

**Dynamic Cyber Resilience of  
Interdependent Critical Information Infrastructures**

المرونة السيبرانية الديناميكية للبنى التحتية المعلوماتية الحيوية المترابطة

by

**MAZEN GHAZI JUMA**

A thesis submitted in fulfilment  
of the requirements for the degree of  
**DOCTOR OF PHILOSOPHY IN COMPUTER SCIENCE**  
at  
**The British University in Dubai**

**December 2021**

**Dynamic Cyber Resilience of  
Interdependent Critical Information Infrastructures**

المرونة السيبرانية الديناميكية للبنى التحتية المعلوماتية الحيوية المترابطة

By

**MAZEN GHAZI JUMA**

**A thesis submitted to the Faculty of Engineering and Information Technology  
in fulfilment of the requirements for the degree of**

**DOCTOR OF PHILOSOPHY IN COMPUTER SCIENCE**

At

**The British University in Dubai**

**December 2021**

**Thesis Supervisor**

**Professor Khaled Shaalan**

**Approved for award:**

\_\_\_\_\_  
Name: Professor Mohammed Ismail  
Designation: External Examiner

\_\_\_\_\_  
Name: Professor Sherief Abdallah  
Designation: Internal Examiner

\_\_\_\_\_  
Name: Professor Husam Al-Malkawi  
Designation: Chair of the Examining Panel

\_\_\_\_\_  
Name: Professor Abdullah Alshamsi  
Designation: Chair of the RDC

Date: 23 Dec 2021

## **DECLARATION**

I warrant that the content of this research is the direct result of my own work and that any use made in it of published or unpublished copyright material falls within the limits permitted by international copyright conventions.

I understand that a copy of my research will be deposited in the University Library for permanent retention.

I hereby agree that the material mentioned above for which I am author and copyright holder may be copied and distributed by The British University in Dubai for the purposes of research, private study or education and that The British University in Dubai may recover from purchasers the costs incurred in such copying and distribution, where appropriate.

I understand that The British University in Dubai may make a digital copy available in the institutional repository.

I understand that I may apply to the University to retain the right to withhold or to restrict access to my thesis for a period which shall not normally exceed four calendar years from the congregation at which the degree is conferred, the length of the period to be specified in the application, together with the precise reasons for making that application.

---

Signature of the Student

## **COPYRIGHT AND INFORMATION TO USERS**

The author whose copyright is declared on the title page of the work has granted to the British University in Dubai the right to lend his/her research work to users of its library and to make partial or single copies for educational and research use.

The author has also granted permission to the University to keep or make a digital copy for similar use and for the purpose of preservation of the work digitally.

Multiple copying of this work for scholarly purposes may be granted by either the author, the Registrar or the Dean only.

Copying for financial gain shall only be allowed with the author's express permission.

Any use of this work in whole or in part shall respect the moral rights of the author to be acknowledged and to reflect in good faith and without detriment the meaning of the content, and the original authorship.

## **ABSTRACT**

We are becoming progressively reliant on the Critical Information Infrastructures (CIIs) to provide essential services in our daily lives, such as telecommunications, energy facilities, financial systems, and power grids. These interdependent infrastructures form one coupled heterogeneous network that qualifies them to deliver new cyber roles and crucial tasks not achievable before in numerous domains worldwide.

The CIIs have to deal with sophisticated cyber risks resulting from cyber vulnerabilities of their scale-free topology targeted by different cyber threats like concurrent and consecutive cyberattacks to the expected failure cause of the single hub nodes in their decentralized structures lead to cascading and escalating cyber failures that interrupt the vital services and considerable losses in modern societies with vast negative impacts on the economy and national security.

Therefore, the research community has attempted over the last decade to pay attention to address the cyber protection gaps of CIIs in many studies by enhancing the existing standard solutions based on cyber trustfulness engineering, for example, distance-vector, link-state, and path-rule solutions, or developing new ones, but still missing one comprehensive technology solution.

The required solution has to bridge the current literature gaps by shifting the paradigm of cyber CIIs protection properly towards dynamic cyber resilience to balance proactive and reactive perspectives at theoretical and empirical levels. Besides, it also needs to understand, analyze, evaluate, and optimize the set of dynamic cyber resilience capabilities consisting of withstanding, mitigation, recovery, and normalization.

These capabilities support the various states of the typical cycle of dynamic cyber resilience,

including threshold, bottom, and equilibrium states to increase CII's robustness against cyberattacks, absorb frequent cyber disturbances that occurred, recover quickly from cyber failures, and re-establish their acceptable performance levels within appropriate timeframe.

This thesis presents the novel proposed solution of dynamic cyber resilience using cyber zero-trust engineering for the first time to cope with highlighted shortcomings of the standard solutions, overcome the single hub node failure and enhance dynamic cyber resilience capabilities of interdependent CII networks against concurrent and consecutive cyberattacks to deliver their core services continuously.

The research goal of this thesis was accomplished by an iterative four-objective cycle through two phases: primary and optimization. In the primary phase, the novel conceptual framework of the proposed solution was developed based on four fundamental concepts: decentralized registry, delegated peers, consensus rules, and dynamic routing. The technology stack of the proposed solution was also implemented with four algorithms and eight protocols.

The evaluation results of the proposed solution were compared to the results of standard solutions under different cyberattack scenarios using quantitative research methods involving computing simulations, emulation experiments, and analytical modeling.

The optimization phase improved the conceptual framework by adding three new fundamental concepts: hubs coupling, encrypted transmission, and end-to-end service quality. The technology stack was also enhanced with three new algorithms and five protocols.

The proposed solution was optimized using the iterative four-objective cycle based on previous primary phase results. Lastly, all results in both phases were analyzed and discussed, and the final findings of the thesis were interpreted.

However, it can be concluded that the proposed solution failed to compete with other standard

solutions in terms of dynamic cyber resilience capabilities and total resilience measurements during the primary phase. Nevertheless, the optimized solution achieved the optimal results compared to the standard solutions. Finally, study limitations and recommendations for future works represented the research outcomes and contributions.

## ملخص

لقد أصبحنا نعتمد بشكل تدريجي على البنى التحتية المعلوماتية الحيوية لتزويدنا بالخدمات الأساسية في حياتنا اليومية، مثل الاتصالات السلكية واللاسلكية ومرافق الطاقة والأنظمة المالية وشبكات الكهرباء. وتشكل هذه البنى التحتية المترابطة غير المتجانسة شبكة واحدة تؤهلها لتقديم أدوار سيبرانية جديدة ومهام حاسمة لم تكن قابلة للتحقق من قبل في العديد من المجالات في جميع أنحاء العالم.

وبناء على ذلك، يتعين على البنى التحتية المعلوماتية الحيوية التعامل مع المخاطر السيبرانية المعقدة الناتجة عن نقاط الضعف السيبرانية لطوبولوجيتها الخالية من النطاق والتي تستهدفها التهديدات السيبرانية المختلفة مثل الهجمات السيبرانية المتزامنة والمتتالية التي تسبب الإفشال الشائع للعقد المحورية الفردية في هيكلها اللامركزية مما يؤدي بدوره إلى الفشل السيبراني المتتابع والمتصاعد للبنى التحتية المعلوماتية الحيوية المترابطة بحيث يتم تعطيل الخدمات الحيوية والتسبب في خسائر فادحة للمجتمعات الحديثة مع حدوث تأثيرات سلبية واسعة النطاق على الاقتصاد والأمن القومي.

لذلك، يحاول المجتمع البحثي على مدار العقد الماضي الانتباه إلى معالجة فجوات الحماية السيبرانية للبنى التحتية المعلوماتية الحيوية في العديد من الدراسات من خلال تعزيز الحلول القياسية الحالية القائمة على هندسة الثقة السيبرانية، ومنها على سبيل المثال، حلول متجه المسافات، وحالة الارتباط، وقواعد المسار، أو تطوير حلول جديدة، ولكن لا يوجد هنالك حل تقني واحد شامل.

الحل المطلوب يجب أن يسد الفجوات الحالية في الأدبيات عن طريق التحول في نموذج الحماية السيبراني للبنى التحتية المعلوماتية الحيوية بشكل ملائم نحو المرونة السيبرانية الديناميكية لموازنة المنظورات الاستباقية والتفاعلية على المستويين النظري والتجريبي. بالإضافة إلى ذلك، الحاجة أيضا إلى فهم وتحليل وتقييم وتحسين مجموعة قدرات المرونة السيبرانية الديناميكية التي تتكون من الصمود والتخفيف والتعافي والتطبيق.

تدعم هذه القدرات الحالات المختلفة للدورة النموذجية للمرونة السيبرانية الديناميكية، بما في ذلك حالات العتبة والقاع والتوازن لزيادة صلابة البنى التحتية المعلوماتية الحيوية ضد الهجمات السيبرانية، وامتصاص الاضطرابات السيبرانية المتكررة التي تحدث، والتعافي بسرعة من حالات الفشل السيبراني، وأخيرا إعادة تأسيس لمستويات الأداء المقبولة للبنى التحتية المعلوماتية الحيوية ضمن الإطار الزمني المناسب.

تقدم هذه الأطروحة حل جديد تقني مقترح للمرونة السيبرانية الديناميكية باستخدام هندسة الثقة السيبرانية



المعدومة لأول مرة للتعامل مع أوجه القصور البارزة في الحلول التقنية القياسية، والتغلب على فشل عقدة المحور الفردية وتعزيز قدرات المرونة السيبرانية الديناميكية لشبكات البنى التحتية المعلوماتية الحيوية المترابطة ضد الهجمات السيبرانية المتزامنة والمتتالية لتقديم خدماتها الأساسية بشكل مستمر.

تم تحقيق هدف البحث من هذه الأطروحة من خلال دورة تكرارية من أربعة أهداف على مرحلتين: الأولى والتحسينية. في المرحلة الأولى، تم تطوير الإطار المفاهيمي الجديد للحل المقترح على أساس أربعة مفاهيم أساسية: السجل اللامركزي، والأقران المفوضون، وقواعد الإجماع، والتوجيه الديناميكي. كذلك، تم تنفيذ الحزمة التقنية للحل المقترح بأربع خوارزميات وثمانية بروتوكولات. حيث تمت مقارنة نتائج تقييم الحل المقترح بنتائج الحلول القياسية في ظل سيناريوهات مختلفة للهجمات السيبرانية باستخدام الأساليب البحثية الكمية التي تتضمن عمليات المحاكاة الحاسوبية وتجارب المضاهاة والنمذجة التحليلية.

في مرحلة التحسين، تم تحسين الإطار المفاهيمي بإضافة ثلاثة مفاهيم أساسية جديدة: اقتران المحاور، الإرسال المشفر، وجودة الخدمة من طرف إلى طرف. وتم تحسين الحزمة التقنية أيضا بثلاث خوارزميات جديدة وخمسة بروتوكولات. لقد تم تحسين الحل المقترح بناء على نتائج المرحلة الأولى باستخدام نفس الدورة التكرارية المكونة من أربعة أهداف سابقاً. وتحليل ومناقشة جميع النتائج في كلا المرحلتين، وتفسير الاستنتاجات النهائية للأطروحة.

كخلاصة عامة، يمكن الاستنتاج أن الحل المقترح فشل في التنافس مع الحلول القياسية الأخرى من حيث قدرات المرونة الإلكترونية الديناميكية ومقاييس المرونة الكاملة خلال المرحلة الأولى. ومع ذلك، حقق الحل المقترح المحسّن أفضل النتائج مقارنة بالحلول القياسية. تم تمثيل نتائج ومساهمات البحث مع تحديد قيود الدراسة والتوصيات للأعمال المستقبلية.

## **ACKNOWLEDGEMENTS**

First of all, thanks to Allah almighty for supporting and guiding me in accomplishing my Ph.D. thesis and, throughout the whole, this challenging journey.

I want to express my sincere gratitude to my supervisor and director of studies, **Prof. Khaled Shaalan**, for the continuous support of the Ph.D. thesis and related papers, for his motivation, helping, and profound experience. Besides, I would like to thank my second supervisor, Dr. Cornelius Ncube, for providing me with insightful comments and encouragement, and special thanks to Dr. Azza Abdel Monem for her Contribution as a coauthor in my publications.

Last but not least, I extend heartfelt thanks to my big family, the soul of my father, my patient mother, and my dear brothers, sisters, and uncle. Words cannot express how grateful I am to my small family, beloved wife, daughters, and sons because I owe it all to you. Many Thanks!

