \beta_{P_{i2j}}\right)\right))$$

where SE_j is self-efficiency of of P_j and $0 \leq SE_j \leq 1$

α_{Pi1j} is the strength of dependency fraction between P_{i1} and P_j and $0 \leq \alpha_{Pi1j} \leq 1$

β_{Pi1j} is the criticality of dependency between P_{i1} and P_j and $0 \leq \beta_{Pi1j} \leq 100(1 - \alpha_{Pi1j})$

α_{Pi2j} is the strength of dependency fraction between P_{i2} and P_j and $0 \leq \alpha_{Pi2j} \leq 1$

β_{Pi2j} is the criticality of dependency between P_{i2} and P_j and $0 \leq \beta_{Pi2j} \leq 100(1 - \alpha_{Pi2j})$

To define the FDNA-Cyber algebra with AND gate, several FDNA-Cyber dependency equations are developed based on examples.

Example 6: Formulate the FDNA equations for the graph in Figure 20

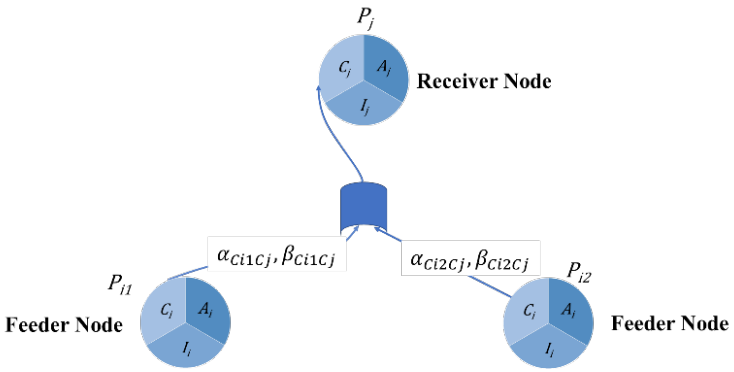


Figure 20. A 3-node FDNA-Cyber graph with OR gate dependency

The FDNA-Cyber graph in Figure 20 consists of three nodes P_i , $P_{i2,}$ *and* $P_{j..}$ The equations for operability level of each single node – P_{i1} , P_{i2} *and* P_j – without considering the dependencies are as follows.

$$P_{i1} = w_{Ci1}V_{Ci1} + w_{Ii1}V_{Ii1} + w_{Ai1}V_{Ai1}$$

$$P_{i2} = w_{Ci2}V_{Ci2} + w_{Ii2}V_{Ii2} + w_{Ai2}V_{Ai2}$$

$$P_j = w_{Cj}V_{Cj} + w_{Ij}V_{Ij} + w_{Aj}V_{Aj}$$

$$w_{Ci1} + w_{Ii1} + w_{Ai1} = 1$$

$$w_{Ci2} + w_{Ii2} + w_{Ai2} = 1$$

$$w_{Cj} + w_{Ij} + w_{Aj} = 1$$

$$V_{Ci1} = V_{Ci1}(X_{Ci1}), V_{Ii1} = V_{Ii1}(X_{Ii1}), V_{Ai1} = V_{Ai1}(X_{Ai1})$$

$$V_{Ci2} = V_{Ci2}(X_{Ci2}), V_{Ii2} = V_{Ii2}(X_{Ii2}), V_{Ai2} = V_{Ai2}(X_{Ai2}),$$

$$V_{Cj} = V_{Cj}(X_{Cj}), V_{Ij} = V_{Ij}(X_{Ij}), V_{Aj} = V_{Aj}(X_{Aj})$$

$$0 \leq V_{Ci1}, V_{Ii1}, V_{Ai1}, V_{Ci2}, V_{Ii2}, V_{Ai2}, V_{Cj}, V_{Ij}, V_{Aj} \leq 100$$

$$0 \leq P_{i1}, P_{i2}, P_j \leq 100$$

$$0 < \alpha_{Ci1Cj}, \alpha_{Ci2Cj} \leq 1\ , 0 \leq \beta_{Ci1Cj,}\beta_{Ci2Cj} \leq 100$$

The FDNA-Cyber dependency function for the graph in Figure 20 is given by the following equations.

$$V_{Cj} = SE_{Cj}(Max\left(Min(SODV_{CjCi1}, CODV_{CjCi1}), Min(SODV_{CjCi2}, CODV_{CjCi2})\right))$$

$$\Rightarrow V_{Cj} = SE_{Cj}(Max\left(Min(\alpha_{Ci1Cj}V_{Ci1} + 100(1 - \alpha_{Ci1Cj}), V_{Ci1} + \beta_{Ci1Cj}), Min(\alpha_{Ci2Cj}V_{Ci2} + 100(1 - \alpha_{Ci2Cj}), V_{Ci2} + \beta_{Ci2Cj})\right))$$

Where SE_{Cj} is self-efficiency of Confidentiality component of P_j and $0 \leq SE_{Cj} \leq 1$

α_{Ci1Cj} is the strength of dependency fraction between V_{Ci1} and V_{Cj} and $0 \leq \alpha_{Ci1Cj} \leq 1$

β_{Ci1Cj} is the criticality of dependency between V_{Ci1} and V_{Cj} and $0 \leq \beta_{Ci1Cj} \leq 100(1 - \alpha_{Ci1Cj})$

α_{Ci2Cj} is the strength of dependency fraction between V_{Ci2} and V_{Cj} and $0 \leq \alpha_{Ci2Cj} \leq 1$

β_{Ci2Cj} is the criticality of dependency between V_{Ci2} and V_{Cj} and $0 \leq \beta_{Ci2Cj} \leq 100(1 - \alpha_{Ci2Cj})$

$$0 \leq V_{Ci1}, V_{Ci2}, V_{Cj} \leq 100$$

Example 7: Formulate the FDNA equations for the graph in Figure 21

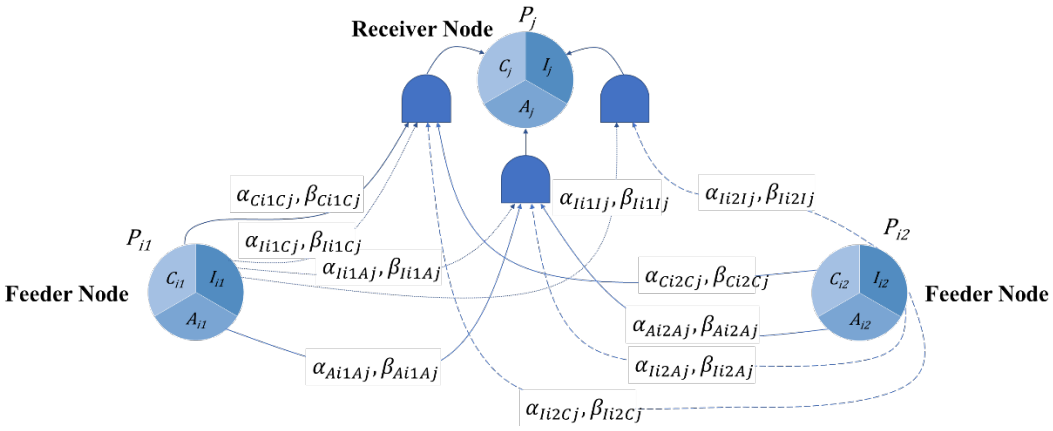


Figure 21. A 3-node FDNA-Cyber graph with OR gate dependency

The FDNA-Cyber graph in Figure 21 consists of three nodes P_i , $P_{i2,}$ *and* $P_{j..}$ The equations for operability level of each single node – P_{i1} , P_{i2} *and* P_j – without considering the dependencies are as follows.

$$P_{i1} = w_{Ci1}V_{Ci1} + w_{Ii1}V_{Ii1} + w_{Ai1}V_{Ai1}$$

$$P_{i2} = w_{Ci2}V_{Ci2} + w_{Ii2}V_{Ii2} + w_{Ai2}V_{Ai2}$$

$$P_j = w_{Cj}V_{Cj} + w_{Ij}V_{Ij} + w_{Aj}V_{Aj}$$

$$w_{Ci1} + w_{Ii1} + w_{Ai1} = 1$$

$$w_{Ci2} + w_{Ii2} + w_{Ai2} = 1$$

$$w_{Cj} + w_{Ij} + w_{Aj} = 1$$

$$V_{Ci1} = V_{Ci1}(X_{Ci1}), V_{Ii1} = V_{Ii1}(X_{Ii1}), V_{Ai1} = V_{Ai1}(X_{Ai1})$$

$$V_{Ci2} = V_{Ci2}(X_{Ci2}), V_{Ii2} = V_{Ii2}(X_{Ii2}), V_{Ai2} = V_{Ai2}(X_{Ai2}),$$

$$V_{Cj} = V_{Cj}(X_{Cj}), V_{Ij} = V_{Ij}(X_{Ij}), V_{Aj} = V_{Aj}(X_{Aj})$$

$$0 \leq V_{Ci1}, V_{Ii1}, V_{Ai1}, V_{Ci2}, V_{Ii2}, V_{Ai2}, V_{Cj}, V_{Ij}, V_{Aj} \leq 100$$

$$0 \leq P_{i1}, P_{i2}, P_j \leq 100$$

$$\forall\, X, Y \in \{C, I, A\}: 0 < \alpha_{Xi1Yj}, \alpha_{Xi2Yj} \leq 1\,, 0 \leq \beta_{Xi1Yj,}\beta_{Xi2Yj} \leq 100$$

The FDNA-Cyber dependency function for the graph in Figure 21 is given by the following equations.

$$V_{Cj} = SE_{Cj}(Max \begin{pmatrix} Min(SODV_{CjCi1}, CODV_{CjCi1}), \\ Min(SODV_{CjIi1}, CODV_{CjIi1}), \\ Min(SODV_{CjCi2}, CODV_{CjCi2}) \\ Min(SODV_{CjIi2}, CODV_{CjIi2}) \end{pmatrix})$$

⇨ $V_{Cj} = SE_{Cj}(Max\left(Min(\alpha_{Ci1Cj}V_{Ci1} + 100(1 - \alpha_{Ci1Cj}), V_{Ci1} + \beta_{Ci1Cj}), Min(\alpha_{Ii1Cj}V_{Ii1} + 100(1 - \alpha_{Ii1Cj}), V_{Ci2} + \beta_{Ci2Cj}), Min(\alpha_{Ci2Cj}V_{Ci2} + 100(1 - \alpha_{Ci2Cj}), V_{Ci2} + \beta_{Ci2Cj}), Min(\alpha_{Ii2Cj}V_{Ii2} + 100(1 - \alpha_{Ii2Ij}), V_{Ii2} + \beta_{Ii2Cj})\right))$

$$V_{Ij} = SE_{Ij}(Max\left(Min(SODV_{IjIi1}, CODV_{IjIi1}), Min(SODV_{IjIi2}, CODV_{IjIi2})\right))$$

⇨ $V_{Ij} = SE_{Ij}(Max\left(Min(\alpha_{Ii1Ij}V_{Ii1} + 100(1 - \alpha_{Ii1Ij}), V_{Ii1} + \beta_{Ii1Ij}), Min(\alpha_{Ii2Ij}V_{Ii2} + 100(1 - \alpha_{Ii2Ij}), V_{Ii2} + \beta_{Ii2Ij})\right))$

$$V_{Aj} = SE_{Aj}(Max\begin{pmatrix} Min(SODV_{AjAi1}, CODV_{AjAi1}), \\ Min(SODV_{AjIi1}, CODV_{AjIi1}), \\ Min(SODV_{AjAi2}, CODV_{AjAi2}), \\ Min(SODV_{AjIi2}, CODV_{AjIi2}) \end{pmatrix})$$

$$\Rightarrow V_{Aj} = SE_{Aj}(Max\Big(Min(\alpha_{Ai1Aj}V_{Ai1} + 100(1-\alpha_{Ai1Aj}), V_{Ai1} + \beta_{Ai1Aj}), Min(\alpha_{Ii1Aj}V_{Ii1} + 100(1-\alpha_{Ii1Aj}), V_{Ii1} + \beta_{Ii1Aj}), Min(\alpha_{Ai2Aj}V_{Ai2} + 100(1-\alpha_{Ai2Aj}), V_{Ai2} + \beta_{Ai2Aj}), Min(\alpha_{Ii2Aj}V_{Ii2} + 100(1-\alpha_{Ii2Aj}), V_{Ii2} + \beta_{Ii2Aj})\Big))$$

Where SE_{Cj} is self-efficiency of Confidentiality component of P_j and $0 \leq SE_{Cj} \leq 1$

α_{Ci1Cj} is the strength of dependency fraction between V_{Ci1} and V_{Cj} and $0 \leq \alpha_{Ci1Cj} \leq 1$

β_{Ci1Cj} is the criticality of dependency between V_{Ci1} and V_{Cj} and $0 \leq \beta_{Ci1Cj} \leq 100(1-\alpha_{Ci1Cj})$

α_{Ci2Cj} is the strength of dependency fraction between V_{Ci2} and V_{Cj} and $0 \leq \alpha_{Ci2Cj} \leq 1$

β_{Ci2Cj} is the criticality of dependency between V_{Ci2} and V_{Cj} and $0 \leq \beta_{Ci2Cj} \leq 100(1-\alpha_{Ci2Cj})$

α_{Ii1Cj} is the strength of dependency fraction between V_{Ii1} and V_{Cj} and $0 \leq \alpha_{Ii1Cj} \leq 1$

β_{Ii1Cj} is the criticality of dependency between V_{Ii1} and V_{Cj} and $0 \leq \beta_{Ii1Cj} \leq 100(1-\alpha_{Ii1Cj})$

α_{Ii2Cj} is the strength of dependency fraction between V_{Ii2} and V_{Cj} and $0 \leq \alpha_{Ii2Cj} \leq 1$

β_{Ii2Cj} is the criticality of dependency between V_{Ii2} and V_{Cj} and $0 \leq \beta_{Ii2Cj} \leq 100(1-\alpha_{Ii2Cj})$

$$0 \leq V_{Ci1}, V_{Ci2}, V_{Cj} \leq 100$$

SE_{Ij} is self-efficiency of Integrity component of P_j and $0 \leq SE_{Ij} \leq 1$

α_{Ii1Ij} is the strength of dependency fraction between V_{Ii1} and V_{Ij} and $0 \leq \alpha_{Ii1Ij} \leq 1$

β_{Ii1Ij} is the criticality of dependency between V_{Ii1} and V_{Ij} and $0 \leq \beta_{Ii1Ij} \leq 100(1-\alpha_{Ii1Ij})$

α_{Ii2Cj} is the strength of dependency fraction between V_{Ii2} and V_{Cj} and $0 \leq \alpha_{Ii2Cj} \leq 1$

β_{Ii2Cj} is the criticality of dependency between V_{Ii2} and V_{Cj} and $0 \leq \beta_{Ii2Cj} \leq 100(1 - \alpha_{Ii2Cj})$

$$0 \leq V_{Ii1}, V_{Ii2}, V_{Ij} \leq 100$$

SE_{Aj} is self-efficiency of Availability component of P_j and $0 \leq SE_{Aj} \leq 1$

α_{Ai1Aj} is the strength of dependency fraction between V_{Ai1} and V_{Aj} and $0 \leq \alpha_{Ai1Aj} \leq 1$

β_{Ai1Aj} is the criticality of dependency between V_{Ai1} and V_{Aj} and $0 \leq \beta_{Ai1Aj} \leq 100(1 - \alpha_{Ai1Aj})$

α_{Ai2Aj} is the strength of dependency fraction between V_{Ai2} and V_{Aj} and $0 \leq \alpha_{Ai2Aj} \leq 1$

β_{Ai2Aj} is the criticality of dependency between V_{Ai2} and V_{Aj} and $0 \leq \beta_{Ai2Aj} \leq 100(1 - \alpha_{Ai2Aj})$

α_{Ii1Aj} is the strength of dependency fraction between V_{Ii1} and V_{Aj} and $0 \leq \alpha_{Ii1Aj} \leq 1$

β_{Ii1Aj} is the criticality of dependency between V_{Ii1} and V_{Aj} and $0 \leq \beta_{Ii1Aj} \leq 100(1 - \alpha_{Ii1Aj})$

α_{Ii2Aj} is the strength of dependency fraction between V_{Ii2} and V_{Aj} and $0 \leq \alpha_{Ii2Aj} \leq 1$

β_{Ii2Aj} is the criticality of dependency between V_{Ii2} and V_{Aj} and $0 \leq \beta_{Ii2Aj} \leq 100(1 - \alpha_{Ii2Aj})$

$$0 \leq V_{Ai1}, V_{Ai2}, V_{Aj} \leq 100$$

4.5 Cost Calculation Model

4.5.1. Cost Factors for an Adverse Cyber Event

Economic cost of cyber actions is an important parameter for well-informed decisions and cyber risk bridging the communication gap between technical and senior level decision makers. Cost components of an adverse cyber event vary in terms of the magnitude of associated cost and difficulty in calculating the cost. According to the Council of Economic Advisors (2018), based on the previous studies by Federal Bureau of Investigation (2017), Verizon (2017), and the Open Web Application security Project (2014), there are 13 cost factors of an adverse cyber event: (1) Loss of IP, (2) Loss of strategic information, (3) Reputational damage, (4) Increased cost of capital, (5) Cybersecurity improvements, (6) Loss of data and equipment, (7) Loss of revenue, (8) Public

relations, (9) Regulatory penalties, (10) Customer protection, (11) Breach notification, (12) Court settlement fees, and (13) Forensics. The comparison of difficulty of quantifying cost and magnitude of cost is given in Figure 22.