## TABLE OF CONTENTS

<b>DECLARATION</b> .....	Error! Bookmark not defined.
<b>COPYRIGHT AND INFORMATION TO USERS</b> .....	Error! Bookmark not defined.
<b>STATEMENT OF ORIGINAL AUTHORSHIP</b> .....	Error! Bookmark not defined.
<b>ABSTRACT</b> .....	<b>V</b>
<b>ACKNOWLEDGEMENTS</b> .....	<b>X</b>
<b>LIST OF TABLES</b> .....	<b>IV</b>
<b>LIST OF FIGURES</b> .....	<b>VI</b>
<b>LIST OF ABBREVIATIONS AND ACRONYMS</b> .....	<b>IX</b>
<b>CHAPTER 1. INTRODUCTION</b> .....	<b>1</b>
1.1 Research Context.....	2
1.2 Rationale and Motivation .....	5
1.3 Research Gaps and Problem Statement .....	8
1.4 Research Purpose, Questions, and Hypotheses .....	10
1.5 Scope, Assumptions, and Originality .....	14
1.6 Research Contributions .....	17
1.7 Author’s Related Publications .....	20
1.8 Thesis Outlines .....	24
<b>CHAPTER 2. LITERATURE REVIEW</b> .....	<b>28</b>
2.1 Critical Information Infrastructures.....	28
2.1.1 Coupling Behavior across Interdependent CIIs .....	30
2.1.2 Cyber Vulnerability Analysis of CIIs Scale-Free Topology.....	46

2.1.3	CII's Failure under Concurrent and Consecutive Cyberattacks .....	55
2.2	Dynamic Cyber Resilience .....	68
2.2.1	Core Principles of Dynamic Cyber Resilience .....	69
2.2.2	Standard solutions of Dynamic Cyber Resilience .....	75
2.2.3	Quantification of Dynamic Cyber Resilience .....	88
2.3	Findings of the Literature Review .....	95
<b>CHAPTER 3. THE PROPOSED SOLUTION .....</b>		<b>98</b>
3.1	The Paradigm Shift of Dynamic Cyber Resilience .....	98
3.1.1	New Perspective of Dynamic Cyber Resilience .....	99
3.1.2	Novel Proposed Solution based on Cyber Zero-Trust Engineering.....	104
3.2	Optimization of Proposed Solution .....	108
3.2.1	Optimized Conceptual Framework .....	108
3.2.2	Heuristic Improvements of Proposed Solution .....	123
<b>CHAPTER 4. DESIGN AND METHODOLOGY .....</b>		<b>138</b>
4.1	Research Design .....	139
4.1.1	Research Roadmap.....	139
4.1.2	Evaluation Metrics .....	142
4.1.3	Scenarios Operationalization .....	148
4.2	Research Methodology .....	167
4.2.1	Data Collection .....	167
4.2.2	Data Analysis .....	173
4.2.3	Data Validation .....	179

<b>CHAPTER 5. RESULTS AND DISCUSSION .....</b>	<b>185</b>
5.1 Optimized Results Analysis of Computing Simulations .....	185
5.2 Optimized Results Analysis of Emulated Experiments.....	198
5.3 Optimized Results Analysis of Analytical Modeling.....	211
5.4 Optimized Results Discussion.....	220
5.5 Final Research Findings .....	229
<b>CHAPTER 6. CONCLUSIONS AND RECOMMENDATIONS.....</b>	<b>233</b>
6.1 Research Conclusions.....	233
6.1.1 Answering Research Questions and Meeting Hypotheses.....	234
6.1.2 Accomplishing of the Research Purpose .....	241
6.1.3 Research Outcomes and Expected Implications .....	243
6.2 Research Recommendations.....	246
6.2.1 Research Limitations and Alternatives .....	247
6.2.2 Suggestions for Future Works .....	249
<b>REFERENCES .....</b>	<b>252</b>
<b>Appendix A: Research Background .....</b>	<b>284</b>
<b>Appendix B: Definition of Key Terminologies.....</b>	<b>291</b>
<b>Appendix C: Secondary Data Overview.....</b>	<b>300</b>
<b>Appendix D: Research Methodological Choices.....</b>	<b>306</b>
<b>Appendix E: Primary Proposed Solution.....</b>	<b>320</b>
<b>Appendix F: Primary Results Analysis and Discussion.....</b>	<b>324</b>

## **LIST OF TABLES**

Table 2.1: Differences between ICS-based Infrastructure and ICT-based Infrastructure .....	33
Table 2.2: Examples of Different Topologies for Networks .....	37
Table 2.3: Classifications of the Cyberattack Scenarios .....	61
Table 2.4: Cyberattack Levels based on Seriousness Degree .....	64
Table 2.5: Cyber Resilience Maturity Matrix of Interdependent CII Networks .....	72
Table 2.6: Comparison of Quantification Approaches for Dynamic Cyber Resilience .....	90
Table 4.1: Matching among Capabilities and Factors of Dynamic Cyber Resilience.....	146
Table 5.17: Optimized Results of OPNET Simulation for the Core-Core Scenario .....	187
Table 5.18: Solutions Ranking of Optimized Simulation Results for the Core-Core Scenario .....	189
Table 5.19: Optimized Results of OPNET Simulation for the Core-Edge Scenario.....	191
Table 5.20: Solutions Ranking of Optimized Simulation Results for the Core-Edge Scenario.....	193
Table 5.21: Optimized Results of OPNET Simulation for the Edge-Edge Scenario .....	195
Table 5.22: Solutions Ranking of Optimized Simulation Results for the Edge-Edge Scenario .....	197
Table 5.23: Optimized Results of GNS3 Emulation for the Core-Core Scenario .....	200
Table 5.24: Solutions Ranking of Optimized Emulation Results for the Core-Core Scenario .....	202
Table 5.25: Optimized Results of GNS3 Emulation for the Core-Edge Scenario .....	204
Table 5.26: Solutions Ranking of Optimized Emulation Results for the Core-Edge Scenario.....	206
Table 5.27: Optimized Results of GNS3 Emulation for the Edge-Edge Scenario .....	208
Table 5.28: Solutions Ranking of Optimized Emulation Results for the Edge-Edge Scenario .....	210
Table 5.29: Results of MAXIMA Analytical Modeling for Optimized Simulated Scenarios .....	213
Table 5.30: Solutions Ranking for Total Resilience in Optimized Simulated Scenarios.....	215
Table 5.31: Results of MAXIMA Analytical Modeling for Optimized Emulated Scenarios .....	217
Table 5.32: Solutions Ranking for Total Resilience in Optimized Emulated Scenarios.....	219
Table 5.33: Solutions Ranking Comparison for Total Resilience in All Research Scenarios.....	220
Table 5.1: Primary Results of OPNET Simulation for the Core-Core Scenario .....	326
Table 5.2: Solutions Ranking of Primary Simulation Results for the Core-Core Scenario .....	328
Table 5.3: Primary Results of OPNET Simulation for the Core-Edge Scenario.....	330
Table 5.4: Solutions Ranking of Primary Simulation Results for the Core-Edge Scenario.....	332
Table 5.5: Primary Results of OPNET Simulation for the Edge-Edge Scenario .....	334

Table 5.6: Solutions Ranking of Primary Simulation Results for the Edge-Edge Scenario .....	336
Table 5.7: Primary Results of GNS3 Emulation for the Core-Core Scenario .....	339
Table 5.8: Solutions Ranking of Primary Emulation Results for the Core-Core Scenario .....	341
Table 5.9: Primary Results of GNS3 Emulation for the Core-Edge Scenario .....	343
Table 5.10: Solutions Ranking of Primary Emulation Results for the Core-Edge Scenario.....	345
Table 5.11: Primary Results of GNS3 Emulation for the Edge-Edge Scenario.....	347
Table 5.12: Solutions Ranking of Primary Emulation Results for the Edge-Edge Scenario .....	349
Table 5.13: Results of MAXIMA Analytical Modeling for Primary Simulated Scenarios .....	352
Table 5.14: Solutions Ranking for Total Resilience in Primary Simulated Scenarios.....	354
Table 5.15: Results of MAXIMA Analytical Modeling for Primary Emulated Scenarios .....	356
Table 5.16: Solutions Ranking for Total Resilience in Primary Emulated Scenarios.....	357
Table 5.34: Proposed Solution Results of MAXIMA Analytical Modeling for Simulated Scenarios.....	360
Table 5.35: Proposed Solution Ranking for Total Resilience in All Simulated Scenarios .....	361
Table 5.36: Proposed Solution Results of MAXIMA Analytical Modeling for Emulated Scenarios.....	363
Table 5.37: Proposed Solution Ranking for Total Resilience in All Emulated Scenarios .....	364

## LIST OF FIGURES

Figure 1.2: Four Sights Diagram of CII with Dynamic Cyber Resilience.....	7
Figure 1.3: The Hierarchy of Research Purpose, Goal, and Iterative Four-Objective Cycle.....	10
Figure 2.4: Typical Architecture of SCADA as an Example of ICS-based Infrastructure.....	31
Figure 2.5: Typical Architecture of SWIFT as an Example of ICT-based Infrastructure.....	32
Figure 2.6: Outline the Properties and Characteristics of CII Networks.....	34
Figure 2.7: Mapping CII Layers with OSI Model Layers and Network Topologies.....	36
Figure 2.8: Comparison between Centric-Distributed-Coupled Architectural Couplings.....	41
Figure 2.9: Cyber Interdependencies among Heterogeneous CII.....	45
Figure 2.10: Quadrants of Key Quantitative Cyber Threat Models.....	57
Figure 2.11: CII Performance Changing after Consecutive Cyberattacks.....	74
Figure 3.1: New Perspective of Dynamic Cyber Resilience.....	100
Figure 3.2: Cyber Trustfulness Engineering vs. Cyber Zero-Trust Engineering.....	105
Figure 3.5: Optimized Conceptual Framework of Proposed Solution.....	109
Figure 3.6: Flowchart Diagram of Technology stack for Optimized Proposed Solution.....	124
Figure 4.3: The Research Roadmap.....	140
Figure 4.9: Diagram of General Scheme of Research Scenarios Operationalization.....	148
Figure 4.10: Diagram of Core CII Networks and Edge CII Networks.....	149
Figure 4.11: Diagram of Coupling CII Network Scale-Free Topology.....	150
Figure 4.12: Diagram of Concurrent and Consecutive DDoS Cyberattacks against CII.....	151
Figure 4.13: Diagram of the Core-Core Scenario.....	155
Figure 4.14: OPNET Simulation for the Core-Core Scenario.....	156
Figure 4.15: GNS3 Emulation for the Core-Core Scenario.....	157
Figure 4.16: Diagram of the Core-Edge Scenario.....	158
Figure 4.17: OPNET Simulation for the Core-Edge Scenario.....	159
Figure 4.18: GNS3 Emulation for the Core-Edge Scenario.....	160
Figure 4.19: Diagram of the Edge-Edge Scenario.....	161
Figure 4.20: OPNET Simulation for the Edge-Edge Scenario.....	162
Figure 4.21: GNS3 Emulation for the Edge-Edge Scenario.....	163
Figure 4.4: The Research Methodology.....	170
Figure 4.5: The Levels of Data Analysis in this Research.....	176



Figure 4.6: The Research Process .....	181
Figure 5.13: Optimized Results of OPNET Simulation for the Core-Core Scenario.....	186
Figure 5.14: Optimized Results of OPNET Simulation for the Core-Edge Scenario .....	190
Figure 5.15: Optimized Results of OPNET Simulation for the Edge-Edge Scenario.....	194
Figure 5.16: Optimized Results of GNS3 Emulation for the Core-Core Scenario.....	199
Figure 5.17: Optimized Results of GNS3 Emulation for the Core-Edge Scenario .....	203
Figure 5.18: Optimized Results of GNS3 Emulation for the Edge-Edge Scenario.....	207
Figure 5.19: MAXIMA Analytical Modeling for Optimized Simulated Core-Core Scenario.....	212
Figure 5.20: MAXIMA Analytical Modeling for Optimized Simulated Core-Edge Scenario .....	212
Figure 5.21: MAXIMA Analytical Modeling for Optimized Simulated Edge-Edge Scenario.....	213
Figure 5.22: MAXIMA Analytical Modeling for Optimized Emulated Core-Core Scenario.....	216
Figure 5.23: MAXIMA Analytical Modeling for Optimized Emulated Core-Edge Scenario .....	216
Figure 5.24: MAXIMA Analytical Modeling for Optimized Emulated Edge-Edge Scenario.....	217
Figure 1.1: Cyber Risk Management Diagram.....	284
Figure 2.1: Research Items based on Publication Year by Domain .....	301
Figure 2.2: Research Items based on Sector Contributions by Domain.....	303
Figure 2.3: Research Items based on Number of Citations by Domain .....	305
Figure 4.1: Methodological Choices of this Research.....	308
Figure 4.2: Proportion of Quantitative Research Methods from Cyber Space to Physical Space .....	310
Figure 4.7: OPNET Simulator Setup Settings and Configurations .....	314
Figure 4.8: GNS3 Emulator Setup Settings and Configurations .....	316
Figure 4.9: MAXIMA Platform Setup Settings and Configurations.....	318
Figure 3.3: Primary Conceptual Framework of Proposed Solution .....	321
Figure 3.4: Flowchart Diagram of Technology stack for Primary Proposed Solution.....	323
Figure 5.1: Primary Results of OPNET Simulation for the Core-Core Scenario.....	325
Figure 5.2: Primary Results of OPNET Simulation for the Core-Edge Scenario .....	329
Figure 5.3: Primary Results of OPNET Simulation for the Edge-Edge Scenario.....	333
Figure 5.4: Primary Results of GNS3 Emulation for the Core-Core Scenario.....	338
Figure 5.5: Primary Results of GNS3 Emulation for the Core-Edge Scenario .....	342
Figure 5.6: Primary Results of GNS3 Emulation for the Edge-Edge Scenario.....	346
Figure 5.7: MAXIMA Analytical Modeling for Primary Simulated Core-Core Scenario.....	351