A cyber-attack might cause some or all of the costs listed above. For instance, a distributed denial of service (DDoS) attack targeting an online retail company causes disruption of operability of the IT systems and business processes. First, in the short term, the company loses sales during the disruption. In the mid-run, the company loses its future revenue since some of the customers switch to another company in the market because of the unavailability of the service. According to the magnitude of the attack, there may exist reputational damage, which may "tarnish the firm's brand name, reducing its future revenues and business opportunities" (Council of Economic Advisors (2018). To reduce the impact of reputational damage, the company should pay public relations efforts to mitigate this damage.

Another scenario is the costs incurred because of an Advanced Persistent Threat (APT) attack targeting the intellectual property and strategic information of a company. The company loses its competitive advantage because of the stolen intellectual property and strategic information. The stolen intellectual property might be owned and utilized by the company's rivals. The company loses it future revenue. To find the attacker, the company spends on forensics to identify the perpetrator, and court settlement fees. The cost of capital, which "is the required return necessary to make a capital budgeting project … and is used by companies internally to judge whether a capital project is worth the expenditure of resources, and by investors who use it to determine whether an investment is worth the risk compared to the return" (Kenton, 2018), also

increases since the investors think the company did not protect the intellectual property adequately (Council of Economic Advisors (2018).

In the case of a data breach of a personally identifiable information (PII) of customers or employees of a company might result regulatory penalties, breach notification and customer protection costs. A ransomware attack might result loss of data. For all the scenarios listed above, the attacked company needs to invest in cybersecurity to mitigate the cyber risks and reduce vulnerabilities to prevent re-occurring of a similar cyber incident.

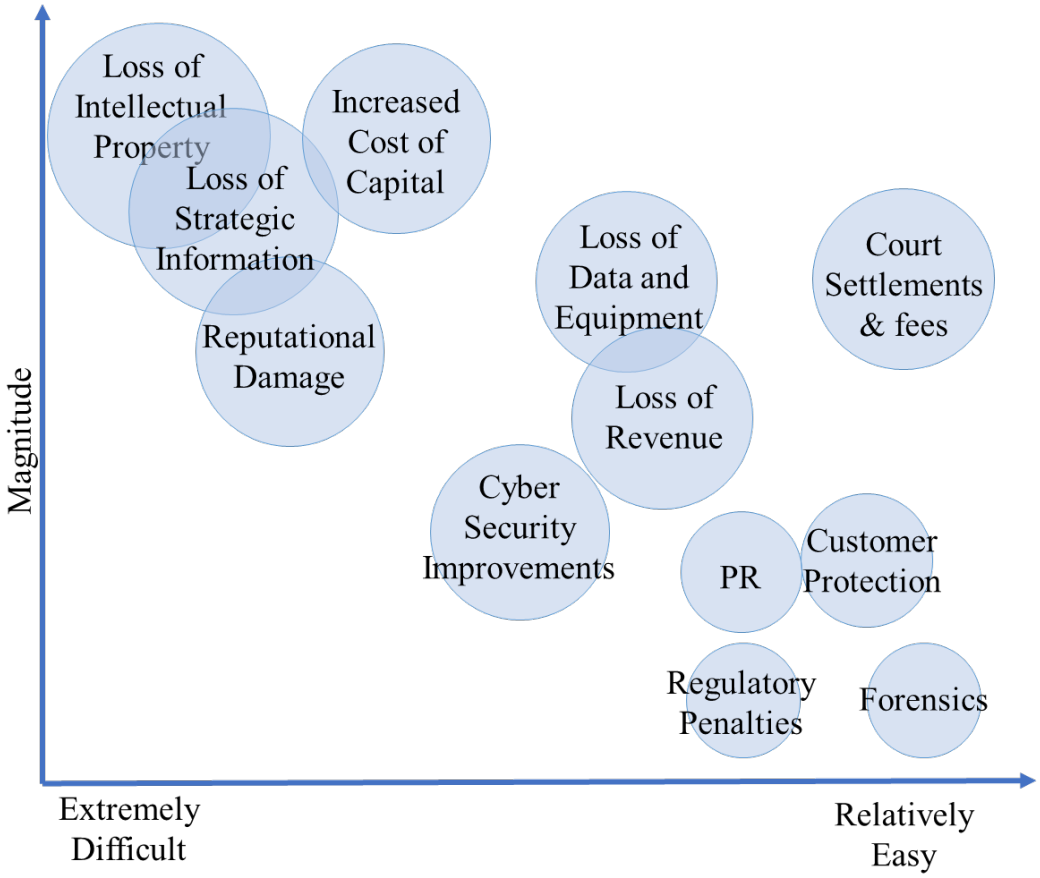


Figure 22. Cost factors of an adverse cyber event (Adapted from Council of Economic Advisors (2018))

4.5.2. Impact of Time and Duration to Cyber Cost

The impact of a cyber-attack is related to the value of the targeted asset, service and business process. The value of each of these factors might differ. For example, the costs of loss of availability of an online retail system during business hours and hours from 2 am to 5 pm are different. The duration is also an important factor of incurred cost of a cyber-incident. The duration of a cyber-attack impacts the attack's magnitude. For instance, if a DDoS attack lasts days, the associated costs (i.e. loss of revenue, loss of reputation etc.) will be higher than a similar attack that lasts hours.

The cost of a cyber-action should be a function of time and duration of the attack.

4.5.3. Case Study: Economic Impact of a DDoS Attack Targeting a Higher Education Institute

In this section, a case study of DDoS attack targeting a higher education institute is discussed to demonstrate the importance of time and duration in calculating economic impact of a cyber incident. Parts of this section have been previously published as (Keskin, Tatar, et al., 2018).

4.5.3.1. Background of Online Learning at Higher Education Institutes

Traditionally, higher education is held in classrooms with professors lecturing to students. In the last few decades, this has been changing in some degree with the synchronous and asynchronous (e.g., CD-ROM) distance learning education methods. Before the wide use of the internet, institutes employed televised delivery methods via satellites for the synchronous distance learning. Later, this approach was almost completely abandoned and the internet has become the platform for distance learning courses. The reasons why higher education institutes have started offering their courses and programs online are to reach more students and increase their tuition

income. Many higher education institutes offer distance learning degrees or at least some distance learning courses. According to the U.S. Department of Education, National Center for Education Statistics (2016), “In fall 2014, there were 5,750,417 students enrolled in any distance education courses at degree-granting postsecondary institutions.”

Distance learning programs help to deliver higher education to anyone who has an internet connection anywhere in the world. However, distance learning highly depends on the internet. Quality of the classes is easily affected by low bandwidth and unreliable internet service. The bandwidth issue is attributed more to the student end. However, the reliability of internet service is much more important at the university end. Given that the universities that provide distance learning have the internet infrastructure to provide a sufficiently good quality stream, no problems are expected. Nevertheless, parallel to the developments in the internet and technology, cyber attacks are also eveloved over time. Universities are among the top targets of the Distributed Denial-of-Service (DDOS) attacks (Cloudbric, 2017; McMurdie, 2017), which result in business interruption. As well, according to the researchers at Akamai Technologies, U.S. colleges and universities are facing an increase in DDoS attacks (Walker, 2017).

In this study, an economics based framework to calculate the economic impact of DDoS attacks is developed. The framework is applied to a distance learning system of a higher education institute.

4.5.3.2. Research Problem

Distance learning programs have become popular. However, distance learning requires continuous, high quality internet connection. This step into cyberspace also comes with the risk of cyber attacks. DDoS attacks can disrupt course delivery and cause financial consequences. Decision makers in the university management need a method to choose the best risk mitigation

strategy to withstand the impact of DDoS attacks. Accordingly, the research question is: *"How to calculate the economic impact of business interruption caused by DDoS attacks targeting a distance learning infrastructure?"*

Quantifying cybersecurity risk in monetary values would help make better decisions while choosing a risk mitigation strategy. There are several methods of cybersecurity risk mitigation: risk control (i.e. reducing the consequence or likelihood), risk acceptance, risk avoidance, and risk transferal (Pinto & Garvey, 2012). This approach will also increase temporal accuracy in acquisition roadmaps, precision on requirements management and effective financial planning.

1.5.3.2.1. Model

In this study, a model to support decision making for choosing risk mitigation strategies is developed. Decision makers need to define methods to predict the possible cost of risk events. The model depends on the predicted Cost of Impact of a DDoS attack. Based on the magnitude of the cost, the model helps to choose different strategies based on The Mitigation Strategy Selection Algorithm is shown in Figure 23.

Condition 1: When the Cost of Impact ($Imp) is less than or equal to the sum of Insurance Deductible ($Ded) and Premium ($Prm), then decision makers should consider accepting the risk since the impact is negligible.

Condition 2: While Condition 1 is False, if the sum of Insurance Deductible ($Ded), Premium ($Prm) and the difference between Cost of Impact ($Imp) and Insurance Coverage ($Cov) is less than the Cost of Control ($Ctl), then the decision makers should consider transferring

the risk. Since the Cost of Impact ($Imp) is too much to accept but not high enough to exceed the Cost of Control, transferring the risk is the best option in this situation.

Condition 3: If both Condition 1 and 2 are False, the decision makers should consider choosing the risk control strategy. Because the Cost of Impact is too much to be accepted and also too much from the insurance coverage amount, the best option is to control risk.

For this model, risk avoidance is not an appropriate risk mitigation strategy since it is assumed that the higher education institute is determined to continue offering distance learning programs.

```
IF $Imp ≤ $Ded + $Prm
    Strategy = Accept
ELSE
    IF $Ded + $Prm + $Imp – $Cov ≤ $Ctl
        Strategy = Transfer
    ELSE
        Strategy = Control
    ENDIF
ENDIF
```

Figure 23. The Mitigation Strategy Selection Algorithm

Predicting the Cost of impact is an integral part of this model. It depends on the direct impact and indirect impact as shown in Equation 1.

$$\$I: Cost\ of\ Impact = f(Direct\ Impact, Indirect\ Impact) \quad (1)$$

The *Indirect Impact* includes the cost of reputation damage, legal procedures, productivity decline, customer turnover, personnel time spent addressing and recovering from the outage and incremental helpdesk expenses (Arbor Networks, 2016; Granidello et. al, 2016). Estimating the

Indirect Impact is harder. Some methods could be developed to estimate the factors that constitute the *Indirect Impact*. For instance, in the distance learning systems, the cost of reputation basically depends on the enrollment along years and is affected by the reputation of the distance learning programs of the higher education institute. Because of the scarcity of data to quantify the *Indirect Impact*, it is out of the scope of this study.

In this study, a model is proposed to gauge the *Direct Impact*. The higher education institutes do not loss money directly when a DDoS attack occurs when compared to an online store or gambling site. However, they need a way of calculating the value of the online service availability. As shown in the Equation 2, *Direct Impact* can be calculated as a function of the duration of the DDoS attack and the number of students who are connected to the distance learning program during this time period.

$$Direct\ Impact = f(DDoS\ Duration, Number\ of\ Students) \quad (2)$$

DDoS duration can be a couple of minutes or may go up to days. The number of connected students depends on the number and type of the courses held during this period (See the Equation 3). Graduate and undergraduate courses typically have a different number of enrolled students and different tuition rates.

$$Number\ of\ Students = f(Number\ of\ Courses, Type\ of\ Courses) \quad (3)$$

Number and type of the courses depend on the course schedule. Hence, the day of the week and the time of the day as shown in the Equation 4.

$$Number\ of\ Courses = f(Day\ of\ the\ Week, Time\ of\ the\ Day) \quad (4)$$

4.5.3.3. Application of the model on distance learning data

The model is applied to real-world data from Old Dominion University distance learning system.

4.5.3.3.1. Data collection and preparation

Schedule data of distance learning courses in Spring 2017 term is used. Based on Equation 4, Number of Courses depend on the Day of the Week and the Time of the Day. Figure 1 illustrates equation 4 by representing the number of courses offered on each day. There are no courses on weekends and in the late hours; therefore, these hours are not included in the plot.

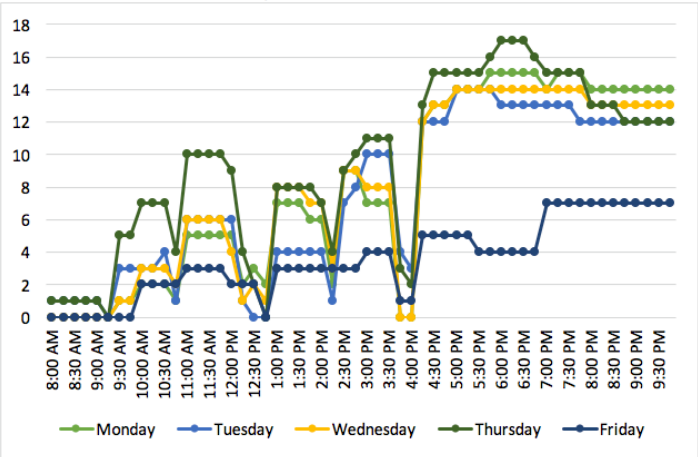


Figure 24. Total number of distance learning courses for each day

In addition to the course schedule, data for enrollment, tuition rates, and domicile is included in the study. Based on the Equation 3, the type of the courses is also needed. The tuition

rates are different for undergraduate and graduate students. It also differs based on domicile. Commonly, out-of-state students pay more tuition than in-state students (See Table 4).

Table 4. Data for domicile, tuition rates, and types of courses

Domicile	Level	Tuition Rates	Domicile
In-state Students	Undergraduate	$325	91.48%
Out-of-State Students	Undergraduate	$355	8.52%
In-state Students	Graduate	$478	74.39%
Out-of-State Students	Graduate	$516	25.61%

Based on the enrollment data, total student credit hours registered to distance learning courses for this semester are 52,200 for undergraduate and 11,388 for graduate level. A course requires 3 credit hours. There are 81 undergraduate, 76 graduate courses, and 27 courses for both undergraduate and graduate levels. Based on these numbers, the average value of a 15-minute period for one course is $1,250.71 for undergraduate level and $428.98 for graduate level. Based on the data given above, the value of streaming for 15-minute periods for each day is visualized in Figure 25. This figure shows the direct impact values (mentioned in the Equation 2) for these time periods without considering the duration of the DDoS attacks.

Figure 2 and Figure 3 have some similarities and differences.

Similarities:

- Trends for each day are similar at each graph. If there is no course within a period of time, the dollar value is also zero (e.g. Wednesday, 3.45 pm; Friday, 8.30 am).
- When the plot in either figures peaks, the related plot in the other figure also reaches a peak (e.g. Thursday, 6 pm).

Differences:

- The vertical axis represents the number of courses in Figure 2 while it stands for the dollar value of each 15-minute-period in Figure 3.
- The graphs in Figure 3 have higher values before 4 pm. This is because most of the undergraduate courses are held until 4 pm and these courses have many more enrolled students on average than the graduate courses. This increases their value even if the tuition rates for the undergraduate level are lower.

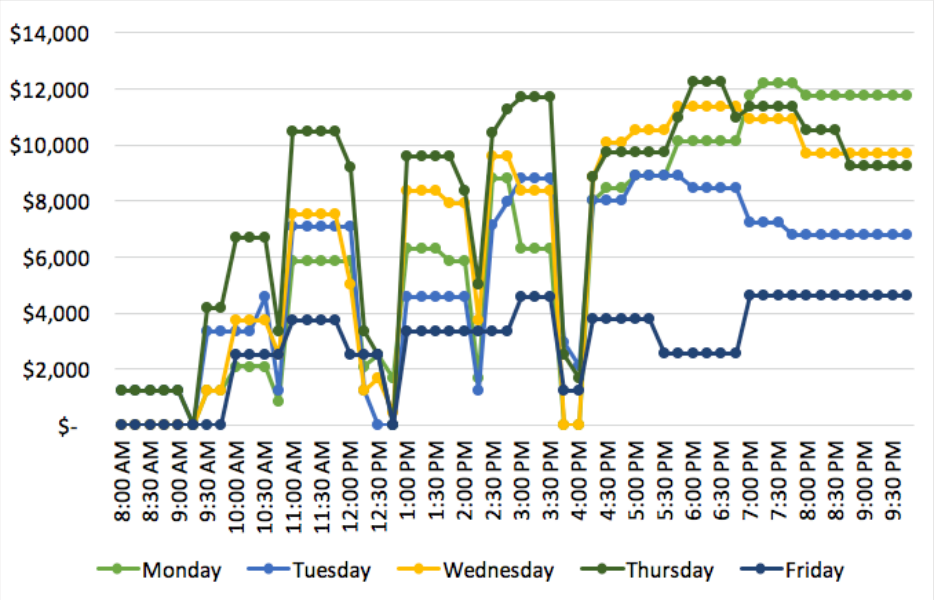


Figure 25. Value of Stream for 15-minute periods for each day (Direct impact without duration information)

The *Direct impact* in Equation 2 is calculated using the duration of the DDoS attack and the number of students. Figure 25 is not a cumulative plot. It gives the value of each specific 15-minute period of service interruption. DDoS attacks commonly last hours or, in some cases, days.

In order to calculate the direct impact of the DDoS attack, the point values given in Figure 25 should be cumulatively added.

For example, the direct impact of a DDoS attack with a duration of 12 hours that occurs on Monday between, 10 am and 10 pm is $355,955. This value is calculated by cumulatively adding 48 data points within this time period. Table 5 presents direct impact values for 12-hour DDoS attacks. Rows specify the start time and the columns specify the day of the week. (+1) in rows indicates that this attack ends on the succeeding day. Darker shading of cells indicates the higher impact. Thus, it can be said that the highest impact of a 12-hour DDoS can be reached if it starts on a Thursday morning at 10 am.