Figure 5.8: MAXIMA Analytical Modeling for Primary Simulated Core-Edge Scenario .....	351
Figure 5.9: MAXIMA Analytical Modeling for Primary Simulated Edge-Edge Scenario.....	352
Figure 5.10: MAXIMA Analytical Modeling for Primary Emulated Core-Core Scenario.....	355
Figure 5.11: MAXIMA Analytical Modeling for Primary Emulated Core-Edge Scenario .....	355
Figure 5.12: MAXIMA Analytical Modeling for Primary Emulated Edge-Edge Scenario.....	356
Figure 5.25: MAXIMA Analytical Modeling of Proposed Solution for Simulated Core-Core Scenarios .....	359
Figure 5.26: MAXIMA Analytical Modeling of Proposed Solution for Simulated Core-Edge Scenarios.....	359
Figure 5.27: MAXIMA Analytical Modeling of Proposed Solution for Simulated Edge-Edge Scenarios .....	360
Figure 5.28: MAXIMA Analytical Modeling of Proposed Solution for Emulated Core-Core Scenarios .....	362
Figure 5.29: MAXIMA Analytical Modeling of Proposed Solution for Emulated Core-Edge Scenarios.....	362
Figure 5.30: MAXIMA Analytical Modeling of Proposed Solution for Emulated Edge-Edge Scenarios .....	363

## LIST OF ABBREVIATIONS AND ACRONYMS

<b>(ISC)<sup>2</sup></b>	International Information System Security Certification Consortium.
<b>aBFT</b>	asynchronous Byzantine Fault Tolerance.
<b>ACE</b>	Application Characterization Environment.
<b>ACRPTB</b>	Advancing Cyber Resilience Principles and Tools for Boards.
<b>AD</b>	Activity Diagram.
<b>ADD</b>	Attack-Defend Dimension.
<b>AIMS</b>	Agent-based Interdependency modeling and Simulation.
<b>APCERT</b>	Asia-Pacific Computer Emergency Response Team.
<b>APS</b>	Automatic Protection Switching Protocol.
<b>ARC</b>	Applied Reconfigurable Computing.
<b>AS</b>	Autonomous Systems.
<b>ATM</b>	Automated Teller Machine.
<b>BGP</b>	Border Gateway Protocol.
<b>BIRR</b>	Better Infrastructure Risk and Resilience.
<b>BSI</b>	British Standards Institution.
<b>CADDY</b>	Cyber Asset Dependency Discovery.
<b>CARVER</b>	Criticality, Accessibility, Recoverability, Vulnerability, Effect, Recognizability.
<b>CASCADE</b>	Loading-Dependent Model of Probabilistic Cascading Failure.
<b>CCNA</b>	Cisco Certified Network Associate.
<b>CCNP</b>	Cisco Certified Network Professional.
<b>CEH</b>	Certified Ethical Hacker.
<b>CI</b>	Critical Infrastructure.
<b>CI3</b>	Critical Infrastructure Interdependencies Integrator.
<b>CIA</b>	Confidentiality, Integrity, Availability.
<b>CIDA</b>	Critical Infrastructure Dependency Analysis.
<b>CII</b>	Critical Information Infrastructure.
<b>CIIP</b>	Critical Information Infrastructures Protection.
<b>CIMS</b>	Critical Infrastructure Modeling Simulation.
<b>CIPI</b>	Critical Infrastructure Protection Initiative.
<b>CIPMA</b>	Critical Infrastructure Protection Modeling and Analysis.
<b>CISIA</b>	Critical Infrastructure Simulation by Interdependent Agent.
<b>CISSP</b>	Certified Information Systems Security Professional.
<b>CLNS</b>	Connectionless Network Service.
<b>CoPP</b>	Control Plane Policing.
<b>COTS</b>	Commercial off the Shelf.
<b>CRAM</b>	Cyber Resilience Assessment Model.
<b>CSIRT</b>	Computer Security and Incident Response Team.
<b>CSPF</b>	Constrained Shortest Path First Algorithm.
<b>CVSS</b>	Common Vulnerability Scoring System.
<b>DAG</b>	Directed Acyclic Graphs.
<b>DCS</b>	Distributed Control Systems.
<b>DDoS</b>	Distributed Denial of Service.

<b>DECRI</b>	Risk and Decision Systems for Critical Infrastructures.
<b>DEWA</b>	Dubai Electricity and Water Authority.
<b>DFD</b>	Data Flow Diagram.
<b>DHCP</b>	Dynamic Host Configuration Protocol.
<b>DHS</b>	U.S. Department of Homeland Security.
<b>DMD</b>	Modular Dynamic Model.
<b>DMZ</b>	Demilitarized Zone.
<b>DNP3</b>	Distributed Network Protocol 3.
<b>DOI</b>	Digital Object Identifier.
<b>DUAL</b>	Diffusion Update Algorithm.
<b>DVS</b>	Distance-Vector Solution.
<b>EBSCO</b>	Elton B. Stephens Company.
<b>EGP</b>	Exterior Gateway Protocol.
<b>EIGRP</b>	Enhanced Interior Gateway Routing Protocol.
<b>ENISA</b>	European Union Agency for Network & Information Security.
<b>ENOC</b>	Emirates National Oil Company.
<b>ERA</b>	Enterprise Risk Assessment.
<b>ERC-SCADA</b>	Evaluating Risk of Cyber-attacks on SCADA.
<b>EU</b>	European Union.
<b>FFIEC</b>	U.S. Federal Financial Institutions Examination Council.
<b>FHRP</b>	First Hop Redundancy Protocol.
<b>FinSIM</b>	Financial System Interdependencies Model.
<b>FIRST</b>	Forum of Incident Response and Security Teams.
<b>FMECA</b>	Failure Mode Effect and Criticality Analysis.
<b>FREMD</b>	Fast Reroute upon Multi-homed Domains.
<b>FRP</b>	Fast Reroute Paths.
<b>FTP</b>	File Transfer Protocol.
<b>FWRP</b>	Floyd-Warshall Routing Protocol.
<b>G8</b>	Group of Eight.
<b>GLBP</b>	Gateway Load Balancing Protocol.
<b>GNS3</b>	Graphical Network Simulator-3 Software.
<b>GNU GPL</b>	GNU is Not Unix General Public License.
<b>GoRAF</b>	Goal-driven Risk Analysis Framework.
<b>GUI</b>	Graphical User Interface.
<b>HCSim</b>	Healthcare Simulation.
<b>HIT</b>	Health Information Technology.
<b>HP-UX</b>	Hewlett Packard UNIX.
<b>HSRP</b>	Hot Standby Router Protocol.
<b>HTC</b>	Hybrid Triple Cryptographic Algorithm.
<b>HTTP</b>	Hypertext Transfer Protocol Secure.
<b>I2Sim</b>	Infrastructures Interdependencies Simulation.
<b>iACLs</b>	Infrastructure Protection Access Control Lists.
<b>iBGP</b>	internal Border Gateway Protocol.
<b>ICMP</b>	Internet Control Message Protocol.
<b>ICS</b>	Industrial Control Systems.

<b>ICT</b>	Information and Communications Technology.
<b>IDMC</b>	Interdependent Markov Chain.
<b>IED</b>	Intelligent Electronic Devices.
<b>IEEE</b>	Institute of Electrical and Electronics Engineers.
<b>IEFT</b>	Internet Engineering Task Force.
<b>IGMP</b>	Internet Group Management Protocol.
<b>IGP</b>	Interior Gateway Protocols.
<b>IGRP</b>	Interior Gateway Routing Protocol.
<b>IMAP</b>	Internet Message Access Protocol.
<b>IN-CORE</b>	Interdependent Networked Community Resilience Modeling Environment.
<b>IoT</b>	Internet of Things.
<b>IPSec</b>	IP Security.
<b>IPv4</b>	Internet Protocol version 4.
<b>IPv6</b>	Internet Protocol version 6.
<b>IRAM</b>	Infrastructure Risk Analysis Model.
<b>IRGC</b>	International Risk Governance Council.
<b>IRRIIS</b>	Integrated Risk Reduction of Information-based Infrastructure Systems.
<b>ISAC</b>	Information Sharing and Analysis Center.
<b>IS-IS</b>	Intermediate System to Intermediate System Protocol.
<b>ISO</b>	International Organization for Standardization.
<b>IT</b>	Information Technology.
<b>ITIL</b>	Information Technology Infrastructure Library.
<b>LAN</b>	Local Area Network.
<b>LIRP</b>	Link-State Information Refreshing Protocol.
<b>LISTA</b>	Library, Information Science, and Technology Abstracts.
<b>LSS</b>	Link-State Solution.
<b>Maxima</b>	Macysma Computer Algebra Software.
<b>MBRA</b>	Model-Based Risk Assessment.
<b>MCSA</b>	Microsoft Certified Systems Administrator.
<b>MCSE</b>	Microsoft Certified Systems Engineer.
<b>MD5</b>	Message-Digest Algorithm, Type 5.
<b>MITM</b>	Man-In-The-Middle.
<b>MITRE</b>	Massachusetts Institute of Technology Research & Engineering.
<b>MOEs</b>	Cyber Resiliency Measures of Effectiveness
<b>MPLS</b>	Multiprotocol Label Switching.
<b>NATO</b>	North Atlantic Treaty Organization.
<b>NCIIPC</b>	National Critical Information Infrastructure Protection Centre.
<b>NEC</b>	Nippon Electric Company.
<b>NEMO</b>	Net-Centric Effects-based Operations Model.
<b>NEXUS</b>	Real-Time Data Fusion and Network Analysis for Urban Systems.
<b>NIPP-RMF</b>	National Infrastructure Protection Plan – Risk Management Framework.
<b>NISD</b>	National Information Security Directive.
<b>NIST</b>	U.S. National Institute of Standards and Technology.
<b>NSAP</b>	Network Service Access Point.
<b>NSRAM</b>	Network Security Risk Assessment Modeling.

<b>OECD</b>	Organization for Economic Cooperation and Development.
<b>OFR</b>	U.S. Office of Financial Research.
<b>OGC</b>	Open GIS Consortium.
<b>OOP</b>	Object-Oriented Programming.
<b>OpenSSL</b>	Open Secure Sockets Layer.
<b>OPNET</b>	Optimized Network Engineering Tools Software.
<b>OPS</b>	Optimized Proposed Solution.
<b>OSI</b>	Open Systems Interconnection Model.
<b>OSPF</b>	Shortest Path First Protocol.
<b>PC</b>	Personal Computer.
<b>PCRN</b>	Path Computation for Resilient Networks.
<b>PDM</b>	Path Diversification Mechanism.
<b>PKI</b>	Public Key Infrastructure Cryptography.
<b>PLC</b>	Programmable Logic Controllers.
<b>PNNL</b>	Pacific Northwest National Laboratory.
<b>POP3</b>	Post Office Protocol 3.
<b>POS</b>	Point-of-Sale.
<b>PPP</b>	Point-to-Point Protocol.
<b>PPS</b>	Primary Proposed Solution.
<b>PRS</b>	Path-Rule Solution.
<b>QoS</b>	Quality-of-Service.
<b>QualNet®</b>	Network Simulation Software.
<b>R4</b>	Robustness, Redundancy, Resourcefulness, Rapidity.
<b>RAMCAP</b>	Risk Analysis and Management for Critical Asset Protection.
<b>RCS</b>	Random Constant Spread Model.
<b>REP</b>	Resilient Ethernet Protocol.
<b>Restore®</b>	Interdependent Repair and Restoration Processes Tool.
<b>RFP</b>	Reliable Flooding Protocol.
<b>RHCSA</b>	Red Hat Certified System Administrator.
<b>RI</b>	Resilience Index.
<b>RIP</b>	Routing Information Protocol.
<b>RPR</b>	Resilient Packet Ring Protocol.
<b>RSA</b>	Rivest, Shamir, Adleman Protocol.
<b>RSTP</b>	Rapid Spanning Tree Protocol.
<b>RTU</b>	Remote Terminal Unit.
<b>SAGE</b>	Sarah and George Publishing.
<b>SARA</b>	Scenario-based Approach to Risk Analysis.
<b>S-BGP</b>	Secure Border Gateway Protocol.
<b>SCADA</b>	Supervisory Control and Data Acquisition.
<b>SCRAM</b>	Structured Cyber Resiliency Analysis Methodology.
<b>SDLC</b>	Software Development Life Cycle.
<b>SHA</b>	Secure Hash Algorithm.
<b>SMTP</b>	Simple Mail Transfer Protocol.
<b>So-BGP</b>	Secure Origin BGP.
<b>SPB</b>	Shortest Path Bridging Protocol.