Table 5. 12-hour DDoS attack impact

Start - End Times	Monday	Tuesday	Wednesday	Thursday	Friday
10AM - 10PM	$355,955	$309,128	$382,232	$447,081	$165,449
1PM - 1AM (+1)	$313,340	$246,950	$327,593	$352,094	$132,931
4PM - 4AM (+1)	$244,618	$178,300	$238,576	$241,029	$91,174
7PM - 7AM (+1)	$142,381	$82,782	$121,227	$123,264	$55,756

Another representation of the values in Table 5 is provided in Figure 26 as a three-dimensional surface plot. Vertical axes represent the attack start day and time while vertical axis stands for the direct impact. It can be seen that the highest impact value for a 12-hour DDoS is reached by an attack that starts on Thursday morning. It can be observed that attacks starting in the afternoon have less impact since there are no classes at night.

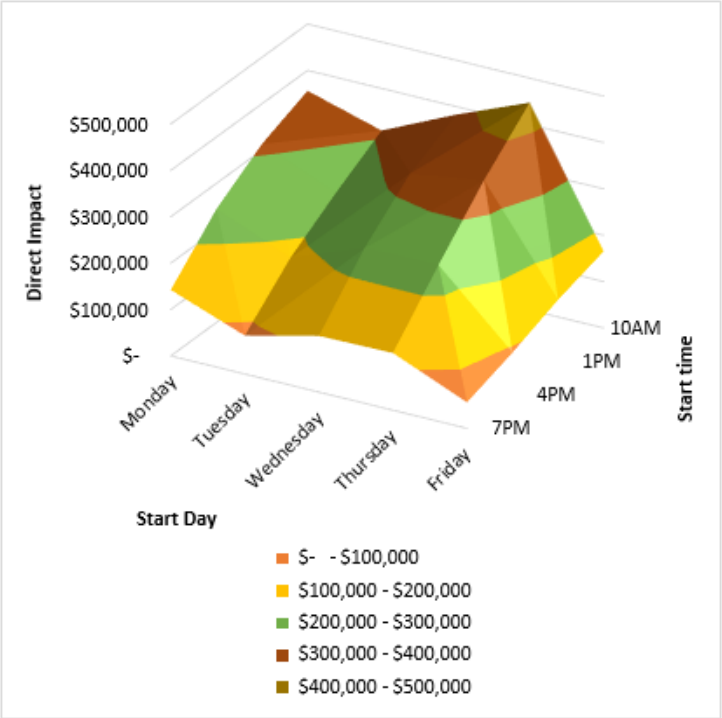


Figure 26. Direct impact of a 12-hour DDoS attack

Figure 27 depicts the direct impact values for 72-hour DDoS attacks. The highest impact, which is almost $M 1.16, is reached by the attack that starts on Monday at 7 pm because this attack includes the highest demand hours. The impact has lower values for later days of the week since the attack covers the weekend.

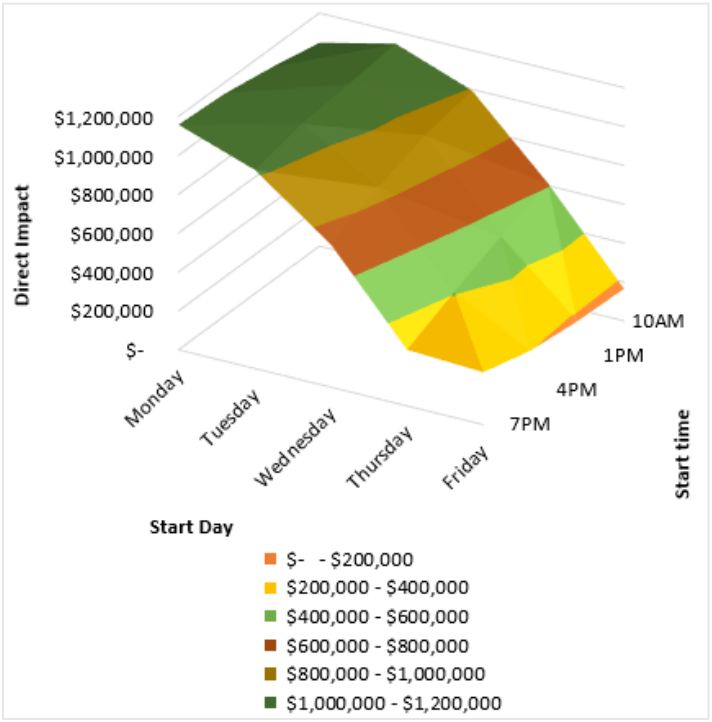


Figure 27. Direct impact of a 72-hour DDoS attack

4.5.3.3.2. Simulation results

To conduct a simulation, the attack is considered to start on Monday at 8 am. Figure 28 represents the Cost of Impact and costs of different risk mitigation strategies. One can compare these functions and choose the best strategy based on the risk tolerance of the organization by using this model and plotting the costs.

For this simulation, the insurance coverage is designated as one million dollars. For simplicity, the deductible and premium amounts are designated as %10 and 1/200 of the coverage, respectively (Skinner, 2017). The average risk control strategy cost is designated as $240,000 (Cdwg, 2017) (See Table 6).

Table 6. Risk Mitigation Strategy Costs

Strategy		Cost
Transfer	Coverage ($Cov)	$ 1,000,000
	Deductible ($Ded)	$ 100,000
	Premium ($Prm)	$ 5,000
Control	Control ($Ctl)	$ 240,000

4.5.3.3.2.1. Risk acceptance

Accepting the risk is basically not taking any precaution. Therefore, the cost of DDoS attack when the risk is accepted is equal to the Cost of Impact. In Figure 28, orange line represents this value. The attack starts on Monday morning and it continues. Cost of Impact increases while there are distance learning courses and stands constantly when there is no class, e.g. during nights. The dollar value for an end time t is the total cost if the attack lasts until the time t. This is applicable to all three risk mitigation strategies.

4.5.3.3.2.2. Risk control

Risk control means taking precaution to decrease the consequence of risk event. In this study, it is considered to acquire a product that prevents the DDoS attack to interrupt online services. In Figure 28, yellow straight line represents the Cost of Control. It is constant since the organization pays its cost in the beginning. It doesn't increase because it prevents an attack to happen. Thus, there is no additional Cost of Impact.

4.5.3.3.2.3. Risk transfer

Transferring the risk is buying an insurance coverage. The organization pays the Premium in the beginning. If an attack occurs, based on the Cost of Impact, the insurance company pays the

cost, or the insured organization pays the deductible. In Figure 28, orange line represents these values cumulatively.

If the Cost of Impact exceeds the Deductible but not the Coverage amount, insured pays only the deductible.

If the cost of Impact exceeds the Coverage amount, the insured organization pays the deductible and the uncovered amount, which is equal to the difference between the Cost of Impact and Coverage.

In Figure 28, the gray line represents the cost that is paid by the insured higher education institute. It starts at $5,000, which is the Premium amount, at the beginning. It increases while the Cost of Impact increases until it reaches the value of the sum of Deductible and Premium. When the Cost of Impact reaches the Coverage amount, which is $1M, it again starts increasing at the same rate that the Cost of Impact increases (After the blue dashed line).

4.5.3.3.2.4. Comparison of risk mitigation strategies

The main goal of this approach is to minimize the cost to the higher education institute. In Figure 28, red stars indicate the important points that the best risk mitigation strategy changes. These stars indicate the IF conditions satisfaction values in the model algorithm provided in Figure 23.

From Monday, 8 am to 3:15 pm, the lowest cost values are provided by risk acceptance strategy. At 3:15 pm, the Cost of Impact ($107,509) exceeds the Cost of Transfer ($105,000), which is equal to the sum of Premium and Deductible. Before this point, the minimum cost to the institute is received by accepting the risk. If the organization doesn’t expect a DDoS attack more than 7 hours and 15 minutes, the decision makers would consider taking no action against the DDoS threat.

From Monday, 3:15 pm to Thursday, 2:15 pm, i.e. between two red stars, risk transferal is the best strategy. If the organization expects an attack more than 7 hours and 15 minutes up to 78 hours and 15 minutes, the decision makers should consider buying a million-dollar insurance coverage. Buying a risk control product is still not a good practice for this situation due to its high cost.

If the organization expects an attack that may last more than 78 hours and 15 minutes, the decision makers should consider choosing the risk control strategy and buying the product for $240,000 because after Thursday, 2:15 pm, other strategies cause higher costs to the institution.

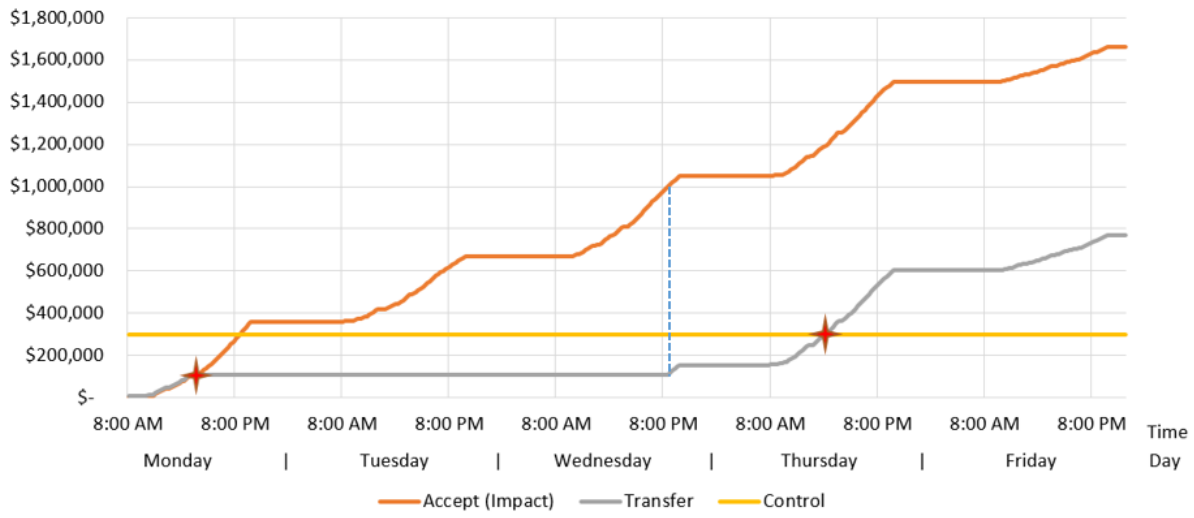


Figure 28. Cost of Impact and Mitigation Strategies

4.5.3.4. Limitations

This study has several limitations. First, different types of DDoS attacks, the bandwidth of the target system and attack size (in Gb/sec) are not considered. It is assumed that the DDoS attack is successful and just results in business interruption. Second, only the cost of service loss is used

to quantify the monetary value of business interruption. The factors that constitute *Indirect Impact* such as legal procedures, help desk costs, and reputation loss are ignored. Also, business interruption of the university's other online services is ignored since they do not have a significant impact.

4.5.3.5. Conclusions

This study develops an economic framework to distinguish economic viability among different risk mitigation strategies against DDoS in distance learning systems of higher education institutes. Publicly available data is used to apply the framework on a real world case. This framework may apply to other cybersecurity incidents (e.g. ransomware) resulting to business interruption. This framework shows that the risk mitigation strategy selection depends on many aspects. The amount of insurance coverage can affect the effectiveness of risk transfer strategy. One of the most important things to know is the likelihood of a long duration DDoS attack to happen. Decision makers should consider these aspects to occur with the most viable solution. Future work will include availability of other online services, such as website access, web applications, and archived courses. It will also include indirect impact factors that are not considered in this study.

4.5.4. Formula for Calculating Cost of a Cyber Action

Economic impact of a cyber action is calculated based on the loss of confidentiality, integrity and availability at the business process level. For each potential cost identified by the Council of Economic Advisors (2018), relevant potential cost factors are identified (Table 7).

Table 7. Relation of potential consequences and cost factors (confidentiality, integrity and availability)

	Cost Factors			
Potential Consequences	**C**	**I**	**A**	**Parameter**
Loss of IP	X			Ct_1
Loss of Strategic Information	X	X	X	Ct_2
Reputational Damage	X	X	X	Ct_3
Increased Cost of Capital	X			Ct_4
Cybersecurity Improvements	X	X	X	Ct_5
Loss of data and Equipment	X	X	X	Ct_6
Loss of Revenue	X	X	X	Ct_7
PR	X	X	X	Ct_8
Regulatory Penalties	X	X	X	Ct_9
Customer Protection	X			Ct_{10}
Breach Notifications	X			Ct_{11}
Court Settlement Fees	X	X	X	Ct_{12}
Forensics	X	X	X	Ct_{13}

Time and duration are also used as parameters in cost calculation.

The economic cost calculation formulas are given below.

$$Cost\ (BP_1) = f(\left(C_{BP_1}, t, d\right), \left(I_{BP_1}, t, d\right), \left(A_{BP_1}, t, d\right))$$

$$C_{BP_1} = g(Ct_1, Ct_2, Ct_3, Ct_4, Ct_5, Ct_6, Ct_7, Ct_8, Ct_9, Ct_{10}, Ct_{11}, Ct_{12}, Ct_{13})$$

$$I_{BP_1} = g(Ct_2, Ct_3, , Ct_5, Ct_6, Ct_7, Ct_8, Ct_9, Ct_{12}, Ct_{13})$$

$$A_{BP_1} = g(Ct_2, Ct_3, , Ct_5, Ct_6, Ct_7, Ct_8, Ct_9, Ct_{12}, Ct_{13})$$

$$TOTAL\ COST = \sum_{k=1}^{n} Cost(BP_k)$$

where C_{BP_1} is the cost of loss of confidentiality for BP_1,

I_{BP_1} is the cost of loss of integrity for BP_1,

A_{BP_1} is the cost of loss of availability for BP_1,

t is the time when impact of cyber action is observed,

d is the duration of cyber action.

CHAPTER 5

RESULTS AND ANALYSIS

5.1 Introduction

In this chapter, the FDNA-Cyber methodology is applied in several hypothetical cases. In these cases, the network topology in Figure 29 is used. The dependency data (i.e., SOD, COD etc.) is generated in Microsoft Excel.

5.2 Case 1: Impact Propagation and Cost Calculation

5.2.1 Build a simple 3-tier network to compare cost and impact difference as per the attacked asset(s)

In order to conduct analyses and show the capabilities of the model proposed, a simple 3-tier network is built. The sample network consists of fifteen assets, seven services, five tasks, and four business processes (See Figure 29). Six of the assets are root nodes meaning that they do not have any dependency on any other node. Two of the business processes are leaf nodes, which don't have any child node. All other nodes have dependency on at least one node and at least one dependent node.

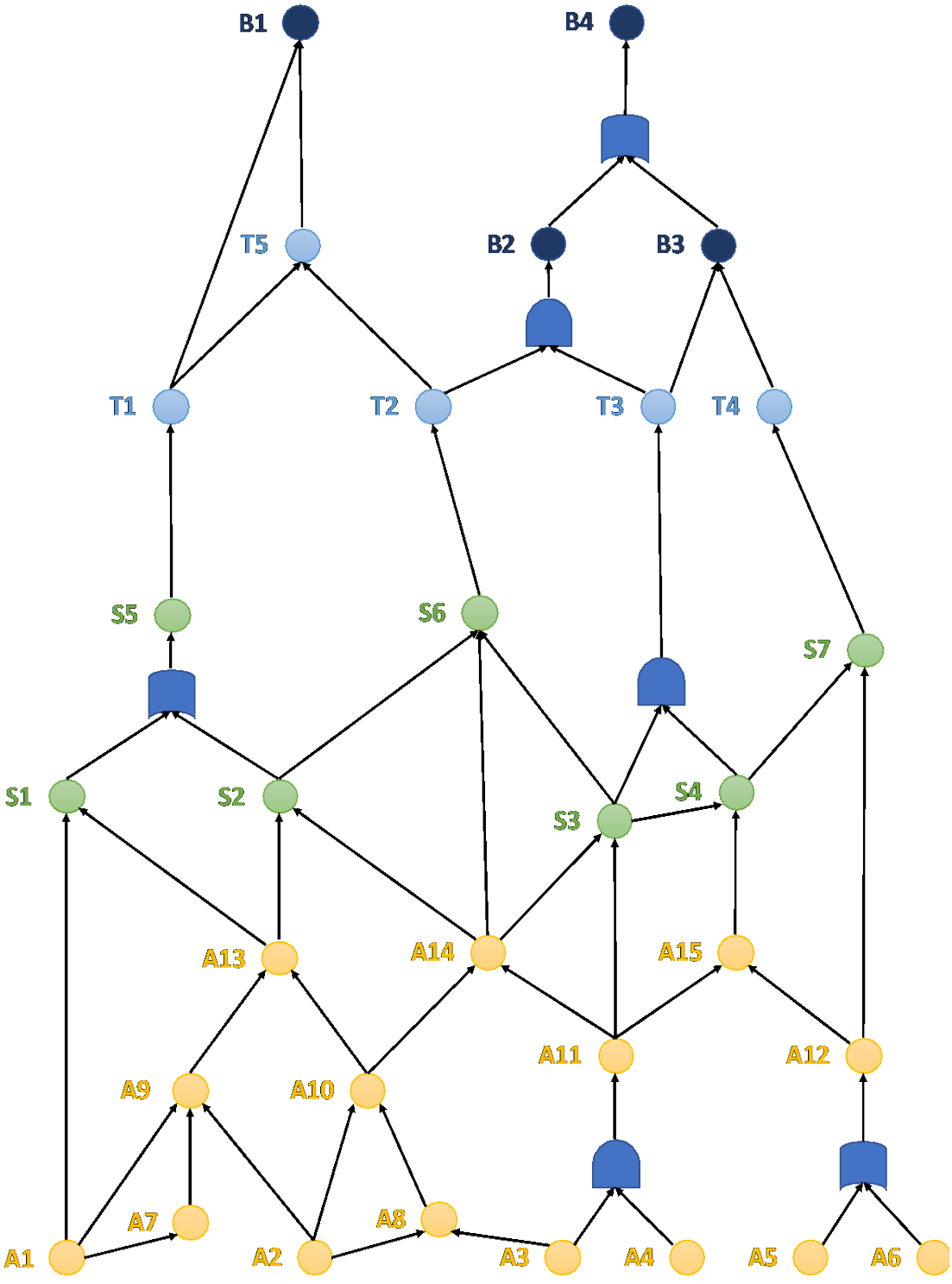


Figure 29. Sample 3-tier enterprise network

The inputs of the model are:

1. Network topology (dependency structure),
2. Asset Self Effectiveness,
3. Alpha and Beta values for each dependency relationship,
4. Time of the day that an attack starts and duration of the attack,
5. Weights of CIA values on the operability of a node
6. Cost values for each potential consequence for CIA.