<b>SRA</b>	U.K. Solicitors Regulation Authority.
<b>S-RAM</b>	Security Risk Assessment Methodology.
<b>SSD</b>	Static-Dynamic Dimension.
<b>STP</b>	Spanning Tree Protocol.
<b>STRIDE</b>	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege.
<b>SWIFT</b>	Society for Worldwide Interbank Financial Telecommunication.
<b>SYN-ACK</b>	Synchronize Acknowledge Message.
<b>T101</b>	IEC 60870-5-101 (IEC101) Protocol.
<b>TCP/IP</b>	Transmission Control Protocol / Internet Protocol.
<b>TLS</b>	Transport Layer Security Protocol.
<b>T-MAP</b>	Threat Modeling Attack Paths.
<b>TTL</b>	Time-to-Live Security Check.
<b>UDP</b>	User Datagram Protocol.
<b>UML-CI</b>	Unified Modeling Language-Critical Infrastructures.
<b>UNISDR</b>	United Nations International Strategy for Disaster Reduction.
<b>VoIP</b>	Voice over Internet Protocol.
<b>VPN</b>	Virtual Private Network.
<b>VRRP</b>	Virtual Router Redundancy Protocol.
<b>WEF</b>	World Economic Forum.
<b>WWW</b>	World Wide Web.

# CHAPTER 1. INTRODUCTION

Many critical infrastructures have been physically separated in the past since the technology boom in the 1970s (Cedergren et al., 2018). However, the revolution of information and communication technologies are stimulating globalization, cutting down the costs of consolidating operations, providing significant social and economic benefits, and improving efficiency, productivity, and competitiveness worldwide (Dan-Suteu & Gânsac, 2020).

Today, modern societies have become more dependent on the reliability, availability, security, and resiliency of many critical information infrastructures by tunneling data to central processing locations (Gatchin & Sukhostat, 2019). As a result, enormous amounts of data and an increasing number of transactions are flowing over the Internet at every moment alongside varying degrees of cyber protection and severe consequences of their malfunctioning (Hansen, 2019).

The critical information infrastructures are networked physical and information-based assets, facilities, which, if damaged, have vast and profound impacts on national security, people well-being, governmental services, and corporate business (Jiang et al., 2018). These interdependent infrastructures have to be cyber resilient against various vectors of cyberattacks (Labaka et al., 2017).

This chapter motivates the research of the dynamic cyber resilience for interdependent critical information infrastructures, discusses the problem statement and thesis purpose, and describes the research scope, assumptions, significance, and originality. In addition, it establishes critical research questions and formulates its appropriate hypotheses from observations of critical information infrastructure challenges to investigate the thesis objectives. Also, it shares the research contributions to the knowledge for the academic community and professional experts.



## **1.1 Research Context**

The topic of this research falls under the umbrella of cyber risk management. It is the overall process for identifying, defining, and analyzing cyber risks to accept, avoid, convey, or control them to a satisfactory level at an affordable cost (Hokstad et al., 2012). Cyber risks are the potentials for undesired outputs caused by cyber events determined by their likelihood and associated consequences (Dunn & Kristensen, 2020).

On the other hand, at the beginning of the third millennium, the world realized the massive influence with vast impacts of the accelerating and the growing threat of cyberattacks against interdependent critical information infrastructures around the globe, from energy facilities, power grids, telecommunications to financial services and business operations, are no longer just theories (Dong et al., 2013).

Many incentives behind the cyberattacks on critical information infrastructures include political statements, financial gains, power show off, and destructive intentions (AlMajali et al., 2012). Cyberattacks take many forms and have different degrees of impact. Based on that, several times over the last two decades, the world has held its breath because of the number of sophisticated cyberattacks on vital critical information infrastructures (Castillo et al., 2019).

For example, and not limited to the first known cyberattack on an entire country, creating instability and disturbance for lasted weeks in a NATO country like Estonia, was hit in 2007 (Cazorla et al., 2016). Unprecedented levels of internet traffic took down Estonian banks' online services, media outlets, and government bodies. DDoS botnets sent massive spam waves, and massive amounts of automated requests swamped servers (Du et al., 2015).

Also, the 2010 attack on Iran's nuclear plant at Natanz has a special place in the history books.

The so-called Stuxnet worm made its first public appearance then, managing to bring the nuclear plant to a halt. The Stuxnet was engineered to damage motors commonly used in uranium-enrichment centrifuges by sending them spinning out of control. It succeeded in temporarily disabling about one thousand centrifuges (Georgiev & Nikolova, 2017). This cyber-attack almost caused a catastrophe similar to the Ukrainian Chernobyl reactor disaster in 1982 (Herrmann et al., 2011).

Likewise, the U.S. northeast blackout in 2014 that caused 11 deaths and an estimated \$6 billion in economic damages were threatened by cyberattacks at least 245 times over 2014 (Fang & Sansavini, 2017). After one year, particularly in December 2015, Ukraine experienced an unprecedented assault on its power grids (Jahromi et al., 2019).

The cyberattack led to widespread electricity outages using the Black Energy 3 malware hidden in fake Microsoft Office attachments and delivered spear-phishing emails to the employees. Hackers infiltrated three energy companies and shut down power generation temporarily in three regions of Ukraine. It left nearly 700 thousand people in the dark without electricity for more than 6 hours in the middle of winter (Prav, 2019).

In 2017, the cyber attackers configured Triton malware specifically for industrial control systems at Saudi Arabia's state-run oil giant, Saudi Aramco, and wiped the hard drives of workstations, led to the stop of the primary operations in four oil refiners for a month (Qiu et al., 2018).

In the same year, a global cyberattack using the so-called WannaCry ransomware lockdown more than 300,000 infected computers in 150 countries worldwide and crippled many critical information infrastructures (Pipyros, 2019). For instance, the national health system across the U.K. with losses up to £100 million, crippled computers in an international shipper FedEx has cost \$19 million, and the Czech security firm's industrial control system Avast was wholly failed.

Simultaneously, the countries most affected were Russia, Taiwan, Ukraine, and India (Kochedykov et al., 2020).

Also, Nitro's cyber-attacks that involved several companies in the chemical sector occurred mainly in the USA, Bangladesh, and Argentina (Shang et al., 2017). Duqu Virus attacks reveal private information, configurations, and accesses to critical information infrastructure in North Korea and Italy, as well as the behavior of Flame worm, was initially designed to open back doors, infect and modify functions, in addition to stealing confidential data, destroying information in Malta, among others (Shaburov & Alekseev, 2019).

According to the most recent annual reports and professional surveys that observed the cyber resilience state, the cyberattacks doubled in 2020 to more than 317 million. Furthermore, they hit 90% of critical information infrastructures with expected costs on the world economy from \$400 billion a year to \$6 trillion between 2021-2025 (Bissell et al., 2020).

Many studies have addressed the cyber vulnerabilities of the interdependent critical information infrastructures and handled cyberattacks' challenges. These studies are divided into two perspectives, policy and technology (McCollum et al., 2018). Researchers in both views continually attempt to debate the need to shift the paradigm of cyber risk management from cybersecurity concepts towards cyber resilience concepts (Strom et al., 2017).

As a quick survey, numerous public cyber governance policies, international security strategies, and risk management practices are published globally in the policy perspective at unprecedented sectoral levels (Prior, 2015). *See Appendix A: Research Background.*

## **1.2 Rationale and Motivation**

Many critical infrastructure sectors, such as transportation, telecommunications, power grids, and banking services, are vital to modern economies and societies (Pedroni et al., 2015). Therefore, their incapacitation or destruction would have a debilitating and cascading effect; due to their dependence on massive information technology and shared significant resources and CII networks that continually take place among these different industry sectors (Orojloo & Azgomi, 2017).

In addition, all critical information infrastructures are subject to rapid change during their operational lifetime to fulfill the increasing demand for services requested by the different stakeholders (Conklin & Kohnke, 2017). These changing conditions, unpredictability, extreme uncertainty, and rapid evolution of potential cyber threats create asymmetry situations between the cyber attacker and cyber defender that justify shifting towards dynamic cyber resilience (Begishev et al., 2019).

The cyber attacker can focus on one target only and succeed once to achieve the goals (Yuan et al., 2014). In contrast, the cyber defender must protect everything from anticipated cyber threats every time and unknown ones and maintain the balancing status between cyber protection requirements and appropriate CII performance levels (Ullah et al., 2018).

The focal point starts from the fact that there is no complete cyber protection a hundred percent to interdependent critical information infrastructures (Dong et al., 2012). In other words, the conventional cybersecurity technologies today can handle 99% of the cyber threats. However, the remaining ones may cause catastrophic cascading failures. Nevertheless, this situation can be coped with cyber continuity (Johnson, 2015).

Therefore, the research community has three points of view for understanding the relationship between cyber risk management and dynamic cyber resilience. The first point of view presents dynamic cyber resilience as an alternative to cyber risk management (Bosetti et al., 2016). It argues that approaches to cyber risk management are insufficient for confronting dynamic cyber threats with high complexity. Instead, it focuses on the CII design by assessing, analyzing the network system's cyber vulnerabilities and enhancing their functions to increase the dynamic cyber resilience to any possible cyber threats (Nezamoddini et al., 2017).

The second point of view considers dynamic cyber resilience as a part of cyber risk management. The core idea is that dynamic cyber resilience complements cyber risk management as it provides a systematic approach to deal with the so-called remaining cyber threats (Hayel & Zhu, 2015). However, these are impossible to prevent entirely. Hence, it is crucial to enhance a network system's ability to integrate potential cyber threats into cyber risk management's operational activities. (Leslie et al., 2018).

The third and final point of view describes dynamic cyber resilience as the overarching cyber risk management goal. Therefore, it does not concentrate on cyber threat avoidance but aims to deal with cyber consequences and reduce their impacts, enabling the network system to survive from cyber threats and quickly recover (Tatar, 2020).

Each point of view focuses separately on one component of cyber risk management, whether cyber vulnerability, cyber threat, or cyber consequences. Therefore, they provide an incomplete solution and leave even more traditional cyber risk assessment approaches that cannot adequately address the challenges of cyber risks faced by interdependent critical information infrastructures (Kott & Linkov, 2019).

For that reason, the motivation of this research stems from the persistent need for conceptual

transformation from the mono view of cyber risk management to the comprehensive view of dynamic cyber resilience (Bergström et al., 2015). Several advanced studies in the area of critical information infrastructures attempt to shift the paradigm from the concepts of cybersecurity towards the concepts of dynamic cyber resilience from four sights (Sansavini, 2017), (Severson et al., 2018), (Tonhauser & Ristvej, 2019), (Rose, 2019), and (Mode, 2020).

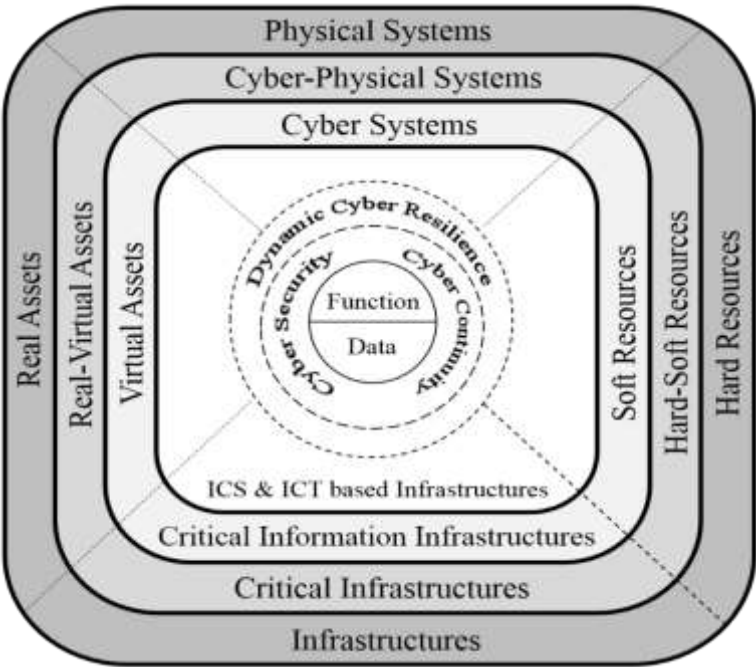


Figure 1.2: Four Sights Diagram of CIIs with Dynamic Cyber Resilience

This research combined these sights in one diagram to illustrate the relationships of critical information infrastructures with dynamic cyber resilience concepts. In the outer shell, as shown in Figure 1.2, the sight of physical systems, real assets, hard resources, or infrastructures are the changeable subject of many research efforts in the past, and several models have proposed to address resiliency that converged primarily on cyber restoration in cases of single or double cyber-attacks (Moraitis et al., 2020).