The outputs of the model are:

1. CIA values of each node,
2. Operability of each node,
3. Cost of not continuing the operation of Business Processes.

During the analyses, as an input, the Self Effectiveness values of asset nodes are given. All of the other inputs have been kept constant for simplicity. All alpha values are kept as 1 meaning that there is a high strength of dependency among nodes. All beta values are kept as 50, thus there is a moderate criticality of dependency among nodes. Cost values are generated randomly within

5.2.2 List effected assets/services/task/business processes

The first analysis that is conducted lists which nodes are affected when an asset is degraded to zero Self Effectiveness. As shown in Table 8, when Asset 1 has a zero Self Effectiveness, Asset (A) 7, A9, A13, Service (S) 1, S2, S5, S6, Task (T) 1, T2, T5, Business Process (B) 1, and B2 are affected. This means that operability of these nodes are degraded from 100 and not working at a full capacity anymore. As can be seen here, when A5 or A6 degraded to zero, it doesn't affect any other nodes since A12 has an OR dependency on these two nodes. In this case, even if either of

them fails, the other one and A12 would still operate normally. Therefore, the OR dependency is a good way of providing redundancy.

Table 8. List of affected nodes when each asset is degraded to zero one by one

A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15
A7	A8	A8	A11			A9	A10	A13	A13	A14	A15	S1	S2	S4
A9	A9	A10	A14			A13	A13	S1	A14	A15	S4	S2	S3	S7
A13	A10	A11	A15			S1	A14	S2	S1	S2	S7	S5	S4	T3
S1	A13	A13	S2			S2	S1	S5	S2	S3	T3	S6	S6	T4
S2	A14	A14	S3			S5	S2	S6	S3	S4	T4	T1	S7	B2
S5	S1	A15	S4			S6	S3	T1	S4	S6	B2	T2	T2	B3
S6	S2	S1	S6			T1	S4	T2	S5	S7	B3	T5	T3	B4
T1	S3	S2	S7			T2	S5	T5	S6	T2	B4	B1	T4	
T2	S4	S3	T2			T5	S6	B1	S7	T3		B2	T5	
T5	S5	S4	T3			B1	S7	B2	T1	T4			B1	
B1	S6	S5	T4			B2	T1		T2	T5			B2	
B2	S7	S6	T5				T2		T3	B1			B3	
	T1	S7	B1				T3		T4	B2			B4	
	T2	T1	B2				T4		T5	B3				
	T3	T2	B3				T5		B1	B4				
	T4	T3	B4				B1		B2					
	T5	T4					B2		B3					
	B1	T5					B3		B4					
	B2	B1					B4							
	B3	B2												
	B4	B3												
		B4												

5.2.3 Cost graph for B1-4

After listing the nodes affected by degradation of the assets, the cost of not operating is computed for each asset's degraded scenario. The only nodes that directly cause cost are Business Processes. All the other nodes indirectly affect cost through the dependencies. Figure 30 presents the total cost and individual costs caused by each business process when each asset is degraded to zero. The horizontal axis represents the Asset that is degraded to zero starting with the case that no asset is degraded and then goes up from Asset 1 to Asset 15. Stacked columns represent the total cost while they are separated by colors to indicate the proportions that are caused by specific Business Processes.

As it can be seen from Figure 30, A5 and A6 do not cause any cost. This situation is in alignment with Table 8. Most of the scenarios cause less than $15 million. A3, A4, and A11 cause the most at almost $24 million.

t_i = 2 (Thursday) d_i = 1.07 (7.29 days)

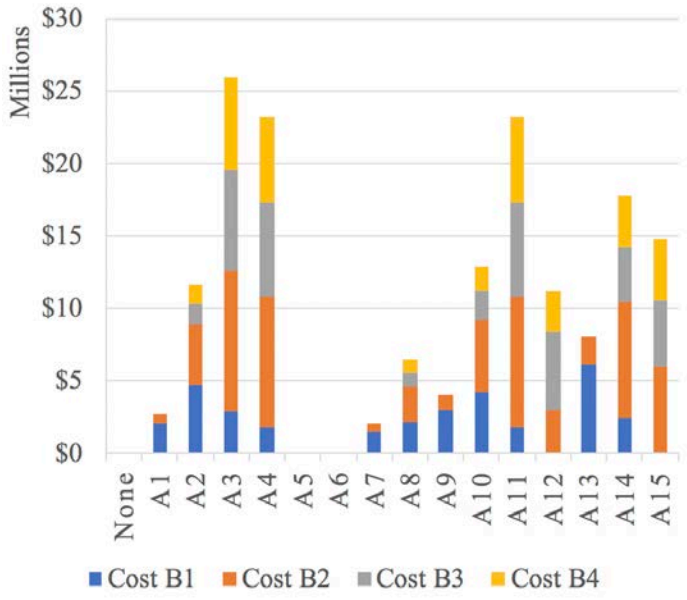


Figure 30. Total cost caused by each failed asset

Figure 31 also shows the total costs caused by degrading the assets one by one. The difference is that it represents the cost related to confidentiality, integrity, and availability portions of the Business Process nodes. Since there are more types of sources of cost for confidentiality than integrity and availability, costs regarding confidentiality are generally more than the others.

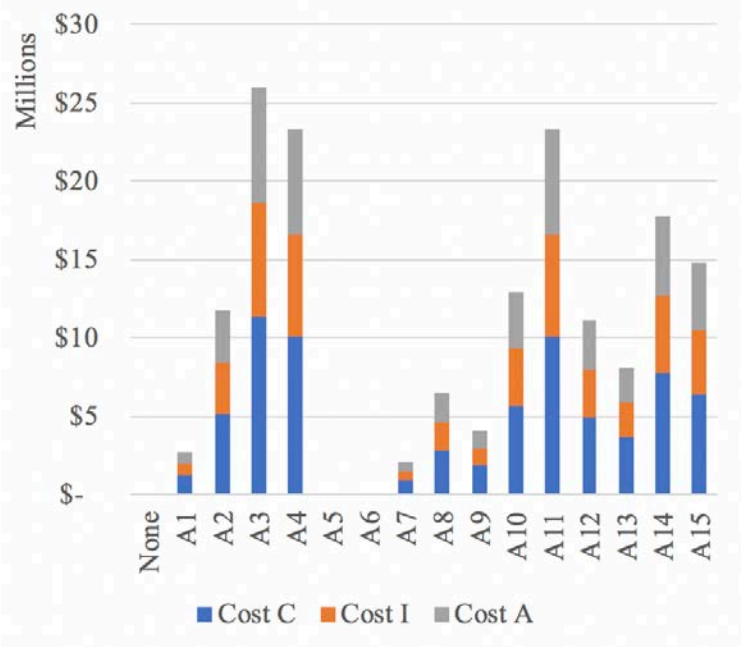


Figure 31. Total costs caused by CIA

5.2.4 Time/Duration impact

According to the cost equation below, cost of losses for Business operations depends on the time the event causing the loss starts and duration it continues since when an attack starts and how long it continues change its effect. In this simulation, t_i is related to the day of the week and determined according to randomly selected day. t_i is 3 for an attack that starts on Monday and

Tuesday, 2 for an attack that starts on Wednesday, Thursday, and Friday, and 1 for an attack that starts on Saturday and Sunday.

$$Cost\ (BP_1) = f((C_{BP_1}, t, d), (I_{BP_1}, t, d), (A_{BP_1}, t, d))$$

d_i is a decimal number between 1 and 1.3. The simulation assigns a random number from 0 to 30 to indicate the days that the attack continues. It computes the d_i based on this number by interpolation.

For the calculations for Figure 2 and 3, t_i is equal to 2 (Thursday) and d_i is equal to 1.07 (7.29 days). In order to show the effect of time and duration, the analysis shown in Figure 32 is conducted with t_i = 3 (Tuesday) d_i = 1.2 (18.42) day. As it can be observed in this graph, most of the total cost values are below $25 million while three of them are close to $40 million. This is because the time and duration factors are higher in the latter scenario.

In order to make comparison simple, t_i and d_i are kept constant for the all other analyses as equal to 2 (Thursday) and 1.07 (7.29 days), respectively.

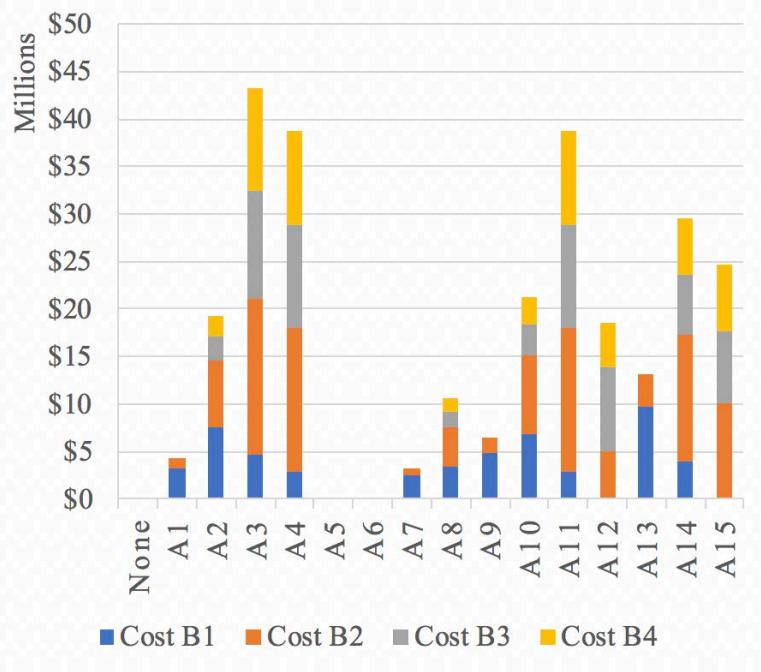


Figure 32. Total cost caused by each failed asset with a different time and duration

5.3 Case 2: Redundancy – Resiliency

5.3.1 Most critical asset analysis

Based on the dependency structure of the network, some nodes are considered more critical than others. There may be multiple measures to determine which nodes are critical. These measures may be the number of nodes whose operability levels have been degraded and the total cost they cause when they are degraded.

Determining the critical assets is an important action for decision makers within enterprises. This information is crucial to making investment decisions for risk mitigation strategies.

5.3.1.1 Find most critical asset(s) (i.e. asset(s) having most impact) for each BP

5.3.1.1.1 Most critical assets in terms of causing loss of operability

Figure 33 presents the cumulative degradation amounts of operability values of each Business Process. Each column is retrieved by giving a zero Self Effectiveness value to each asset and keeping others at 100, one by one, as similar to the previous analyses. In this network, there are four Business Process nodes. This graph presents the how many of the total of 400 utils (operability) of these four nodes are degraded in total. According to this figure, A3 is the most critical asset with the highest number, 215. A4, and A11 follows A3 with 193.

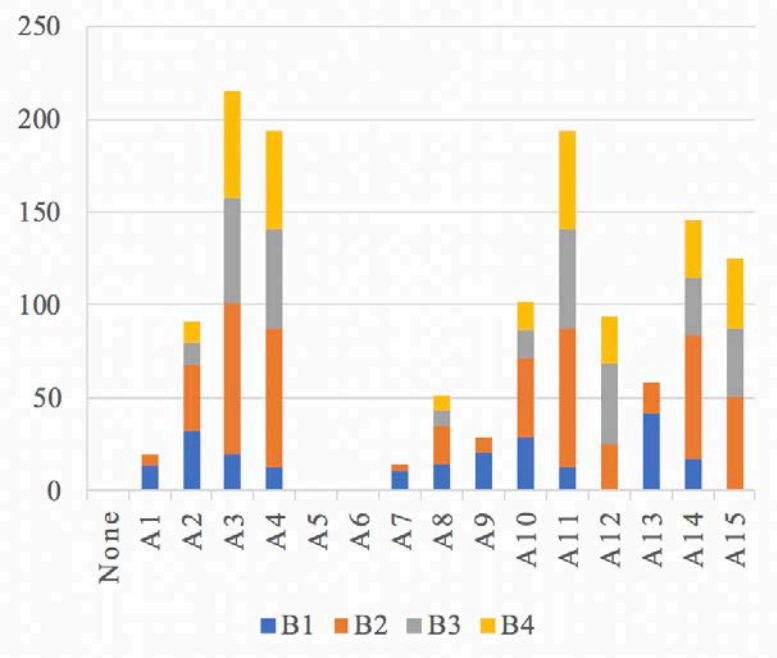


Figure 33. Cumulative performance degradation of business process nodes caused by each failed asset

5.3.1.1.2 Most critical assets in terms of causing cost of loss

Another way to measure the criticality of the assets is comparing costs. According to Figure 30, Figure 31, and Table 9, degradation of Asset 3 to zero Self Effectiveness causes the highest cost, more than $26 million. A4 and A11 follow A3 with almost $23 million while all the others fall below $18 million. Therefore, A3 is the most critical asset according the cost of loss it causes when it fails.

Table 9. Business Process costs caused by degradation of each asset

Zero-	Cost B1	Cost B2	Cost B3	Cost B4	TOTAL COST
A1	$ 2,027,731	$ 663,844	$ -	$ -	$ 2,691,575
A2	$ 4,717,250	$ 4,236,642	$ 1,435,217	$ 1,315,801	$ 11,704,910
A3	$ 2,891,123	$ 9,718,441	$ 6,986,804	$ 6,408,210	$ 26,004,580
A4	$ 1,826,126	$ 8,970,869	$ 6,508,399	$ 5,968,861	$ 23,274,255
A5	$ -	$ -	$ -	$ -	$ -
A6	$ -	$ -	$ -	$ -	$ -
A7	$ 1,521,529	$ 498,780	$ -	$ -	$ 2,020,309
A8	$ 2,129,994	$ 2,491,509	$ 956,811	$ 877,575	$ 6,455,890
A9	$ 3,043,057	$ 996,365	$ -	$ -	$ 4,039,422
A10	$ 4,260,718	$ 4,984,215	$ 1,914,235	$ 1,755,151	$ 12,914,319
A11	$ 1,826,126	$ 8,970,869	$ 6,508,399	$ 5,968,861	$ 23,274,255
A12	$ -	$ 2,990,290	$ 5,359,858	$ 2,809,140	$ 11,159,288
A13	$ 6,086,845	$ 1,993,925	$ -	$ -	$ 8,080,770
A14	$ 2,434,592	$ 7,974,504	$ 3,828,470	$ 3,511,425	$ 17,748,991
A15	$ -	$ 5,980,579	$ 4,594,164	$ 4,213,710	$ 14,788,453

5.3.1.2 Scenarios where assets are randomly degraded

Other scenarios have been analyzed where groups of two or three randomly selected assets fails at the same time. Figure 34 presents the cost caused by these scenarios. As it can be observed, as more assets fail, more cost increases. While the largest cost is almost $24 million for the scenarios that only one asset fails, it can be seen that the effect is more significant and reach more than $42 million when Assets 1, 2, and 3 fail at the same time. Another implication of this figure is that the first scenario in which A2 and A9 fail, Costs related to Business Processes 3 and 4, are lower than 1 and 2.

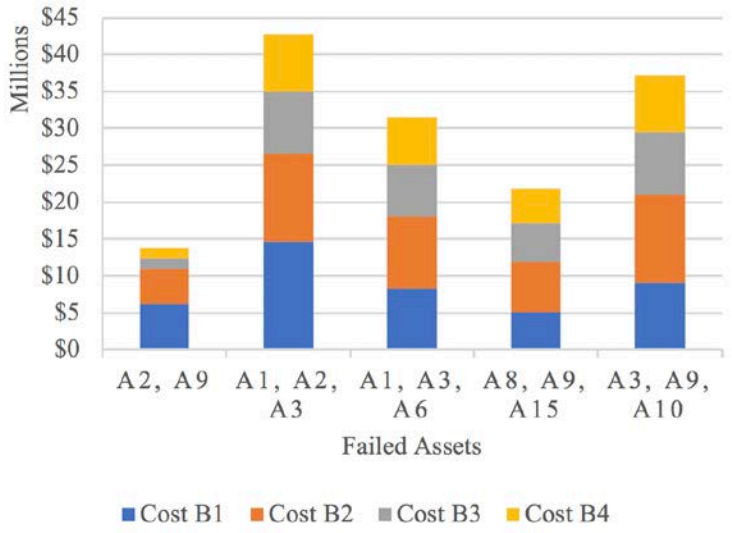


Figure 34. Total cost caused by each failed group of assets

5.3.2 Assess the impact of adding redundancy on resiliency

5.3.2.1 Add a redundant asset (i.e. an asset with the same functionality with OR gate)

In order to mitigate the risk associated with critical assets, a redundant node was added to function as the original node does. In this case, even if the original node fails for some reason internally or externally, the redundant node would continue its function and the dependent nodes' operability would not be affected.