However, with the ever-increasing reliance on CII network-based services in today’s society, the

issue of cyber resilience in cyberattack scenarios has started to gain a great deal of attention (Lopez et al., 2017). The middle shell studies focus on the interaction between the physical and cyber parts in the cyber-physical systems, real-virtual assets, hard-soft resources, or critical infrastructures (Alcaraz, 2018). Same wise in the inner shell but with purely cyber deliberation of research works for the cyber systems, virtual assets, soft resources, or critical information infrastructures (Viswanathan et al., 2017).

On the basis of the cyber resilience concept that supports the ability to react to, survive, and recover from damaging cyberattacks. The above diagram's core describes integrating both parts of the dynamic cyber resilience, cybersecurity, and cyber continuity, to protect the function and data in the ICS-based and ICT-based critical information infrastructures (Wang et al., 2019).

### **1.3 Research Gaps and Problem Statement**

The relevant literature on this research topic was published over the past two decades; It turns out that there are critical research gaps in the most related studies that mainly focus on a few aspects merely in the areas of cyber resilience and critical information infrastructures. They are:

(1) ***Limited studies on critical information infrastructures compared to critical infrastructures.***

The majority of studies focus on handling the issues of physical resilience and cyber-physical resilience rather than cyber resilience such as (Canzani, 2016), (Deng et al. 2017), (Grafenauer et al., 2018), (Maglaras et al., 2018), (Ferreira, 2019), and (Alqahtani, 2020).

(2) ***Lack of conducted research on cyber interdependency of heterogeneous critical information infrastructures.*** ICS-based CII and ICT-based CII together, where the widespread scientific efforts consternate cyber interdependency of homogeneous critical information infrastructures, i.e. (ICS-based CII or ICT-based CII separately). For instance,

(Mattioli & Moulinos, 2015), (Li et al., 2018), (Haque et al., 2019). (Chowdhury et al., 2020), and (Dan-Suteu & Gânsac, 2020).

- (3) ***The absence of works deals with the scale-free topology vulnerability of coupled networks of critical information infrastructures.*** The common ones discuss the technical vulnerabilities of critical information infrastructures such as operating systems, legacy characteristics, and administration issues. For example, (Hadjisaid et al., 2010), (Schneider et al., 2013), (Tian et al., 2015), (Cao et al., 2017), and (Fotouhi et al., 2017).
- (4) ***Shortage of research discussions on the concurrent and consecutive cyberattacks that execute as cyber-attack waves within the same time frame with serial order-independent against critical information infrastructures causes common, escalating, and cascading failures.*** At the same time, the recent discussions dedicated to the single or multiple cyberattacks with spaced time intervals and cascading failures only such as (Hui et al., 2014), (Du et al., 2015), (Canzani, 2016), (Di Pietro et al., 2017), (Palleti et al., 2018), and (Kochedykov et al., 2020).
- (5) ***No research papers were identified concerning the dynamic cyber resilience for interdependent critical information infrastructures using cyber zero-trust engineering.*** Most of the existing papers are about cyber risk management, cybersecurity, and cyber resilience in critical infrastructures using cyber trustfulness engineering as (Filippini & Silva, 2012), (Balchanos et al., 2012), (Rasouli et al., 2014), (Björck et al., 2015), (Liu et al., 2016), (Alcaraz, 2018), (Petrenko et al., 2019), (Brennan et al., 2019), and (Carias et al., 2019).

The problem statement of this research is that there is still missing nowadays a comprehensive technology solution of dynamic cyber resilience using cyber zero-trust engineering in interdependent critical information infrastructures enables bridging the above research gaps



recommended by many studies mentioned above.

It also highlights the need to adequately address the related issues for shifting paradigms towards dynamic cyber resilience to balance proactive and reactive perspectives at both theoretical and empirical levels.

## 1.4 Research Purpose, Questions, and Hypotheses

The thesis's principal research aims to seek a theoretical and empirical solution to bridge the critical research gaps resulting in an intensive review of relevant literature. Therefore, the research goal is to create a novel proposed solution. Such a goal accomplishes by an iterative four-objective cycle that includes the research objectives of development, implementation, evaluation, and optimization of the proposed solution. Each aim is several research questions with associated hypotheses, as shown in Figure 1.3.



Figure 1.3: The Hierarchy of Research Purpose, Goal, and Iterative Four-Objective Cycle

The first research objective (RO1) is developing a conceptual framework and prototyping a novel proposed solution to enhance dynamic cyber resilience capabilities for interdependent critical information infrastructures to continuously deliver their missions and core services under concurrent and consecutive cyberattacks within acceptable timelines and performance levels. The

research questions with associated hypotheses (Barami, 2013), (Ledesma, 2014), (Barrett & Conostas, 2014), (Laderman et al., 2015), (Dimase et al., 2015), (Labaka et al., 2016), (Bosetti et al., 2016), (Haque et al., 2018), (Wu et al., 2020), and (Grachkov et al., 2020) that can be formulated to address with the RO1 include the following:

- Research Question 1 (RQ1): Theoretically, how can the conceptual framework of the proposed solution bridge the critical research gaps and underpin dynamic cyber resilience?

RQ1 Hypothesis:

- H<sub>1</sub>: The conceptual framework of the proposed solution can theoretically bridge the critical research gaps and underpin dynamic cyber resilience.

- Research Question 2 (RQ2): Empirically, how can the technology stack of the proposed solution bridge the critical research gaps and underpin dynamic cyber resilience?

RQ2 Hypothesis:

- H<sub>2</sub>: The technology stack of the proposed solution can empirically bridge the critical research gaps and underpin dynamic cyber resilience.

The second research objective (RO2) is implementing the proposed solution using analytical modeling, emulated experiments, and computing simulations. This set of research methods and preparing the generation requirements of testing scenarios and studying the influence of the scale-free topology structure of CII networks on its ability to fulfill dynamic cyber resilience capabilities successfully. Understanding the cascading effects in the coupled network of interdependent CIIs against concurrent and consecutive cyberattacks. The research questions with associated hypotheses (Marais & Uday, 2015), (Hehenberger et al., 2016), (Sharif & Sadeghi-Niaraki, 2017), (Nan & Sansavini, 2017), (Grafenauer et al., 2018), (Castillo et al., 2019), (Dan-

Suteu & Gânsac, 2020), (Chowdhury et al., 2020), and (Kochedykov et al., 2020) that can be formulated to address with the RO2 include the following:

Research Question 3 (RQ3): Does the proposed solution reduce the disruptive effects among coupled CII networks against concurrent and consecutive cyberattacks?

RQ3 Hypothesis:

- H<sub>3</sub>: The proposed solution reduces the disruptive effects among coupled CII networks against concurrent and consecutive cyberattacks.

The third research objective (RO3) evaluates the capabilities of dynamic cyber resilience for the proposed solution based on the quantitative cyber resilience factors correlated with considered networking metrics. Also, performing results analysis of the proposed solution, comparing it with the results of previously standard solutions through identified specific scenarios with the defined network topology, potential cyberattacks, and research methods, and determined the impacts on interdependent CIIs failures in desired aspects of the proposed solution may be preferred over standard solutions commonly discussed in the literature. The research questions with associated hypotheses (Creese et al., 2011), (Bhuyan et al., 2015), (Banescu et al., 2015), (Wright et al., 2016), (Liu et al., 2017), (McCollum et al., 2018), (Luijff et al., 2018), (Mbanaso et al., 2019), (Sepúlveda-Estay et al., 2020), and (Faramondi et al., 2020) that can be formulated to address with the RO3 include the following:

- Research Question 4 (RQ4): Can cyber resilience factors and networking metrics provide quantitative evaluation appropriately of dynamic cyber resilience capabilities for the proposed solution and enable comparisons with standard solutions?

RQ4 Hypothesis:

- H<sub>4</sub>: Cyber resilience factors and networking metrics appropriately evaluate dynamic cyber resilience capabilities for the proposed solution and enable comparisons with standard solutions.

The fourth research objective (RO4) is optimizing the primary proposed solution after evaluation to enhance interdependent critical information infrastructures' dynamic cyber resilience capabilities. The new improvements foster the optimized proposed solution by advancing knowledge of the primary proposed solution's strengths and weaknesses. In addition, redesigning the optimization alternatives of the proposed solution and their relations to each other to become more efficient, effective, and able to handle the potential cyberattacks' cascading failures and increase the dynamic cyber resilience to excel the standard solutions. The research questions with associated hypotheses (Davendralingam & DeLaurentis, 2013), (Labaka et al., 2017), (Fang & Ouyang, 2017), (Ouyang, 2017), (Abdin et al., 2019), (Zio & Fang, 2019), and (Brigantic et al., 2020) that can be formulated to address with the RO3 include the following:

- Research Question 5 (RQ5): How can the proposed solution's improvements optimize the capabilities of dynamic cyber resilience for CII?

RQ5 Hypothesis:

- H<sub>5</sub>: The improvements of the proposed solution can optimize dynamic cyber resilience capabilities for CII.
- Research Question 6 (RQ6): Does the optimized proposed solution achieve optimal results in dynamic cyber resilience capabilities than standard solutions?

RQ6 Hypothesis:

- H<sub>6</sub>: The optimized proposed solution achieves the optimal results in dynamic cyber resilience capabilities than standard solutions.
- Research Question 7 (RQ7): Is the dynamic cyber resilience of the optimized proposed solution higher than the dynamic cyber resilience of standard solutions?

RQ7 Hypothesis:

- H<sub>7</sub>: The dynamic cyber resilience of the optimized proposed solution is higher than the dynamic cyber resilience of standard solutions.

## **1.5 Scope, Assumptions, and Originality**

The literature's fundamental concerns cover the main challenges associated with critical infrastructures: natural-made and human-made causes, inner and outer boundaries, and direct and indirect targets (Heinbockel et al., 2013). Also, malicious and non-malicious objectives, deliberate and indeliberate intents, competent and incompetent capabilities, software, and hardware dimensions (Chaves et al., 2017). Besides, physical and logical medium domains, nodes and links scopes, major and minor significances, long-lived and short-lived persistence, and single and multiple repetitions (Caron, 2019).

This research's scope mainly focuses on the open datasets collected from various sources and analyzes the cyber failure impacts through quantitative research methods such as analytical modeling, emulated experiments, and computing simulations to support the developing, implementing, evaluating, and optimizing the proposed solution.

Such a solution innovates novel network layer-3 technology and provides in-depth insights into the dynamic cyber resilience to enhance their capabilities about three key themes. Firstly, the

influence of the scale-free topology structure of the coupled network in interdependent CIIs. Secondly, the cascading effects are caused by concurrent and consecutive cyberattacks. Thirdly, the results of dynamic cyber resilience for the proposed solution are compared with standard solutions.

The investigation of these three themes contributes to bridging the critical research gaps in the literature to the extent that it helps clarify the significant role of dynamic cyber resilience in building more resilient networks of interdependent critical information infrastructures.

Instead, this research focuses on the technology perspective of cyber resilience, quantitative research methods, external cyberattacks, cyber parts of critical infrastructures, and scale-free topology vulnerability of critical information infrastructures.

The related areas that are out of scope and were not addressed in this research include the policy perspective of cyber resilience, qualitative research methods, cost-benefit calculations, natural hazards, insider cyberattacks, physical parts of critical infrastructures, and technical and administrative vulnerabilities of critical information infrastructures.

Additionally, a set of research assumptions were made in the process of designing the thesis methodology, implementing the proposed solution, and performing testing scenarios as follows:

- Dynamic cyber resilience can be measured quantitatively. This assumption stems from the idea of resilience operationalization put forward by Klein et al. (2003).
- Interdependent CII adopts one technology solution when building dynamic cyber resilience. Support for this assumption was founded in Handmer and Dovers' (1996) typology of resilience literature.

- Dynamic cyber resilience is evolving and controlled by numerous factors. Connor and Zhang (2006) and Fleming and Ledogar (2008) elaborate on this assumption's pillars.
- Interdependent CII networks have scale-free topology structures at a logical level. This assumption was established by Faloutsos et al. (1999) and modeled by Barabási (1999).
- Targeted concurrent and consecutive cyberattacks against interdependent CIIs are existing and sophisticated. This assumption was obtained from the Petri-Nets threat modeling of dynamic systems by Davied and Alla (1994).

Moreover, this research is original and provides beneficial elements clarified from two aspects. At first, future reference. The novel proposed solution presented in this research is considered a source material that may serve the research community to find the appropriate answers to the frequent questions regarding critical research gaps and enhance dynamic cyber resilience capabilities for interdependent CIIs.

In the second place, the practical promotion. The thesis's proper recommendations based on the characteristic findings of the emulated and simulated comparisons between the proposed solution and standard solutions over primary and optimization stages support the researchers' substantial endeavors to increase the dynamic cyber resilience for interdependent CIIs.

Additionally, the significance of this research considers both academia and industry directions. In academia, the lack of scientific consensus on the standard conceptual framework of dynamic cyber resilience for interdependent CIIs poses a problem for researchers.

The proposed solution's architecture design allows further research into the cyber efficiency and effectiveness of the most common solutions and encourages developing a standardized framework of dynamic cyber resilience. However, it argued that verifiable measures of dynamic

cyber resilience capabilities are becoming increasingly important and require progressing a consent on the effective constitution for interdependent CII networks.

On the other hand, the industry direction focuses on quantifying dynamic cyber resilience for interdependent CII networks to identify cyber vulnerabilities exploited by cyberattacks. The prototyping and optimizing of the proposed solution help the professionals collect, maintain, and update information about dynamic cyber resilience capabilities. The establishment of empirical comparisons through emulations and simulations in this research provides the practitioners concerning ensure that concurrent and consecutive cyberattacks can be addressed.

## **1.6 Research Contributions**

The thesis has several progressive contributions to both knowledge and practice. The scientific value of these contributions profoundly enhanced the common cross understanding of the research community for the new perspective of cyber risk management towards dynamic cyber resilience.

Furthermore, the study represented the originating benefits of the optimized conceptual framework and the technology stack for the novel proposed solution to boost dynamic cyber resilience capabilities of interdependent critical information infrastructures based on cyber zero-trust engineering. This research contribution is summarized in the following areas:

- ***1<sup>st</sup> Contribution: The thesis bridges the critical research gaps for interdependent CIIs.***

The systematic literature review in this research revealed critical research gaps that the number of studies for heterogeneous CIIs (combination of ICS CIIs and ICT CIIs) is minimal. Similarly, regarding scale-free topology vulnerability of coupled CII networks against concurrent and consecutive cyberattacks. At large, it also explored and analyzed that all



available standard technologies are based on cyber trustfulness engineering; therefore, they have no comprehensive solution to enhance the dynamic cyber resilience capabilities of interdependent CIIs.

- ***2<sup>nd</sup> Contribution: The thesis focuses on a new cyber zero-trust engineering research area.***

The novel proposed solution in this study is starting a new research area by introducing a conceptual framework and technology stack on the basis of cyber zero-trust engineering at the network layer-3 OSI model for the first time. Unlike the standard solutions, all-inclusive modules of the proposed solution embedded with fundamental concepts, algorithms, and protocols empower the academics to boost the dynamic cyber resilience capabilities in interdependent critical information infrastructures under concurrent and consecutive cyberattacks.

- ***3<sup>rd</sup> Contribution: The thesis highlights the vital importance of optimization envisions.***

The optimization of the proposed solution gives further envisions for the research community concerning the vital importance of the revised phasing and multi-evaluation stages to reach precise findings and accurate interpretations. This study proved that the optimized achieves optimal total dynamic cyber resilience results by successfully improving the conceptual framework and technology stack compared to the primary proposed solution and other standard solutions simultaneously. This optimization might also help other knowledge disciplines where dynamic cyber resilience is crucial at national economic and security.

- ***4<sup>th</sup> Contribution: The thesis connects theory to the practice of dynamic cyber resilience.***

The well-structured methodology and research process enhances particular understanding and designing dynamic cyber resilient of the CII networks via the strategic use of quantitative

multi-methods for data collection, analysis, and validation. Thereby, this thesis is a step forward, linking up the research implementation of critical services and cyber-infrastructures for Dubai as a smart city showcase with the internal and external characteristics of CII environment. This linkage allows professional experts to guide practically efficient decision-making for extended development and application to predominantly smart cities and support global dynamic cyber resilience readiness.

- ***5<sup>th</sup> Contribution: The thesis presents significant findings for the research community.***

The marshaling of two types of research data: primary data collected empirically from the unique testing scenarios and secondary data derived from the existing literature studies analyzing, comparing, and defining their inter-relationships to build significant findings that other interested researchers could use in relevant domains. Especially the scholars are facing difficulties in observing genuine data of cyberattacks. These datasets are costly to generate and collect due to the instrumentational complexity and special labs' requirements with dedicated setups that are not always available.

- ***6<sup>th</sup> Contribution: The thesis generates new knowledge in the neoteric research domain.***

The neoteric domain application of technical instrumentation and scenarios operationalization was organized and performed to test, validate, and analyze the conceptual framework of dynamic cyber resilience capabilities for interdependent CII networks to cope with concurrent and consecutive cyberattacks. Similarly, the modernistic association of influential factors and evaluation metrics was discovered and conducted to strengthen the overall implemented experience. The study was led to generate new knowledge supporting filling the missing gap

in the literature and identifying the smooth and effective research implementation characteristics, focusing on coupled and heterogeneous CIIs.

- ***7<sup>th</sup> Contribution: The thesis shapes future trends of dynamic cyber resilience research.***

The thesis shaped the understanding of the cyber zero-trust engineering for the cyber resilience industry by analyzing current trends of standard solutions and forecasting future CIIs market behaviors. Apart from the theoretical issues identified through literature review, the research entails adopting the proposed solution from the primary phase to the optimization phase to render the needed guidance based on or influenced by results for formalizing essential aspects of the new standard to provide cyber protection that can be explored and developed different alternative solutions.

In sum, from pure theoretical foundations to simulated and emulated models for reaching applied relevance, the thesis introduced the oriented design for bridging theory and practice. Besides, the relevant mention is the important collaboration among industry and academia actors. The priority point is to enable an improved proposed solution to implement effective dynamic cyber resilience with enhancing its development and optimization, which highly supported the main research contributions.

## **1.7 Author's Related Publications**

This thesis has been inspired by the author's preliminary works between 2017 and 2021 in cyber resilience, cybersecurity, and cyber networks. He is playing two roles: author and peer-reviewed. In one of his papers, the author presented an in-depth survey of the challenges and opportunities, introducing visionary ideas, research strategies, and future trends expected for future-oriented technology solutions like Cloud Computing, the Internet of Things (IoT), and Big Data. These

technology solutions play crucial roles in cyber-physical systems and significantly influence smart cities' critical information infrastructures.

In another work, the author developed a proposed solution of a hybrid end-to-end VPN security approach that combines the IPSec/IPv6 and OpenSSL cybersecurity approaches that can secure smart objects of the Internet of Things (IoT) in different critical areas information infrastructures. This proposed solution achieves the best combinations of complementary advantages of the IPSec/IPv6 VPN approach and the OpenSSL VPN approach and eliminates their shortcomings. Performance evaluation of the proposed hybrid approach and the analysis of the comparative performance of both IPSec/IPv6 VPN and OpenSSL VPN approaches assessed in terms of a set of standard measurements, such as throughput, round-trip delay, and bandwidth consumption.

Likewise, the author developed the first novel tool for the Arabic question-answering app. The proposed solution enables the users to find accurate, direct, and quick answers for many Arabic language questions anywhere and anytime through their Android smartphones. The proposed solution's architecture framework was implemented, deployed, and tested based on the android studio platform.

Furthermore, in one more research, the author analyzes the topology structure and critical influences for the online social networks in the space of cybersecurity awareness. They understood better the relationships among network actors over time through social data mining and patterns examining social network growth. Following the quantitative research methodology, the hypotheses were tested and analyzed using appropriate statistical tests, such as correlations, t-tests, and regression.

In the broader field of cyber resilience, the author provided in the recent paper an analysis of the cyber fragility for interdependent networks in the form of cascading failures is complemented by

the presentation of a measure of structural coupling for critical infrastructures. Experiments with generating random cyberattacks to emulate interdependent networks show that cascading failures initiated in one critical infrastructure have a high possibility of leading to a collapse of another coupled critical infrastructure, even before leading to total failure in the originating interdependent network.

Outputs of the author's comparative study demonstrate the performance results of well-established cyber resilience approaches. Furthermore, such comparisons motivated examples of developing valuable tools and instruments to explore the cyber resilience of interdependent critical information infrastructures by combining two quantitative research methods that account for several evaluation metrics.

The author has done the above self-funded works and published them online through a global publisher with good publication impact factors after processing peer and blind reviews. These works introduce a set of contributions to build many aspects in the context of the thesis topic and improve the overall research methodology and results adopted to develop the proposed solution for dynamic cyber resilience of interdependent CIIs as the following:

A. Journal Publication | Impact Factor: 5.570 | Status: Published | Role: Corresponding Author.

Juma, M., Monem, A. A., & Shaalan, K. (2020). *Hybrid End-to-End VPN Security Approach for Smart IoT Objects*. Journal of Network and Computer Applications, (158)102598, pp.1-12.

Link: <https://www.sciencedirect.com/science/article/abs/pii/S1084804520300722>

Contribution to this thesis: 1) Defining problem statement, research objectives, questions, and hypotheses. 2) Developing a conceptual framework and coding the algorithms. 3) Implementing of proposed solution based on popular cyber protocols. 4) The methodology of data collection, data analysis, and research instrumentations. 5) Building the testing scenarios

using a quantitative research method computing simulations. 6) Evaluating the performance of the proposed solution employing standard metrics like throughput. 7) Comparing the performance of standard solutions, discussing the hypotheses, answering the questions, and achieving the research objectives.

B. Book Chapter Publication | Impact Factor: 0.131 | Status: Published | Role: Corresponding Author.

Juma, M., and Shaalan, K. (2020). *Cyber-Physical Systems in Smart City: Challenges and Future Trends for Strategic Research*. Swarm Intelligence for Resource Management on the Internet of Things, pp.65-85. Elsevier Inc.

Link: <https://www.sciencedirect.com/science/article/pii/B9780128182871000085>

Contribution to this thesis: 1) Conducting a comprehensive survey on the state-of-the-art using the systematic review approach. 2) Identify the literature's recent challenges, opportunities, and future trends. 3) Critiquing the previous works, findings, and observations for other researchers in the same field. 4) Focusing on the limitations and recommendations to find new research gaps and pursue innovative research solutions.

C. Book Chapter Publication | Impact Factor: 0.236 | Status: Published | Role: Corresponding Author.

Juma, M., and Shaalan, K. (2021). *Online Social Network Analysis for Cybersecurity Awareness*. In Recent Advances in Intelligent Systems and Smart Applications, pp.585-614. Springer, Cham.

Link: [https://link.springer.com/chapter/10.1007/978-3-030-47411-9\\_32](https://link.springer.com/chapter/10.1007/978-3-030-47411-9_32)

Contribution to this thesis: 1) Defining problem statement, research objectives, questions, and hypotheses. 2) The methodology of data collection, data visualization, and research instrumentations. 3) Analyzing the data of the structural topology and influence of the hub nodes in the complex cyber networks. 4) Testing the research hypotheses and evaluating the

outcomes with defined metrics. 5) Interpreting the significant findings and discussing the results to answer the questions and achieve the research objectives.

## **1.8 Thesis Outlines**

The organization of the thesis includes six main chapters covers the overall research efforts done by the author for more than three years to deal with the target research topic is the following:

Chapter 1 presents the introduction of the thesis that consists of eight sections. The first section of the research context highlights the cyberattacks' impacts and incentives against critical information infrastructures over the past two decades. The second section of the research rationale and motivation introduces the research viewpoints for the relationship between dynamic cyber resilience and cyber risk management with a summary of their concepts, in addition to justifications to shifting paradigms towards dynamic cyber resilience.

The third section presents the literature observations identifying the significant research gaps and maturing the thesis's problem statement. The fourth section develops the research purpose and goal along with research objectives in detail as well as formulates the extended research questions with their associated hypotheses. The fifth section displays the scope of this research, besides demonstrating the research assumptions and specifying the main points that prove the thesis's significance and originality.

The sixth section reveals the thesis contributions to the research topic's theoretical knowledge and practical domain. The seventh section demonstrates the author's papers recently published and currently submitted and under review in the same subject matter. Finally, the last section in this chapter depicts the overall thesis outlines.