The OR gate is used to add redundant nodes since it is the appropriate dependency type for this purpose. In a scenario below, a redundant node added to Asset 3, which is the most critical asset, and then in another scenario, redundancy is added for A1. The results are compared

5.3.2.2 Add to A3 (A3.1 and A3.2)

In this scenario, a redundant node is added to the most critical node, A3, as shown in Figure 35. It is added with an OR gate.

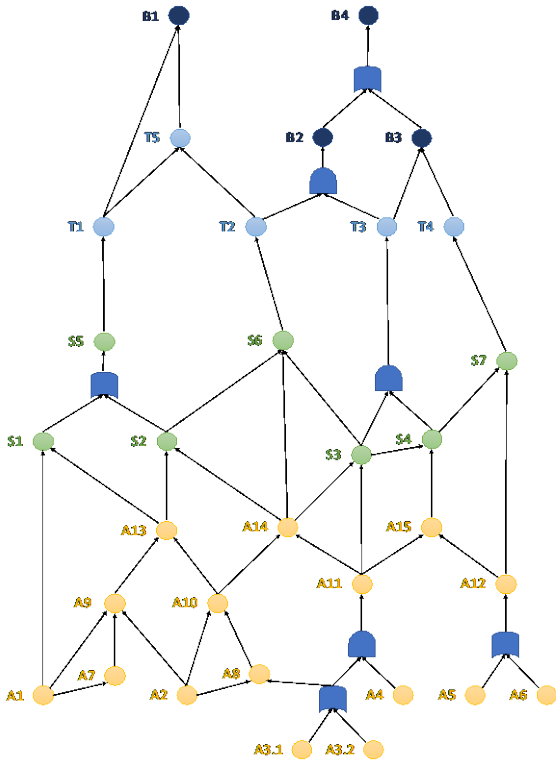


Figure 35. Modified network with redundancy added for A3

The same analysis is conducted to compute the effect of degrading the nodes to zero to the total cost. According to the results presented in Table 10 when either of the original or redundant node's Self Effectiveness is degraded to zero and all other nodes are kept at 100% operability, the Business Processes are not affected, and this causes no cost.

Table 10. Effect of adding a redundant node for A3 on total cost

Zero-	Cost B1	Cost B2	Cost B3	Cost B4	TOTAL COST
A3	$ 2,891,123	$ 9,718,441	$ 6,986,804	$ 6,408,210	$ 26,004,580
A3.1	$ -	$ -	$ -	$ -	$ -
A3.2	$ -	$ -	$ -	$ -	$ -

5.3.2.3 Add to A1 (A1.1 and A1.2)

In another scenario, a redundant node is added to another node, A1, as shown in Figure 36. It is added with an OR gate.

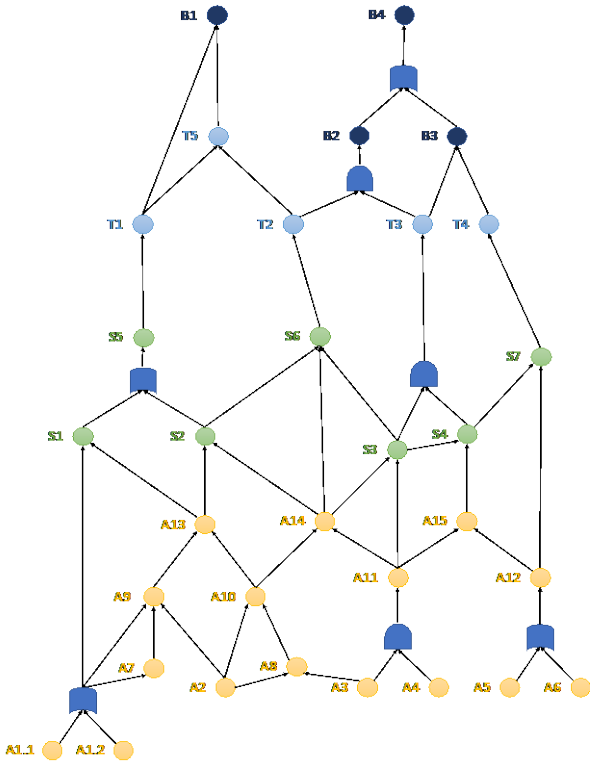


Figure 36. Modified network with redundancy added for A1

The same analysis is conducted to compute the effect of degrading the nodes to zero to the total cost. According to the results presented in Table 10 when either of the original or redundant node's Self Effectiveness is degraded to zero and all other nodes are kept at 100% operability, it does not affect the Business Processes and causes no cost.

When the same analysis is conducted, again, it is shown that after a redundant node is added to the topology, it does not affect the total cost only if the original and the redundant node do not fail simultaneously.

Table 11. Effect of adding a redundant node for A1 on total cost

Zero-	Cost B1	Cost B2	Cost B3	Cost B4	TOTAL COST
A1	$ 2,027,731	$ 663,844	$ -	$ -	$ 2,691,575
A1.1	$ -	$ -	$ -	$ -	$ -
A1.2	$ -	$ -	$ -	$ -	$ -

5.3.2.4 Compare the impact of adding a redundant node to A3 and A1

The results of these two scenarios are also shown in Figure 37 in comparison to the other scenarios. It can be implied that adding a redundant node to A3 reduces the risk significantly, and this could be an important investment for decision makers to consider.

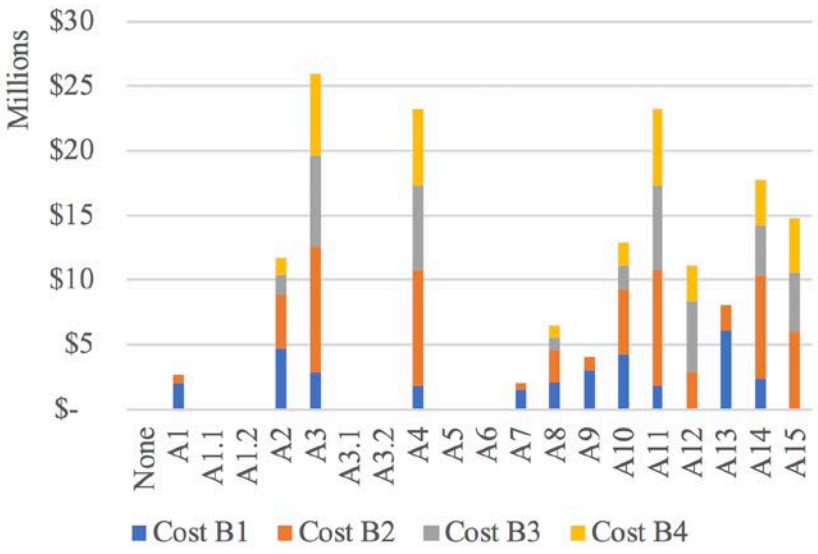


Figure 37. Total cost caused by each failed asset and redundant nodes

5.4 Case 3: Compare impact (cost) of attack and security/infrastructure investment scenarios

5.4.1 Change system configuration (add a redundant node)

As it is shown in Case 2, adding a redundant asset node to the network can be helpful to eliminate the criticality of a node since even the original asset fails the redundant asset still would be working. The probability of two systems fail simultaneously is lower than the probability of one of these systems to fail. This is apparent, but adding one more node costs, and decision makers need to make sure the investment would be beneficial. Suppose that adding one more node to the network costs $1 million. If the decision makers can analyze the network and find a node that if it fails, it would cost more than the cost of adding a replicate of it. Failure of Asset 3 costs more than 26 million dollars. In this case, if another system that would continue working and providing the functionality of Asset 3, its benefit would be that much. Therefore, investing $1 million to add such a system to the network would be highly beneficial.

5.4.2 Buy a security tool to prevent attack (Anti-virus, Host Based IDS etc.)

Redundancy is not the only way to diminish the cost of loss. There are also ways to improve the reliability of the assets and reduce their vulnerabilities. Cybersecurity tools, such as Anti-virus programs may prevent an attack from happening or reduce the effect of an attack and keep operability of the asset above zero. Although partially degraded operability of an asset is not ideal, it is better than having the asset completely lost. Moreover, these tools would cost less than adding a redundant node from the investment point of view.

Suppose that the enterprise considers buying a security tool that would decrease the amount of degradation when an attack happens. In this scenario, by investing $200K to an improvement, an asset will not degrade from 100 utils to 0, instead it will degrade to 50.

Based on the results presented in Figure 38, investing in A3 and A4 returns well and the total costs are divided almost in half. Total cost by A3 reduces from more than $25 million to almost $13 million and Total cost by A4 reduces from almost $23 million to $12 million.

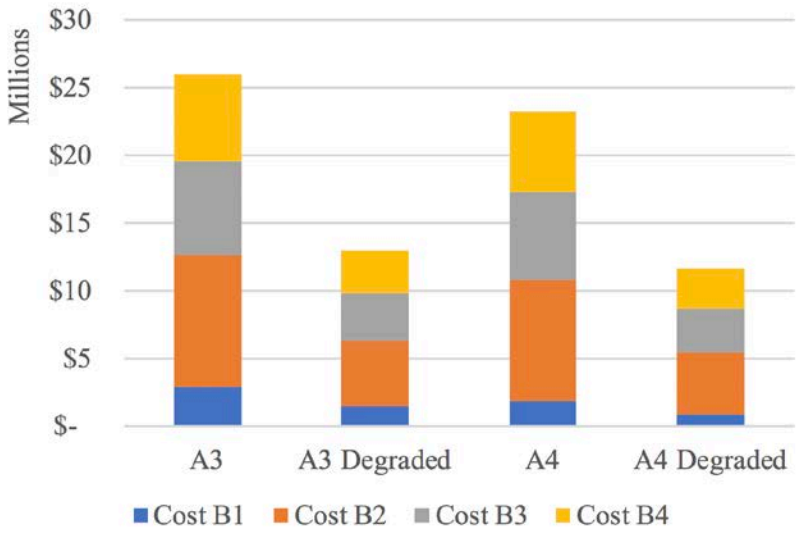


Figure 38. Total cost caused by partially degraded assets in comparison with the full degradation scenarios

5.4.3 Comparison of mitigation strategies

The different approaches to risk mitigation allow us to select the most suitable solution for the network. It may be useful to be able to choose the appropriate method to mitigate the dependency risks of the specific critical nodes. Figure 39 presents the total costs of different scenarios, such as some specific assets are kept original, some redundancy added, or partially degraded with the employment of the security tools. As it can be observed, the original scenarios cost the largest amount. Degraded versions decrease the cost almost to the half. And redundancy resolves the issue. However, these scenarios only include situations where one asset failed at a time.

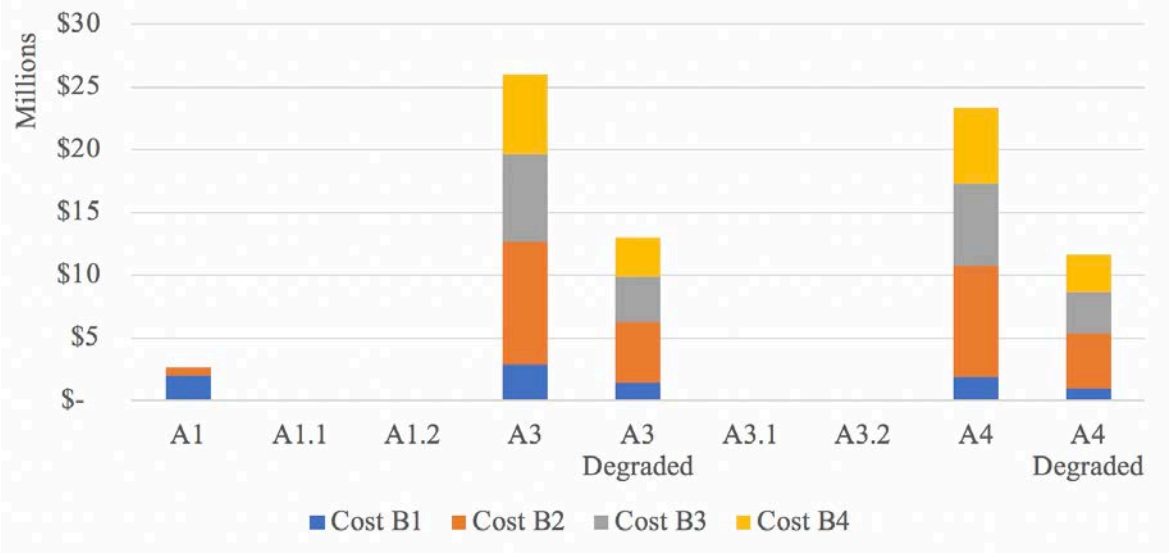


Figure 39. Total cost caused by partially degraded assets in comparison with the redundancy scenarios

The same scenarios are also compared in Figure 40 from the perspective of confidentiality, integrity, and availability values. The general picture does not change in this graph since the average degradation cost for confidentiality is slightly higher than integrity and availability and their weights are kept constant during the analyses to make the comparison easier.

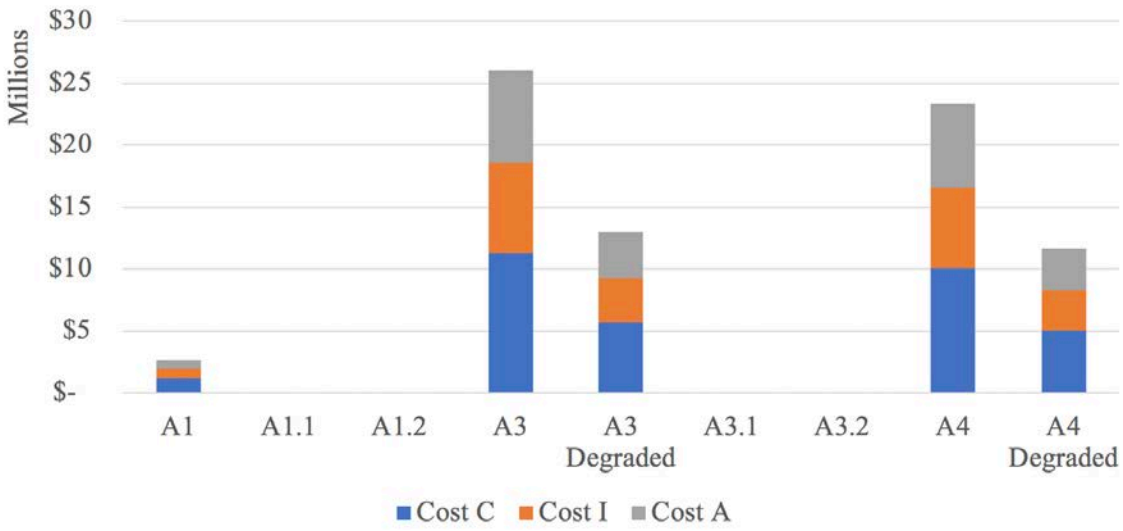


Figure 40. Total cost caused by partially degraded assets in comparison with the redundancy scenarios with regards to CIA values

5.5 Case 4: Risk Management Decision Making

5.5.1 Risk management decision making

Different approaches to risk mitigation exist, and when it is combined with the large number of nodes and the dependency relations of the network topology, it becomes more complicated to find the best way to manage the risks of the enterprise network. There are four main strategies to manage the risks: risk acceptance, risk avoidance, risk control, and risk transfer.

5.5.1.1 Risk acceptance

Risk acceptance means that any consequences caused by the risk event are accepted. Therefore, no precaution is taken in this strategy. No investment is necessary to implement this strategy but possibly the consequences would be higher than other strategies.

5.5.1.2 Risk avoidance

The risk avoidance strategy is abandoning business processes that cause the risk. This strategy can be a good option for outdated processes, but it is not considered in this simulation as an option.

5.5.1.3 Risk control

Risk control is a strategy where some investment is done to take an action to reduce the risk by reducing either the likelihood or the impact of the risk event. This requires analyses and investment to be conducted but since the risk is reduced, there is a probability that the investment returns sooner or later. In this simulation the risk control methods are as follows:

1. Buy a security tool to prevent attack (Anti-virus, Host Based IDS, etc.)
2. Change system configuration (add a redundant node)

5.5.1.4 Risk transfer (insurance)

Transferring the risk is the last risk management strategy where the consequences of the risk event are transferred to another organization with some conditions.

For this simulation, suppose that the enterprise is considering acquiring cyber insurance coverage. The intended amount for the cyber insurance to cover is $20 million. The deductible amount for this coverage is $2 million and the annual premium is $100,000.

5.5.2 Scenarios for risk management strategies

The scenarios to compare risk management strategies include a gradually propagated failure starting from no failed nodes and goes to the complete failure of the network. One more asset is failed at each consecutive scenario.

5.5.2.1 Risk acceptance

Figure 41 presents the total cost caused as a result of selection risk acceptance strategy. It starts with zero cost when there is no failed asset. There is no investment to mitigate the risks. There is no increase when A4 is added to the failed assets group since A11 has an AND dependency on A3 and A4. When A3 is already failed, there is no need for A4 to fail to effect A11, since it is already affected at a maximum rate.

There is also no increase in cost when A5 fails in addition to the other nodes since A12 has an OR dependency on A5 and A6, meaning that unless both of them fail, A12 is not affected.

The total cost in this strategy goes up to almost $50 million.