Specifically, Chapter 2 presents the literature review of the thesis that consists of three sections.

The first section of critical information infrastructures has three subsections that introduce a broad background of coupling behavior across interdependent networks, outlining ICS-based and ICT-based critical information infrastructures' properties and characteristics. The section also focuses on modeling cyber vulnerability analysis for the scale-free topology of CIIs, besides covering the impacts of their failures under concurrent and consecutive cyberattacks and reviewing the quantitative cyber threats models and scenarios.

The second section of dynamic cyber resilience states the related studies. It works within three subsections: core principles with a maturity matrix of cyber resilience for interdependent CII networks and the current dynamic cyber resilience solutions with technical and functionality comparison detail. The capability-based quantification to evaluate the capabilities of these solutions and their performance implications. Finally, the third section represents the general findings of the literature review that meet the research gaps.

The overall objective of Chapter 3 is to provide deep insights for describing the conceptual framework of the proposed solution in the first section that deals with the aspects before, during, and after adverse cyber events in the context of dynamic cyber resilience. The second section organizes the overall phases of the architecture design, technical development, algorithms and protocols, optimization, and deployment of the proposed solution. It displays the improvements to optimize the proposed solution through cyber zero-trust algorithms and protocols.

Accordingly, Chapter 4 provides a suite of sections to overview the design and methodology developed by this research. More precisely, the first section illustrates the research design's milestones starting with a research roadmap then measuring the standard networking metrics to evaluate the cyber resilience factors such as throughput, response time, and average delay. The scenarios operationalization includes the illustrations of the scale-free topology for the coupling



network formed by interdependent connections of critical information infrastructures' core and edge networks. The scenarios generation of the concurrent and consecutive cyberattacks explores the escalating and cascading effects.

The second section's description of research methodology consists of three subsections. They focus on the quantitative data collection procedures to obtain high-quality data for the model and five data analysis levels of research results across two measurement rounds, primary and optimized ones. In this regard, the further procedure shows how the research validity and reliability are applied to both data collected and analyzed.

Furthermore, the results and discussion adopted to conduct this research work described in Chapter 5 provides via five sections the optimized analysis of the proposed solution, evaluation metrics, comparison measurements, testing outputs, and results in discussion with a particular emphasis on performing an optimized analysis comparing a proposed solution to standard solutions of dynamic cyber resilience. Likewise, the optimized results were collected and analyzed in the second section by similar quantitative research methods in the previous section.

Both sections have three subsections that use the same cyberattack scenarios and networking metrics to analyze the proposed solution results compared with standard solutions' results. The fourth section in this chapter elaborates on the optimized results. It discusses in the fifth section the close gaps' findings with complete interpretations to judge the associated hypotheses and answer the research questions to achieve the thesis purpose.

Finally, Chapter 6 summarizes the developed methodology, results from the implementation methods, further limitations, and potential extensions of this research in the future. Subsequently, a brief overview of related conclusions is demonstrated in the first section and its subsections towards meeting research hypotheses, answering questions, accomplishing the research purpose,

and reporting the research outcomes and implications. Moreover, the second section of research recommendations clarifies the thesis's limitation and their alternatives on top of presented guidelines to inspire possible areas of the suggested future works.

Appendix A summarizes the cyber risk management components and a quick survey of the works for policy and technology to handle the cyberattacks. Appendix B defines terminologies studying linguistically and technically a particular set of essential research terms and expressions used in the thesis. Appendix C shows an overview of secondary data collected and analyzed based on the systematic literature review approach, demonstrating the scientific materials' classification by specific domains upon the number of citations, sector contributions, and publication year.

Appendix D indicates the methodological research choice, philosophy, approach, strategy, time horizon, technical instrumentation, and procedures with all fine points of the quantitative research methods used in the thesis, including analytical modeling, emulated experiments, and computing simulations.

Appendix E shows the details of the primary phase prototyping development for a proposed solution that identifies the essential requirements to fulfill dynamic cyber resilience capabilities.

Appendix F analyzes the primary phase results in this research incorporating the results collected by OPNET computing simulations, GNS3 emulated experiments, and MAXIMA analytical modeling. It elaborates on the discussion of the primary results.

## CHAPTER 2. LITERATURE REVIEW

The literature review motivated this research for illuminating how knowledge has evolved within the under-researched issues, highlighting what already has done, what is generally accepted, and emerged, surveying the area of contributions, building upon the crucial observations, and departing from the current state-of-the-art and state-of-the-practice (Assenza et al., 2019).

In this chapter, the theoretical studies and empirical works are deeply discussed to contrast, judge, and make arguments in an attempt to meet up the research purpose. The most substantial body of selected literature is divided into twofold parts: critical information infrastructures and dynamic cyber resilience (Begishev et al., 2019).

The first part provides a definitive appraisal and interpretative analysis. It reveals contradictions concerning coupling behavior across cyber interdependency, vulnerability analysis of cyber scale-free topology, and cascading failure under concurrent and consecutive cyberattacks for critical information infrastructures (Hausken, 2020).

Likewise, the second part focuses on the discredited publication sources directly relevant to fundamental principles, exciting solutions, and capability-based evaluation of dynamic cyber resilience. Finally, the following sections present an overview of screening outputs of research items and the definition of terminologies used in the thesis (Erokhin, 2019). *See Appendix B: Definition of Key Terminologies and Appendix C: Secondary Data Overview.*

### 2.1 Critical Information Infrastructures

In the 21<sup>st</sup> century, the growing demand for quality services, tensions of profitability, globalization, transboundary dependencies, unforeseen dynamics, and the rapid institutional and technological transforms have changed the landscape of traditional critical infrastructures that

mainly operated with legacy architectures in centralized, isolated, and homogeneous environments (Reich, 2019).

Therefore, the need increasing nowadays for interconnections intricately among such infrastructures to maintain the well-being of life and fulfill the objectives, especially in modern society, is becoming more dependent on the desirable outcomes that are contingent on the availability of large-scale services provided profoundly by interdependent critical information infrastructures (Tsochev et al., 2019).

When cyber interdependency relationships exist among these heterogeneous infrastructures, new dynamic relationships are created and formed coupling networking. Moreover, since CIIs are interdependently planned, accidental exposure can affect the whole CII network via the connecting nodes (Sukach et al., 2020).

The constant contact with other infrastructures ensures a constant level of exposure from the interconnected infrastructures and makes the essential operations and critical functions potential for cascading failures under concurrent and Consecutive cyberattacks (Shevchuk, 2019).

This section espouses the current dialog interplay commonly associated with CIIs research concepts to expound virtually expected effects of coupling behavior across them and illustrates the importance of understanding relationships among coupled networks of interdependent CIIs (Vasilyev et al., 2019).

Furthermore, it presents the advancing vulnerability analysis of scale-free topology because working on the assumption that the goal of the relationship among infrastructures is not one-to-one; instead, it is multidirectional that takes on new distinctive meanings beyond their conventional formulations (Sokolov et al., 2019).

The whole critical information infrastructures become vulnerable and can affect other facets of

the coupling network if one interdependent critical information infrastructure is open to and capable of being damaged since it does not operate in isolation (Potii & Tsyplinsky, 2020).

Additionally, it demonstrates the tremendous consequences of cutting off the line of vital services delivery in discovering possible ways to improve the dynamic cyber resilience and reduce the negative influences on CIIs outputs (Petukhov et al., 2019).

### **2.1.1 Coupling Behavior across Interdependent CIIs**

At the current digital age, critical information infrastructures have come to be all-embracing and seen as a fundamental part to make critical infrastructure more interrelated simultaneously with numerous domains for underpinning a broad range of modern services that people, societies, and countries depend on around the globe (Hadjsaid et al., 2010).

In general, critical information infrastructures include two heterogeneous subtypes: ICS-based infrastructure and ICT-based infrastructure (Fotouhi et al., 2017). The first type is the critical legacy infrastructure managed by the Industrial Control Systems (ICS) like Supervisory Control and Data Acquisition (SCADA) system, commonly controlled the operations of the industrial production in oil and gas facilities, electrical power plants, water pipelines, and dams ... etc. (Ostfeld et al., 2014) as illustrated below in Figure 2.4.

ICS-based infrastructures are cyber-physical infrastructures; that is, the cyber part consists of controls and communications; interact as a cohesive and unified whole with the physical part, consisting of sensors and actuators (Mattioli & Moulinos, 2015). The combination of both parts includes the collecting of the information via Remote Terminal Unit (RTU), Programmable Logic Controllers (PLC), and Intelligent Electronic Devices (IED), transferring it back to the leading site, carrying out any necessary control and analysis, then displaying that information on many operating views (Dan-Suteu & Gânsac, 2020).

Three of the most critical ICS-based infrastructure architecture zones are Master Station, Remote Terminal (RTU, PLC, IED), and the communication between them using two standard communication protocols like DNP3 and T101 (Schneider et al., 2013). Today, such infrastructures align with the standard networking technologies; TCP/IP protocols also replace their old proprietary standards for coupling other critical information infrastructures (Nazir et al., 2017).

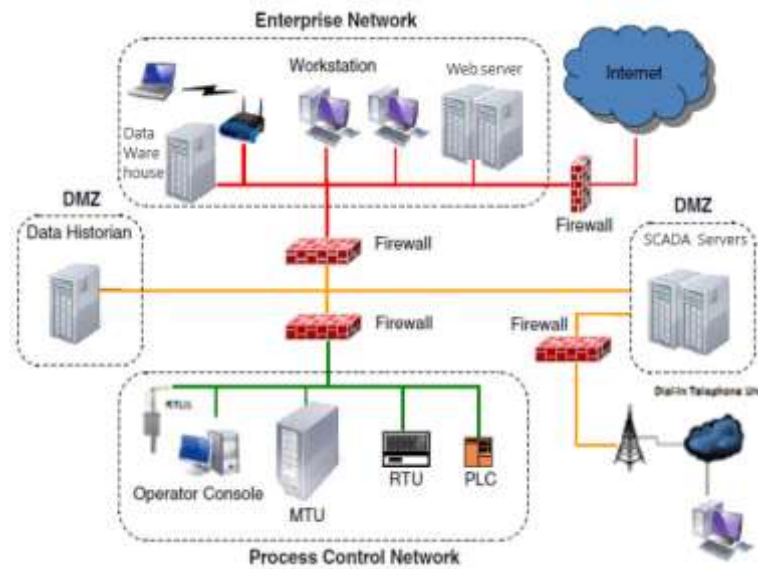


Figure 2.4: Typical Architecture of SCADA as an Example of ICS-based Infrastructure (Nazir et al., 2017 modified)

With the integration of IP-based Ethernet protocols into ICS-based infrastructures, particularly in the enterprise network zone, the ability to remotely control, monitor, troubleshoot network devices and offer web services has increased (Tsochev et al., 2019). In contrast, this increase in cyber visibility and availability has led to more exposure of ICS-based infrastructures to cyberattacks over internet connections with fewer constraints on reliability, latency, and uptime, precluding some dynamic cyber requirements resilience (Haque et al., 2019).

The second type of critical information infrastructure is the ICT-based infrastructure managed by Information and Communication Technologies (ICT) (Maglaras et al., 2018). It has become

more important to shape modern society today and contribute immensely to social and economic improvements (Theron & Bologna, 2013).

The necessary ICT-based infrastructure components encompass a combination of all information, devices, networks, protocols, procedures, and employed people. To foster complex operations and exchange of harmonized information required amongst different stakeholders, enable cross-border continuity of a wide range of digital services, and support public and private sectors (Anne et al., 2018), as illustrated in Figure 2.5.

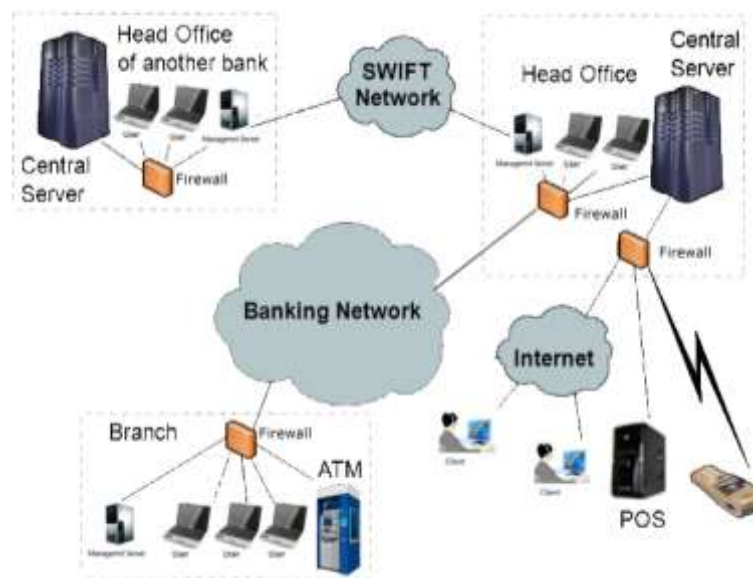


Figure 2.5: Typical Architecture of SWIFT as an Example of ICT-based Infrastructure (Theron & Bologna, 2013 modified)

The ICT-based infrastructures are providing necessary conditions to accomplish the enormous values of many systems in the world, such as the Health Information Technology (HIT) system, nationally handled the patient records, nursing resources, care protocols, medication administration, and case documentation (Greenhalgh et al., 2019). Likewise, the Society for Worldwide Interbank Financial Telecommunication (SWIFT) system universally supervised the global banking and financial messaging services (Njemaze et al., 2019).