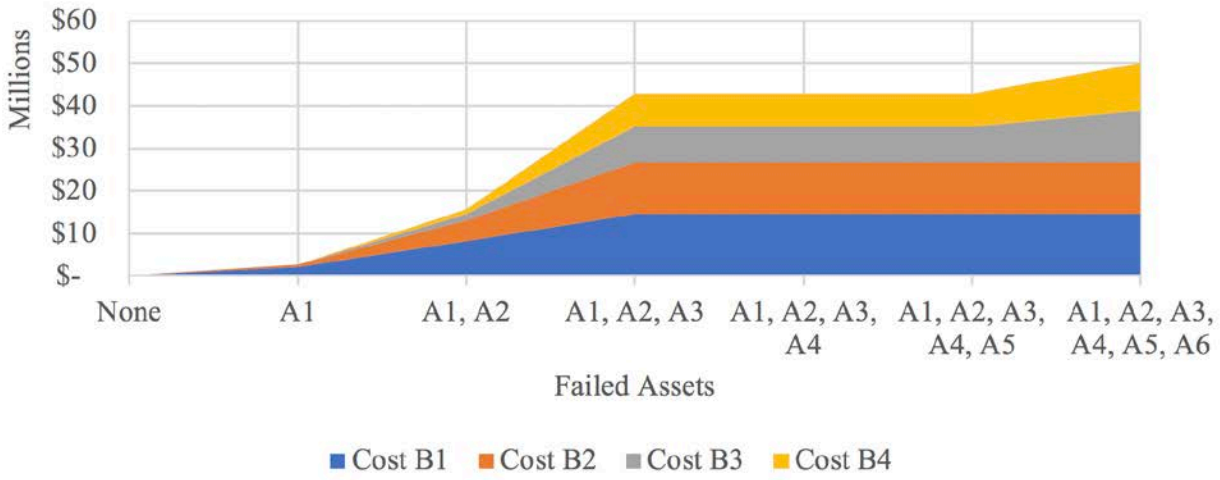


Figure 41. Total costs for risk acceptance strategy

5.5.2.2 Risk control

The risk control strategy for this simulation includes buying a security tool for Asset 2 and Asset 4 and implementing redundancy for Asset 3. Therefore, in the scenario, Self Effectiveness

of A2 and A4 degrades from 100 to 50 rather than 100 to 0 as for the other nodes. Also, when the original node A3.1 fails, the redundant node A3.2 continues working, and they are connected with an OR gate as conducted in Figure 35.

The investment of a security tool for two nodes is $400,000 in total, and cost to add a redundant node is $500,000. Thus, there is a total investment amount of $900,000 even if no node failed as it can be observed in Figure 42.

Failure of A3.1 does not affect the cost as explained, and it can be observed in Figure 42. The total cost for this strategy is almost $31 million, $19 million less than the risk acceptance strategy.

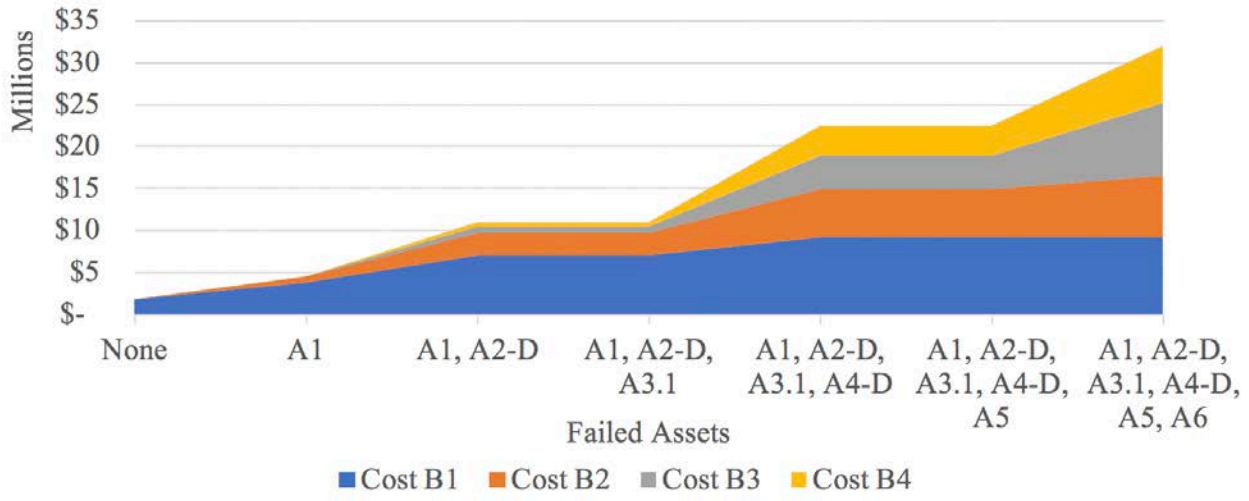


Figure 42. Total costs for risk control strategy

5.5.2.3 Risk transfer

For this simulation, cyber insurance coverage is $20 million. The deductible amount is $2 million, and the annual premium is $100,000. Therefore, any cost up to $2 million is paid by the

enterprise; after that, any amount up to $20 million is covered by the insurance company. Any number above this is again paid by the enterprise. The total cost can be seen in Figure 43 with a gray line.

5.5.2.4 Risk control and risk transfer

As a final strategy for the simulation, risk control and risk transfer methods are combined and used simultaneously. The same precautions are made before the analysis starts, and the same coverage is applied when any cost occurred. The total cost can be seen in Figure 43 with a yellow line.

5.5.3 Comparison of risk management strategies

All risk management strategies are summarized and presented in Figure 43. At first glance, it is easy to indicate that the risk acceptance strategy causes significantly larger cost in most scenarios. If there is no risk of failure, it would be the best strategy, but this is almost never the case since there is commonly some risk events. The reason costs for other strategies are more than zero is that there is an investment amount or insurance premium paid in advance.

For the first two scenarios where only A1 failed and both A1 and A2 failed, the risk transfer strategy is the best since the insurance covers most of the losses. If the decision makers predict failure propagation among the network would not get further, they would need to consider getting insurance coverage. The difference is at least $5 million from other strategies' costs.

Other scenarios where three or more of the nodes are failed because of the propagation causes more cost for all strategies. The risk control and transfer strategy is the best strategy for this kind of big scale attack. It causes almost $2 million less than the risk control strategy for each scenario at this scale.

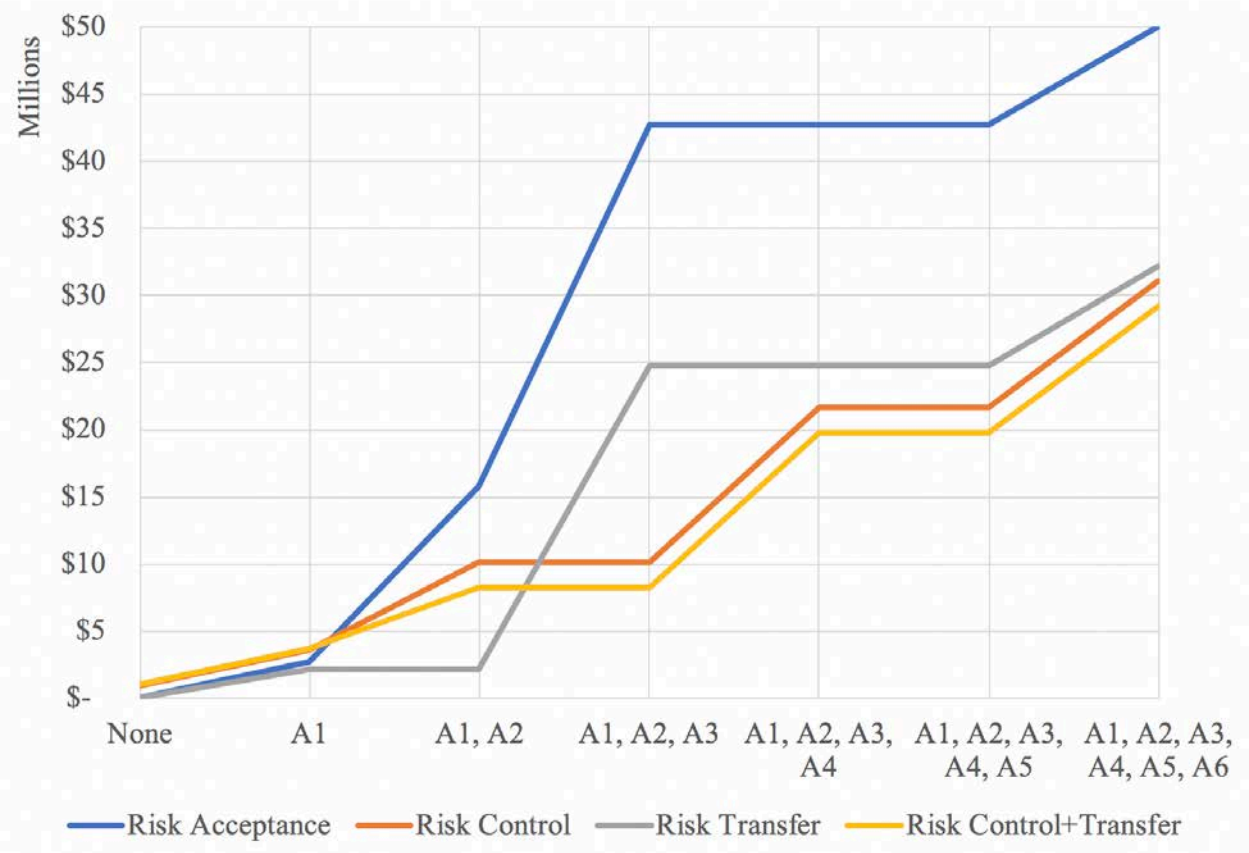


Figure 43. Comparison of risk management strategies

The detailed results for the simulation are presented in Table 12. The first column indicates the degraded nodes for each scenario. For the control strategies, A2 and A4 are partially degraded (indicated with -D) and A3 has a dependent node that is not degraded. Only A3.1 degrades for the control strategies. As it can be seen, with a right strategy it is possible to save more than $20 million in some cases.

Table 12. Comparison of risk management strategies for each scenario

Degraded Nodes	Risk Acceptance	Risk Control	Risk Transfer	Risk Control + Transfer
None	$ -	$ 900,000	$ 100,000	$ 1,000,000
A1	$ 2,691,575	$ 3,591,575	$ 2,100,000	$ 3,691,575
A1, A2(-D)	$ 15,778,781	$ 10,134,908	$ 2,100,000	$ 8,234,908
A1, A2(-D), A3(.1)	$ 42,717,939	$ 10,134,908	$ 24,817,939	$ 8,234,908
A1, A2(-D), A3(.1), A4(-D)	$ 42,717,939	$ 21,646,179	$ 24,817,939	$ 19,746,179
A1, A2(-D), A3(.1), A4(-D), A5	$ 42,717,939	$ 21,646,179	$ 24,817,939	$ 19,746,179
A1, A2(-D), A3(.1), A4(-D), A5, A6	$ 50,057,834	$ 31,138,579	$ 32,157,834	$ 29,238,579

5.6 Sensitivity Analysis

Several simulations are run for sensitivity analysis on the architecture given in Figure 29.

In Figures 44 to 51, total costs of degraded operability values of CIA components of Assets A1-A4 are plotted while all other operability values are kept fully operable. Horizontal axes of Figures 44 to 51 indicate the operability level of the indicated node's CIA values and the vertical axes stand for total costs. In Figure 44, CIA values of four nodes, A1, A2, A3, and A4 are plotted. As it can be seen, degradation of the Integrity value of node A3 causes the largest cost, followed by Integrity values of nodes A4 and A2. The reason why degradation of the integrity values cost more than confidentiality and availability is that the feeder node's operability of the integrity value can affect not only integrity value but also the integrity and availability values of the receiver nodes.

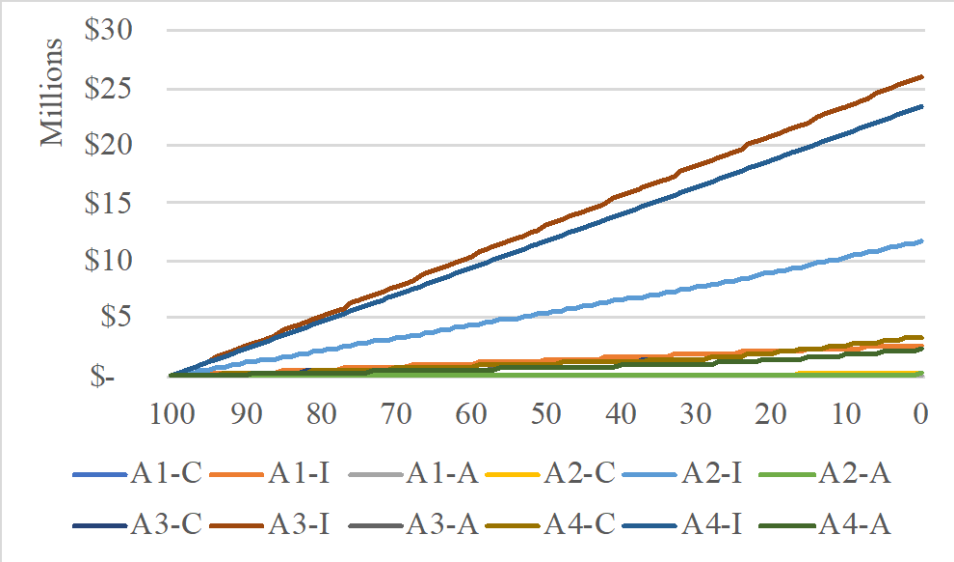


Figure 44 Cost of degradation of C-I-A values of Asset 1 to 4

Figure 45 plots the total costs caused by degradation of operability levels of CIA values of node A1. Total costs caused by confidentiality and availability degradation are negligible.

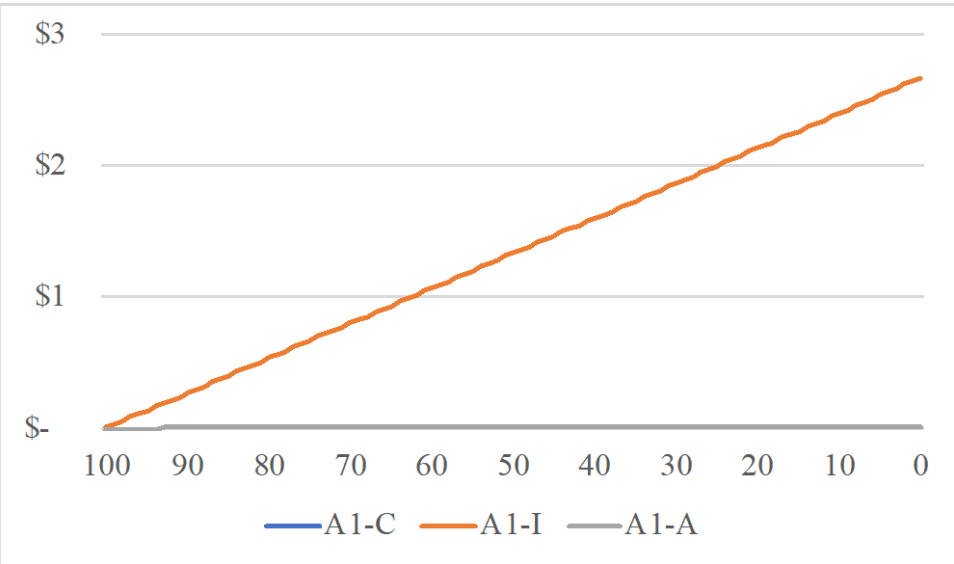


Figure 45 Operability level of C-I-A for Asset 1

Figure 46 plots the total costs caused by degradation of operability levels of CIA values of node A2. Total costs caused by confidentiality and availability degradation are negligible.

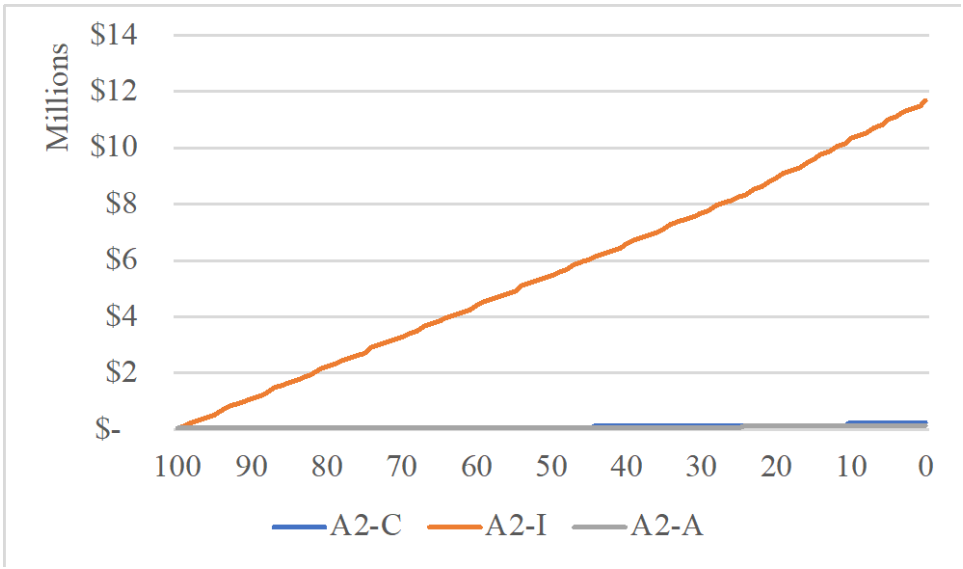


Figure 46 Operability level of C-I-A for Asset 2

Figure 47 plots the total costs caused by degradation of operability levels of CIA values of node A3. Total costs caused by confidentiality and availability degradation are relatively low.

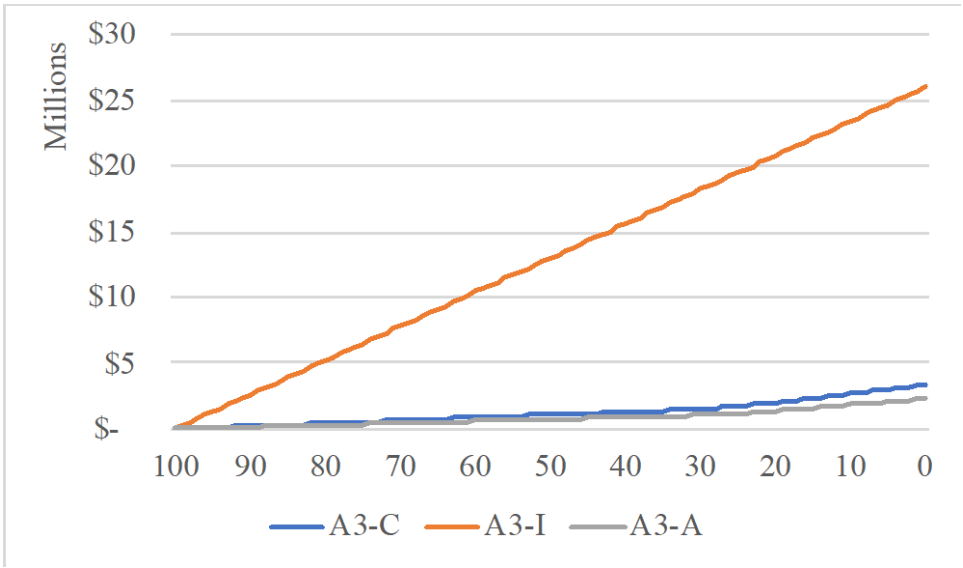


Figure 47 Operability level of C-I-A for Asset 3

Figure 48 plots the total costs caused by degradation of operability levels of CIA values of node A4. Total costs caused by confidentiality and availability degradation are relatively low.

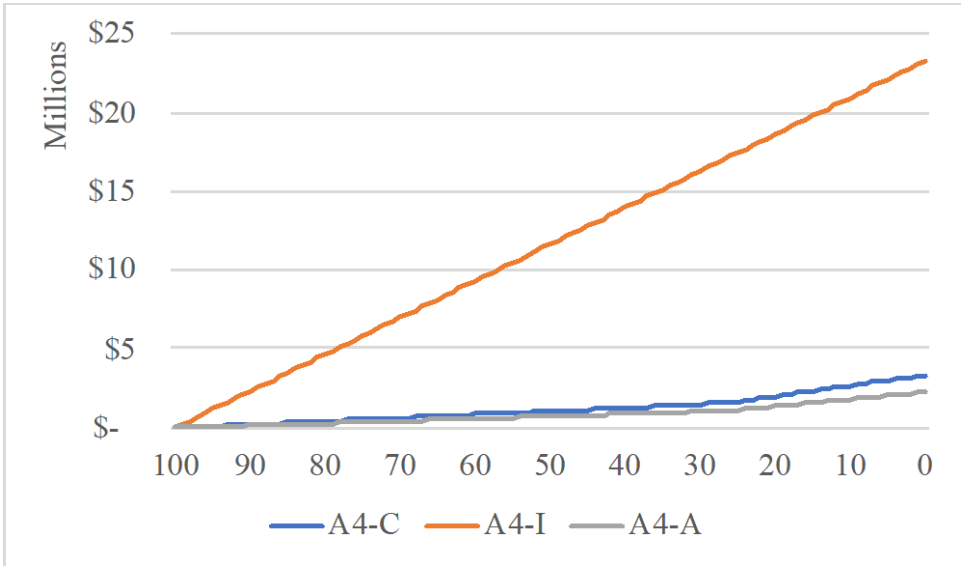


Figure 48 Operability level of C-I-A for Asset 4

Figure 49 plots the total costs caused by degradation of operability levels of Confidentiality values of Assets A1-A4. Total costs caused by confidentiality level degradation of A3 and A4 are significantly higher than A1 and A2.

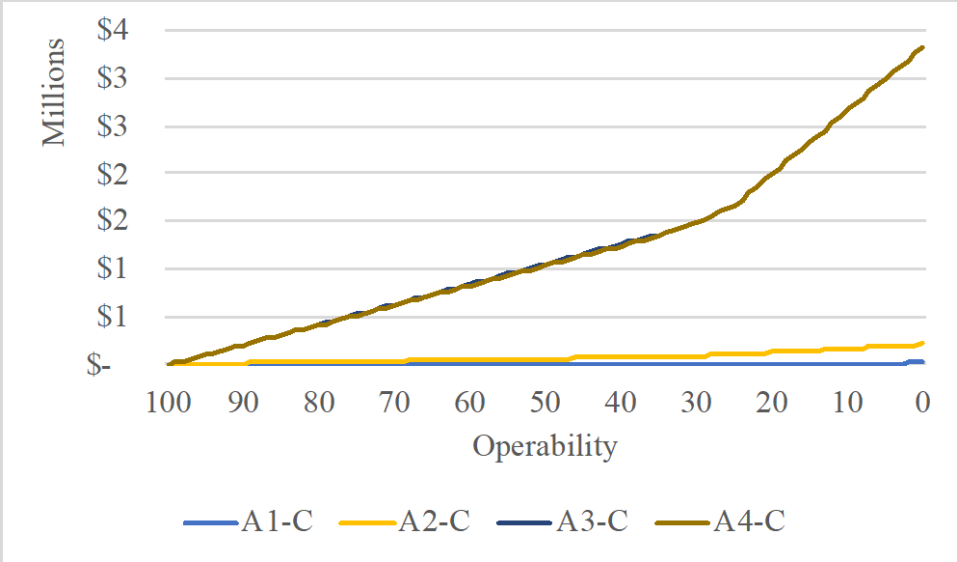


Figure 49 Operability levels of Confidentiality values of Assets A1 to A4

Figure 50 plots the total costs caused by degradation of operability levels of Integrity values of Assets A1-A4. Total costs caused by integrity level degradation of A3 and A4 are higher than A1 and A2.

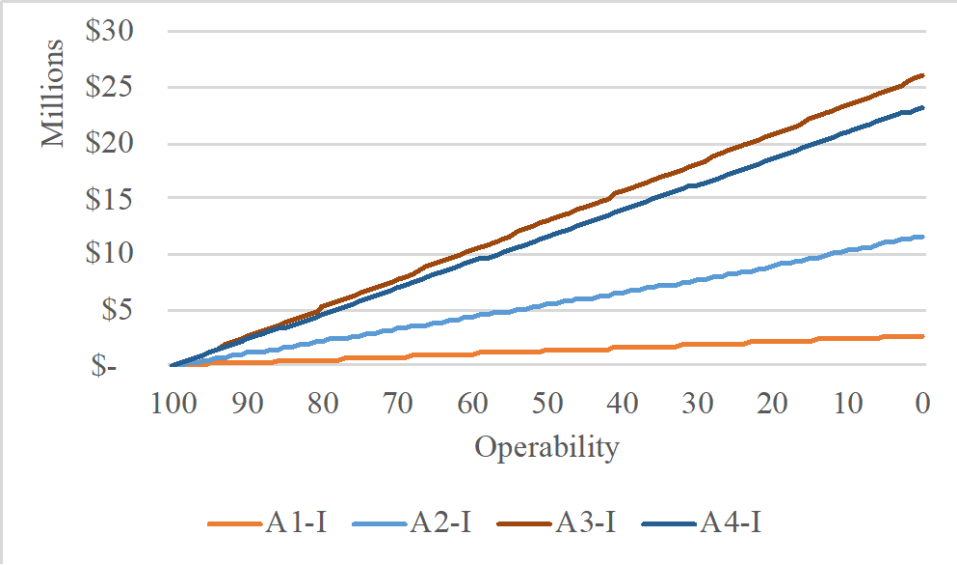


Figure 50 Operability levels of Integrity values of Assets A1 to A4

Figure 51 plots the total costs caused by degradation of operability levels of Availability values of Assets A1-A4. Total costs caused by availability level degradation of A3 and A4 are higher than A1 and A2.

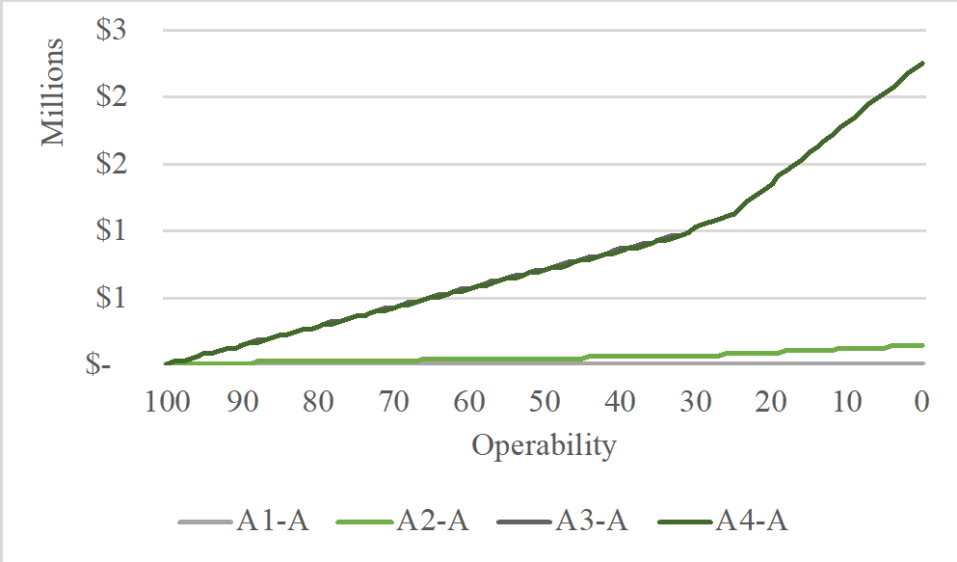


Figure 51 Operability levels of Availabilty values of Assets A1 to A4

CHAPTER 6

CONCLUSION

6.1 High Level Summary of Findings

This study aims to modify FDNA to develop FDNA-Cyber, which is a new quantitative modeling method to develop a quantitative model to determine the impact of propagation within a layer, develop a quantitative model to determine the impact propagation between different layers within an enterprise, and develop an approach to estimate the economic cost of a cyber incident or event.

The innovations of this study are (a) introducing *Self-Efficiency* of nodes, (b) Integrating *Confidentiality*, *Integrity* and *Availability* values to nodes, (c) new dependency relations (AND and OR dependecies). Another innovation of the study is calculating the impact in monetary values by considering time of the cyber action and duration of the event or incident as two of the parameters.

6.2 Significance of the Study

The proposed research has several contributions in the fields of cybersecurity and engineering management. The contributions of the research are examined under the following categories: (a) Risk Management, (b) System Resiliency, (c) Security Economics.

a) Risk Management

The proposed research contributes to the field of risk management in two areas: risk analysis and risk communication.

Risk Analysis: According to Society of Risk Analysis (Aven et al., 2015), risk analysis is defined as “Systematic process to comprehend the nature of risk and to express the risk, with the available knowledge”. Kaplan and Garrick (1981) define risk in the following formula.

Risk = Probability of a loss event X Magnitude of loss

Consequences or impact are another concept used interchangeably with “Magnitude of loss”. Most of the current studies just consider the impact at the asset layer and ignore impact on services and business processes. The studies which consider the other layers alongside asset layer do not handle the vertical and horizontal dependencies (Shameli-Sendi et al., 2016), so the proposed research will contribute to calculation of risk analysis by providing a more accurate value of “Magnitude of loss”.

Risk Communication: According to Society of Risk Analysis (Aven et al., 2015), risk communication is defined as “Exchange or sharing of risk-related data, information and knowledge between and among different target groups (such as regulators, stakeholders, consumers, media, general public)”.

The language of communication between cybersecurity decision makers at different layers of an organization varies. Decision making in cybersecurity, as similar to many other areas, is accomplished in three levels: tactical, operational and strategic. In the tactical level, capabilities of cybersecurity experts heavily depend on rapidly converting existing knowledge into practical problem solving efforts in complex IT environments. All of the security operations, like hardening IT systems, conducting penetration tests, managing IT security products, etc. can be achieved by having a high level of hands-on expertise and problem solving capability. Decision makers of the operational level need to manage cybersecurity under the technical, legal and organizational constraints so that training them requires work on cases covering the various combination of these aspects. Decision makers of the strategic level should understand the possible effects of cyber threats to the pursued mission and strategic objectives.

Risk analysis can provide common ground for all levels of decision making if a common understanding of risk is established. Senior level decision makers want to hear risk analysis results from a strategic point of view. This is possible by presenting impact with meaningful values, mission impact or impact on business processes not impact individual assets. However, technical level decision makers are more focused on the impact at the asset level, so the holistic impact calculation approach of the proposed research provides a common ground for all levels of decision makers in an organization, improves risk communication, and enhances well-informed decision making.

b) System Resiliency

The Society of Risk Analysis provides the following definitions for resiliency (Aven et al., 2015): “Probability that a system can sustain its functionality in the face of high stress or (unexpected) disturbances” or “Probability that a system can restore functionality to its pre-disaster level (or higher) within a specified time”.

The proposed research will help to identify the asset nodes that might produce the maximum impact on a business process or mission. To have a resilient system, redundant nodes can be added to the system to mitigate degradation caused by this most critical assets. Another application of resilient system engineering can be using simulation techniques to measure the cyber resiliency level of a system while architecting it.

c) Security Economics

Cybersecurity Investment

Cyber risk has become a top agenda item for businesses all over the world and is listed as one of the top three global risks with significant economic implications for businesses (Allianz,

2016). In fact, cybersecurity rating of companies is an emerging consideration in investment assessments (Bloomberg, 2014). Chief Information Security Officers (CISO) are playing more important roles in company's' managerial boards as they are not only responsible for securing organizations from cyber threats but also providing strategic guidance to other board members especially on the effectiveness and efficiency of cybersecurity investments. Board relies on CISOs for information about the company's cybersecurity posture in a language they understand – risk, cost, and benefits – and how cyber risk maps to dollars instead of the latest purchase of an IT security product (Rifai, 2017). To transform cyber risk management from a technical issue to a business issue cyber risk has to eventually be quantified as monetary value. As well, valuation of cyber risk will be integrated into Enterprise Risk Management frameworks (Ruan, 2017) eventually. Consequently, cyber risk management has become an emerging and vital part of the enterprise risk management.

Since the proposed method will calculate the impact of cyber incidents and events in monetary value, C-level managers can make better decisions to manage cyber risks and choose the economically most convenient risk management strategy (i.e. acceptance, avoidance, transfer or mitigation).

Cyber Insurance

To respond to cyber threats via risk transfer, the cyber insurance market is also emerging all over the world, including the U.S. According to AON (2017), the global stand-alone cyber market had $1.7bn in annual gross written premium in 2015 and increased to $2.3bn in 2016 and is expected to reach $5.6bn in 2020. There are 70 insurers offering the standalone cyber product in the U.S.

One of the main issues of cyber risk insurance is lack of ability of accurate cyber risk calculation particularly in economic terms. The holistic impact calculation method also provides a solution to the underinsurance problem.

6.3 Future Research

Future research which can enhance or extend this research includes: (a) extending the FDNA –Cyber model to cover dependency relations in a supply chain network, (b) integrating attack propagation at Asset layer with the functional dependencies at Asset layer, (c) extending FDNA-Cyber to have stochastic approach while modeling dependencies, and (d) developing automatic or semi-automatic techniques for extracting dependencies from network data.

REFERENCES

Abercrombie, R., Sheldon, F. and Grimaila, M. (2010) "A Systematic Comprehensive Computational Model for Stake Estimation in Mission Assurance", *IEEE International Conference on Social Computing (SocialCom)*, pp 1153-1158.

Abercrombie, R., Sheldon, F. and Mili, A. (2008) "Synopsis of Evaluating Security Controls Based on Key Performance Indicators and Stakeholder Mission Value", *11th IEEE High Assurance Systems Engineering Symposium*, pp 479-482.

Allianz. Top business risks 2016. Allianz Risk Barometer, 2016.

Angelini, M. and Santucci, G. (2015) "Visual Cyber Situational Awareness for Critical Infrastructures", *Proceedings of the 8th International Symposium on Visual Information Communication and Interaction*, pp 83-92.

AON Inpoint. (2017). *Global Cyber Market Overview*. Retrieved from https://doi.org/http://www.aon.com/attachments/risk-services/cyber/Cyber.pdf

Arora, A., Hall, D., Pinto, C. A., Ramsey, D., & Telang, R. (2004). Measuring the risk-based value of IT security solutions. *IT professional*, *6*(6), 35-42.

Bahşi, H., Udokwu, C. J., Tatar, U., & Norta, A. (2018, March). Impact Assessment of Cyber Actions on Missions or Business Processes: A Systematic Literature Review. In *ICCWS 2018 13th International Conference on Cyber Warfare and Security*(p. 11). Academic Conferences and publishing limited.

Bernard, H.R. (2011) “Research Methods in Anthropology” 5th edition, AltaMira Press, p.7

Bloomberg. KKR adds cyber risk score to its assessment of companies; 2014. Available from: http://www.bloomberg.com/news/articles/2014-04-11/kkr-adds-cyber-risk-score-to-its-assessment-of-companies.

Cam, H. and Mouallem, P. (2013) "Mission Assurance Policy and Risk Management in Cybersecurity", *Environment Systems and Decisions, 33*(4), pp 500-507.

Cavusoglu, H., Raghunathan, S., & Yue, W. T. (2008). Decision-Theoretic and Game-Theoretic Approaches to IT Security Investment. *Journal of Management Information Systems, 25*(2), 281–304. https://doi.org/10.2753/MIS0742-1222250211

Cole, R. (2017). Data Dependency Network Analysis in SoS. In *System of Systems Engineering Conference (SoSE), 2017 12th* (pp. 1-6). IEEE.

Council of Economic Advisors. (2018). *The cost of malicious cyber activity to the US economy.* Retrieved from https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

Costa, A., McShane, M. K., & Pinto, C. A. (2015). Investigating Interbank Contagion with Agent-based Modeling and Functional Dependency Network Analysis (FDNA).

Choobineh, J., Anderson, E. and Grimaila, M. (2012) "Measuring Impact on Missions and Processes: Assessment of Cyber Breaches", *45th Hawaii International Conference on System Sciences*, pp 3307-3316.

Creese, S., Goldsmith, M., Moffat, N., Happa, J. and Agrafiotis, I. (2013) "CyberVis: Visualizing the Potential Impact of Cyber Attacks on the Wider Enterprise", *IEEE International Conference on Technologies for Homeland Security (HST)*, pp 73-79.

David Barr, "Common DNS operational and configuration errors", *Internet Request for Comments (RFC 1912)*, February 1996.

DeLaurentsi, D. A., & Marais, K. (2012). *Assessing the Impact of Development Disruptions and Dependencies in Analysis of Alternatives of System-of-Systems Final Technical Report*. SYSTEMS ENGINEERING RESEARCH CENTER HOBOKEN NJ.

Diallo, S. Y., Padilla, J. J., Bozkurt, I., & Tolk, A. (2013). Modeling and simulation as a theory building paradigm. In *Ontology, Epistemology, and Teleology for Modeling and Simulation* (pp. 193–206). Springer.

Drabble, B. (2011, May). Dependency based collaboration: Ontology based information management. In *Collaboration Technologies and Systems (CTS), 2011 International Conference on* (pp. 579-586). IEEE.

Drabble, B. (2012). Information propagation through a dependency network model. *2012 International Conference on Collaboration Technologies and Systems (CTS)*, 266–272. https://doi.org/10.1109/CTS.2012.6261059

Drake, D. L., & Morse, K. (2012). Data-Driven Monetization of Acquisition Risk. in Ninth Annual Acquisition Research Symposium, Monterey, CA

Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance?. *The Journal of Risk Finance*, 17(5), 474-491. http://dx.doi.org/10.1108/jrf-09-2016-0122

Erickson, B. (2016). Cybersecurity Figure of Merit. In Proceedings of the Thirteenth Annual Acquisition Research Symposium (pp. 323–324). Naval Postgraduate School, Monterey, CA

Federal Bureau of Investigation. (2017). *Intellectual Property Theft/Piracy*. Retrieved from https://www.fbi.gov/investigate/white-collar-crime/piracy-ip-theft.

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision Support Systems*, *86*, 13–23. https://doi.org/10.1016/j.dss.2016.02.012

Firestone, W. A. (1993). Alternative Arguments for Generalizing From Data as Applied to Qualitative Research. *Educational Researcher*, *22*(4), 16–23. https://doi.org/10.3102/0013189X022004016

Garbin, C. (n.d.). External Validity Types. Retrieved from http://psych.unl.edu/psycrs/350/unit1/p_extval.pdf

Garvey, P. (2009). *An analytical framework and model formulation for measuring risk in engineering enterprise systems: a capability portfolio perspective.* (Doctoral Dissertation). Retrieved from ProQuest Dissertations and Theses Global.

Garvey, P. and Patel, S. (2014). "Analytical Frameworks to Assess the Effectiveness and Economic-Returns of Cybersecurity Investments", *IEEE Military Communications Conference*, pp 136-145.

Garvey, P. R., & Pinto, C. A. (2009). Introduction to functional dependency network analysis. In The MITRE Corporation and Old Dominion, *Second International Symposium on Engineering Systems*, MIT, Cambridge, Massachusetts (Vol. 5).

Garrido-Pelaz, R., González-Manzano, L., & Pastrana, S. (2016). Shall we collaborate?: A model to analyse the benefits of information sharing. In *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security* (pp. 15-24). ACM.

Giani, A., Bent, R., Hinrichs, M., McQueen , M. and Poolla, K. (2012) "Metrics for Assessment of Smart Grid Data Integrity Attacks", *IEEE Power and Energy Society General Meeting*, pp 1-8.

Goddard, W. & Melville, S. (2004) “Research Methodology: An Introduction” 2nd edition, Blackwell Publishing

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC), 5*(4), 438–457.

Guariniello, C., & DeLaurentis, D. (2013a). Dependency analysis of system-of-systems operational and development networks. *Procedia Computer Science*, *16*, 265-274.

Guariniello, C., & DeLaurentis, D. (2013b). Dependency network analysis: fostering the future of space with new tools and techniques in space systems-of-systems design and architecture. In *IAF International Astronautical Congress*.

Guariniello, C., & DeLaurentis, D. A. (2013c). Maintenance and recycling in space: functional dependency analysis of on-orbit servicing satellites team for modular spacecraft. In *AIAA SPACE 2013 Conference and Exposition* (p. 5327).

Guariniello, C., & DeLaurentis, D. (2014a). Communications, information, and cyber security in systems-of-systems: Assessing the impact of attacks through interdependency analysis. *Procedia Computer Science, 28*, 720-727.

Guariniello, C., & DeLaurentis, D. (2014b). Integrated analysis of functional and developmental interdependencies to quantify and trade-off ilities for system-of-systems design, architecture, and evolution. *Procedia Computer Science, 28*, 728-735.

Guariniello, C., & DeLaurentis, D. (2017). Supporting design via the system operational dependency analysis methodology. *Research in Engineering Design*, *28*(1), 53-69.

Granadillo, G., Motzek, A., Garcia-Alfaro, J. and Debar, H. (2016) "Selection of Mitigation Actions Based on Financial and Operational Impact Assessments", *11th International Conference on Availability, Reliability and Security (ARES)*, pp 137-146.

Heinbockel, W., Kertzner, P. and McQuaid, R. (2010) "Providing Mission Assurance for Airborne Networks", *IEEE Second International Conference on Social Computing*, pp 1183-1187.

Holzgrefe, J. P. L. (2015). *A framework to simplify the choice of alternative analysis and selection methods*. Old Dominion University.

Inductive Approach (Inductive Reasoning). (n.d.). Retrieved March 5, 2018, from https://research-methodology.net/research-methodology/research-approach/inductive-approach-2/

Jajodia, S., Noel, S., Kalapa, P. and Williams, J. (2011) "Cauldron Mission-Centric Cyber Situational Awareness with Defense in Depth", *Military Communications Conference*, pp 1339-1344.

Jakobson, G. (2011) "Mission Cyber Security Situation Assessment Using Impact Dependency Graphs", *Proceedings of the 14th International Conference on Information Fusion (FUSION)*, pp 1-8.

Janofsky, A. (2017). *Equifax Breach Could Cost Billions*. [online] WSJ. Available at: https://www.wsj.com/articles/equifax-breach-could-cost-billions-1505474692 [Accessed 14 Nov. 2017].

Kaestner, S., Arndt, C., & Dillon-Merrill, R. (2016). *The Cybersecurity Challenge in Acquisition*. Georgetown University Washington United States. Retrieved from http://www.dtic.mil/docs/citations/AD1016746

Kanoun, W., Papillon, S. and Dubus, S. (2015) "Elementary Risks: Bridging Operational and Strategic Security Realms", *11th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS)*, pp 278-286.

Kaplan, S., & Garrick, B. J. (1981). On the quantitative definition of risk. *Risk analysis*, *1*(1), 11-27.

Keeney, R. L., Raiffa, H., (1976). *Decisions with Multiple Objectives Preferences and Value Tradeoffs*, John Wiley & Sons, New York, NY.

Kenton, W., (2018). *Cost of capital.* Retrieved from https://www.investopedia.com/terms/c/costofcapital.asp

Keskin, O., Tatar, U., Poyraz, O., Pinto, A., & Gheorghe, A. (2018, March). Economics-Based Risk Management of Distributed Denial of Service Attacks: A Distance Learning Case Study. In *ICCWS 2018 13th International Conference on Cyber Warfare and Security* (p. 343). Academic Conferences and publishing limited.

Landry, M., Malouin, J.-L., & Oral, M. (1983). Model validation in operations research. *European Journal of Operational Research*, *14*(3), 207–220. https://doi.org/10.1016/0377-2217(83)90257-6

Lange, M., Krotofil, M. and Möller, R. (2015) "Mission Impact Assessment in Power Grids", *Proceedings of the NATO IST-128 Workshop: Assessing Mission Impact of Cyberattacks*, pp 51-59.

LaVallee, D., Fix, S. and Edell, D. (2015) "Mission-level Space Situational Awareness", *IEEE Aerospace Conference*, pp 1-9.

Law, A. M. (2008). How to build valid and credible simulation models. In *2008 Winter Simulation Conference* (pp. 39–47). https://doi.org/10.1109/WSC.2008.4736054

Lei, J. (2015) "Cyber Situational Awareness and Mission-Centric Resilient Cyber Defense", *4th International Conference on Computer Science and Network Technology (ICCSNT)*, pp 1218-1225.

Lemay, A., Fernandez, J. and Knight, S. (2014) "Modeling Physical Impact of Cyber Attacks", *Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES)*, pp 1-6.

Llansó, T. and Klatt, E. (2014) "CyMRisk: An Approach for Computing Mission Risk due to Cyber Attacks", *IEEE International Systems Conference Proceedings*, pp 1-7.

Martin Eling, & Werner Schnell. (2016). What do we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance*, *17*(5), 474–491. https://doi.org/10.1108/JRF-09-2016-0122

Morse, K.L. & Drake, D.L., (2012). *Data-driven monetization of acquisition risk.* Johns Hopkins University Laurel MD Applied Physics Lab.

Musman, S. and Temin, A. (2015) "A Cyber Mission Impact Assessment Tool", *IEEE International Symposium on Technologies for Homeland Security*, pp 1-7.

Noel, S., Ludwig, J., Jain, P., Johnson, D., Thomas, R., McFarland, J. and Tello, B. (2015) "Analyzing Mission Impacts of Cyber Actions", *Proceedings of the NATO IST-128 Workshop: Assessing Mission Impact of Cyberattacks*, pp 80-86.

Open Web Application Security Project (2014). Retriewed from https://www.owasp.org/index.php/Main_Page

Polit, D. F., & Beck, C. T. (2010). Generalization in quantitative and qualitative research: myths and strategies. *International Journal of Nursing Studies*, *47*(11), 1451–1458. https://doi.org/10.1016/j.ijnurstu.2010.06.004

Rifai, F. (2017). History is Repeating Itself (In a Good Way) - Corporate Compliance Insights. Corporate Compliance Insights. Retrieved 10 June 2017, from

Riley, M., Robertson, M. and Sharpe, M. (2017). *The Inside Story of Equifax's Massive Data Breach*. [online] Bloomberg.com. Retrieved from: https://www.bloomberg.com/news/features/2017-09-29/the-equifax-hack-has-all-the-hallmarks-of-state-sponsored-pros [Accessed 14 Nov. 2017].

Robinson, S. (2013). Conceptual modeling for simulation. In *2013 Winter Simulations Conference (WSC)* (pp. 377–388). https://doi.org/10.1109/WSC.2013.6721435

Ruan, K. (2017). Introducing cybernomics: A unifying economic framework for measuring cyber risk. *Computers and Security*, *65*(2017), 77–89. https://doi.org/10.1016/j.cose.2016.10.009

Saunders, M., Lewis, P. & Thornhill, A. (2012) "Research Methods for Business Students" 6th edition, Pearson Education Limited

Sargent, R. G. (2009). Verification and validation of simulation models. In *Simulation Conference (WSC), Proceedings of the 2009 Winter* (pp. 162–176). IEEE.

Sargent, R. G. (2015). An introductory tutorial on verification and validation of simulation models. In *2015 Winter Simulation Conference (WSC)* (pp. 1729–1740). https://doi.org/10.1109/WSC.2015.7408291

Schultz, E. M., & Wydler, V. (2015). *Integrating Cybersecurity into the Program Management Organization*. MITRE Corp McLean VA.

Servi, L. D., & Garvey, P. R. (2017). Deriving global criticality conditions from local dependencies using functional dependency network analysis (FDNA). *Systems Engineering*, *20*(4), 297-306.

Shaikh, A., Tewari, R., & Agrawal, M. (2001). On the effectiveness of DNS-based server selection. In *INFOCOM 2001. Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*(Vol. 3, pp. 1801-1810). IEEE.

Shameli-Sendi, A., Aghababaei-Barzegar, R. and Cheriet, M., 2016. Taxonomy of information security risk assessment (ISRA). *Computers & security*, *57*, pp.14-30.

Shaw, J. (2003) "Predicting the impact of cyber-attacks on BMC/sup 3/ enterprises", *Proceedings DARPA Information Survivability Conference and Exposition*, vol. 2. pp 208-213.

Sheldon, F. T., Abercrombie, R. K., & Mili, A. (2009). Methodology for evaluating security controls based on key performance indicators and stakeholder mission. In *System Sciences, 2009. HICSS'09. 42nd Hawaii International Conference on* (pp. 1–10). IEEE.

Short, A. R., Lai, A. D., & Van Bossuyt, D. L. (2018). Conceptual design of sacrificial sub-systems: failure flow decision functions. *Research in Engineering Design*, *29*(1), 23-38.

Tatar, Ü., Çalik, O., Çelik, M. and Karabacak, B., (2014), January. A Comparative Analysis of the National Cyber Security Strategies of Leading Nations. In *International Conference on Cyber Warfare and Security* (p. 211). Academic Conferences International Limited.

Tolk, A. (2013). Truth, Trust, and Turing – Implications for Modeling and Simulation. In *Ontology, Epistemology, and Teleology for Modeling and Simulation* (pp. 1–26). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-31140-6_1

Valerdi, R., & Davidz, H. L. (2009). Empirical research in systems engineering: challenges and opportunities of a new frontier. *Systems Engineering*, *12*(2), 169–181. https://doi.org/10.1002/sys.20117

Van Der Aalst, W. (2012). Process mining: Overview and opportunities. *ACM Transactions on Management Information Systems (TMIS)*, *3*(2), 7.

Verizon. (2017). *2017 Data Breach Investigations Report.* Retrieved from https://enterprise.verizon.com/resources/reports/2017_dbir.pdf

Wang, Y., Zhang, W. X., & Li, Q. (2014). Functional dependency network analysis of security of navigation satellite system. In *Applied Mechanics and Materials* (Vol. 522, pp. 1192-1196). Trans Tech Publications.

Wu, W., Kang, R. and Li, Z. (2015) "Risk Assessment Method for Cybersecurity of Cyber-Physical Systems Based on Inter-Dependency of Vulnerabilities", *IEEE International Conference on Industrial Engineering and Engineering Management*, pp 1618-1622.

Xiang, Y., Wang, L. and Zhang, Y. (2014) "Power System Adequacy Assessment with Probabilistic Cyber Attacks against Breakers", *IEEE PES General Meeting | Conference & Exposition*, pp 1-5.

VITA

Unal Tatar

EDUCATION

2019	**Ph.D.**	**Engineering Management & Systems Engineering**, Old Dominion University
2009	**M.S.**	**Cryptography**, METU, Turkey
2004	**B.S.**	**Computer Engineering**, Bilkent University, Turkey

PROFESSIONAL EXPERIENCE

2015 – 2018	**Research Assistant**, Old Dominion University
2013 – 2015	**Academic Advisor of Cyber Security**, NATO COE-DAT
2004 – 2015	**Principal Researcher**, National Cyber Security Research Institute, Turkey

SELECTED PUBLICATIONS

1. Alla, S., Soltanisehat, L., **Tatar, U.**, & Keskin, O. (2018, May). Blockchain Technology in Electronic Healthcare Systems. IISE Annual Conference. Orlando, FL.
2. Keskin, O., **Tatar, U.,** Poyraz, O., Pinto, A., & Gheorghe, A. (2018, March) Economics-Based Risk Management of Distributed Denial of Service Attacks: A Distance Learning Case Study. In 13th International Conference on Cyber Warfare and Security. Washington DC, USA.
3. Bahsi, H., Udokwu, C., **Tatar, U.**, & Norta, A. (2018, March) Impact Assessment of Cyber Actions on Missions or Business Processes – A Systematic Literature Review. In 13th International Conference on Cyber Warfare and Security. Washington DC, USA.
4. **Tatar, U.,** Gokce, Y. & Gheorghe, A. (2017). Strategic Cyber Defense: A Multidisciplinary Perspective. Amsterdam: IOS Press
5. **Tatar, U.,** Bahsi, B., Gheorghe, A. (2016, June) "Impact Assessment of Cyber Attacks: A Quantification Study on Power Generation Systems". System of Systems Engineering Conference (SoSE), 2016 11th, Kongsberg, Norway.
6. **Tatar, U.,** Karabacak, B., Gheorghe, A. (2016, March) "An Assessment Model of Improving National Cyber Security Governance". 11th International Conference on Cyber Warfare and Security. Boston, USA.
7. **Tatar, U.,** & Karabacak, B. (2012, June). "A Hierarchical Asset Valuation Method for Information Security Risk Analysis". International Conference on Information Society (i-Society) (pp. 286-291). IEEE. London, UK.
8. **Tatar, U**., Calik, O., Celik, M., Karabacak, B. (2014, March) "A Comparative Analysis of the National Cyber Security Strategies of Leading Nations". 9th International Cyber on Warfare and Security Conference. Indiana, USA.
9. Caliskan, E.; **Tatar, U**.; Bahsi, H.; Ottis, R.; Vaarandi, R. (2017, March) "Capability detection and evaluation metrics for Cyber Security lab exercises" 12th International Conference on Cyber Warfare and Security, Dayton, Ohio, USA
10. **Tatar, U**., Calik, O., Celik, M., Karabacak, B. (2014, March) "A Comparative Analysis of the National Cyber Security Strategies of Leading Nations". 9th International Cyber on Warfare and Security Conference. Indiana, USA.