Table 2.1: Differences between ICS-based Infrastructure and ICT-based Infrastructure  
(Maglaras et al., 2018, Dan-Suteu & Gânsac, 2020 modified)

<i>Aspect</i>	<i>ICS-based Infrastructure</i>	<i>ICT-based Infrastructure</i>
<i>Environments</i>	Industrial Production.	Socioeconomic Services.
<i>Sectors</i>	Energy, Nuclear, Manufacturing, Chemical, Defense, Emergency, Food, Water, Transportation.	Commercial, IT, Communications, Financial, Education, Government, Healthcare.
<i>Hardware</i>	Main Servers, Workstations, Programmable Logic Controllers (PLC), Sensors, Actuators ... etc.	Data Centers, Central Servers, PCs, Peripheral Devices, Hubs, Switches Routers, firewalls ...etc.
<i>Operating Systems</i>	Windows.	Commonly Unix, Linux, and Windows.
<i>Software</i>	Generally, the SCADA system and Distributed Control Systems (DCS).	Financial and administration systems, Business Intelligent, Special systems, MS Office ... etc.
<i>Protocols</i>	Regularly DNP3, IEC 61850, IEC 60870-5-101, IEC 60870-5-104.	Mainly TCP/IP, HTTP, PPP, VoIP, DHCP, POP3, SMTP, IMAP, FTP.
<i>Procedures</i>	Specific Procedure.	Well-Known Procedure.
<i>P/E Ratios</i>	No. of Person $\ll$ No. of Equipment.	No. of Person $\approx$ No. of Equipment.
<i>Lifetime</i>	Fifteen to Thirty Years.	Three to Five Years.
<i>Availability</i>	No less than 99.9%.	It is Possible Between 95% & 99%.
<i>Downtime</i>	The accepted range is between 5.25 minutes to 8.76 hours per year.	The accepted range is between 3.65 to 18.25 days per year.
<i>Protection</i>	Focus on Function.	Focus on Data.
<i>Security Priorities</i>	1) Availability, 2) Integrity, and 3) Confidentiality, respectively.	1) Confidentiality, 2) Integrity, and 3) Availability, respectively.
<i>Threat Vectors</i>	Function Interruption and/or Interception.	Data Modification and/or Fabrication.
<i>Threat Impacts</i>	Disruption of Service, Loss of Production and Safety, and \$ Cost.	Disruption of Service, Loss of Information, and \$ Cost.
<i>Main Vendors</i>	Universally Siemens, ABB, GE, Emerson, Honeywell ... etc.	Universally IBM, Microsoft, Sun, Cisco, SAP, Oracle ... etc.

The ICS-based infrastructure and ICT-based infrastructure as a cyber-based infrastructure play a crucial role in ensuring smooth and reliable operations within the critical infrastructure. Nevertheless, there are many differences between both of them technically and practically in various aspects (Hadsaid et al., 2010), (Theron & Bologna, 2013), (Mattioli & Moulinos, 2015), (Anne et al., 2018), (Mbanaso et al., 2019), (Haque et al., 2019), and (Dan-Suteu & Gânsac,



2020) as shown in Table 2.1.

The critical information infrastructures have predominantly popular network properties and characteristics (Beyza et al., 2019) shown in the dotted boxes in Figure 2.6. Most CIIs are characterized by dynamic behavior, interdependent reliance, combined architecture, and heterogeneous configuration (Cao et al., 2017). Moreover, CII network properties mainly involve radial centrality, load-balance clustering, complex layering, and topologies with the giant vital component (Fraccascia et al., 2018).

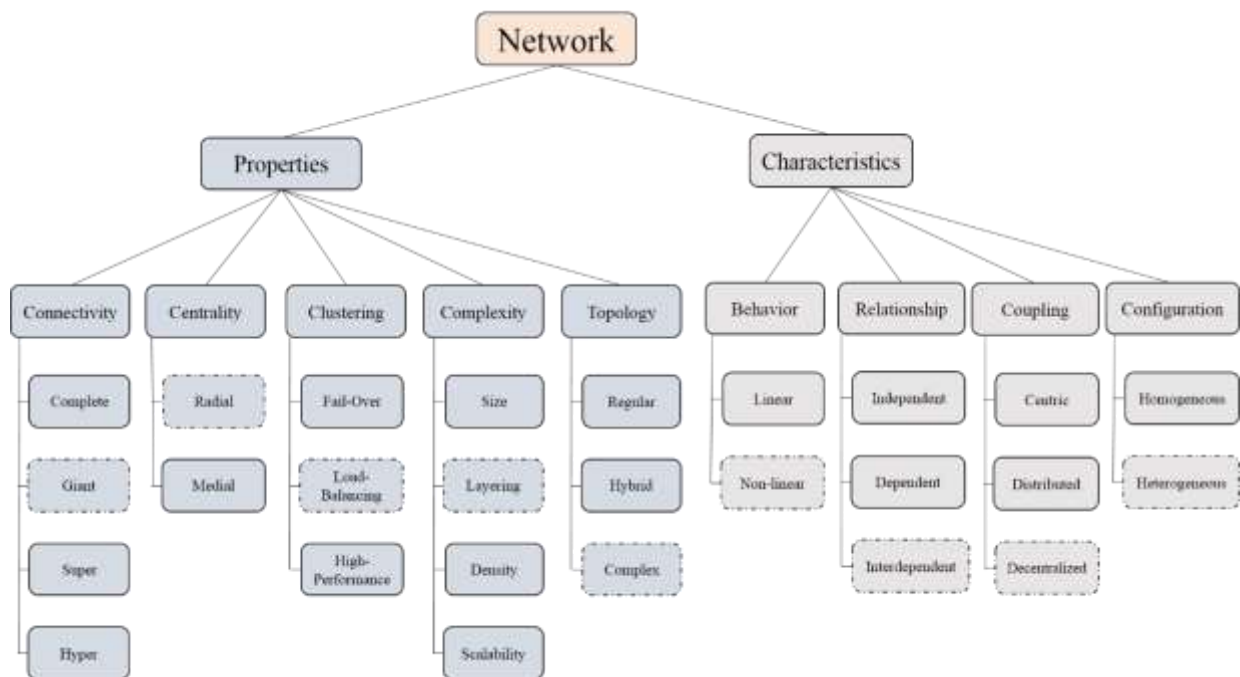


Figure 2.6: Outline the Properties and Characteristics of CII Networks

As illustrated in Figure 2.6, the significant network properties of CIIs describe the inner, collective, non-changeable features of the network that involve centrality at the single node level, clustering at a group of nodes level, complexity at the network level or network of networks level, and end with connectivity, and topology at all levels in the network. (Gao et al., 2016).

Firstly, the property of centrality recognizes the essential nodes within a network. It has split into

two categories, radial and medial. Radial centrality counts hops that start and end from a specific node, while medial centrality counts hop passing through an individual node (Li et al., 2018). Secondly, clustering organizes similar nodes in a particular partition. It is classified into three classes: failover, load balancing, and high-performance (Setola & Theocharidou, 2016).

Thirdly, the property of network complexity identifies by size, density, layering, and scalability. The network size is the number of nodes, and the network density is the ratio between the number of existent links and the number of possible links in the whole network (Torres et al., 2013). Besides, the multilayer networking interacts within the single or multiple networks increase the network complexity as well as the ability of a network to scale over time (Liu et al., 2015).

Furthermore, CII are divided virtually into six interrelated layers as follows: facilities layer, physical layer, logical layer, information layer, a functional layer, and organizational layer, each layer consist of a set of integrated components and operations that interact with the inputs and the outputs of other layers (Jiang et al., 2018).

Three of the CII layers are considered cyber layers; the first is a logical layer, which runs operations like routing, switching, and security (Herrington & Aldrich, 2013). The second is an information layer containing data warehouses and distributions and data storage and analytics. Ultimately, the third layer is the functional layer, which presents the services, platforms, and controls for CII (Ghanbari et al., 2018).

These cyber layers played many roles in the CII environment. For example, they could map with the layers of The Open Systems Interconnection (OSI) reference model, which was established by The International Organization for Standardization (ISO) to describe the implementations, processes, and protocols for functions and data over the CII networks (Masood et al., 2016).

Conceptually, the CII functional layer is associated with the OSI application layer. Likewise, the

CII information layer relates to OSI presentation and session layers, CII logical layer links with OSI transport and network layers (Kamissoko et al., 2019), as illustrated in Figure 2.7.

Fourthly, connectivity describes the connecting process of different network parts. It consists of four types, complete connectivity, where each couple of nodes are connected by a link (Bashan et al., 2011). The giant vital component is a fraction of nodes connected in one significant network component (Cetinkaya et al., 2017). When cutting any node, the super-connected network will isolate another node, while the hyper-connected network will create just two components when cutting any node, one of them isolated (Milanović et al., 2018).

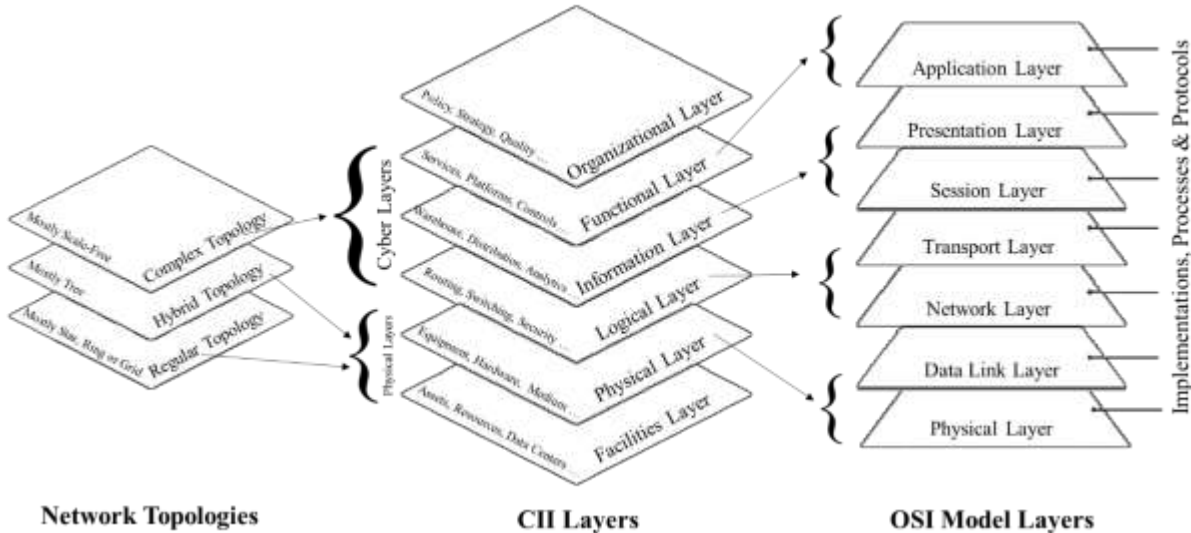













Figure 2.7: Mapping CII Layers with OSI Model Layers and Network Topologies

Lastly, the topology property designates the nodes' geometrical arrangements and links them physically or logically in the network (Buldirev et al., 2012). Both terms of graph and network have interchangeable use (Cetinkaya et al., 2017). The graph components consist of vertices and edges, same as network components made up of a set of nodes connected by links. The graph is a mathematical representation, while the network is related to the real system (Herrmann et al.,

2011).

As a part of graph theory, the Network theory has many applications in various disciplines to study the relations among discrete objects (Beyza et al., 2019). Consequently, Alderson (2008) defined the term of the network as *"a set of connected items. These items are known as nodes or vertices, and the connections between them as links or edges"*. In 2015, The Canadian National Research Council stated the definition of network science as *"a study of network representations of physical, biological, and social phenomena leading to predictive models of these phenomena."* The network topology is classified into three main categories: regular, hybrid, and complex (Milanović et al., 2018).

Table 2.2: Examples of Different Topologies for Networks (Beyza et al., 2019 modified)

<i>Network Type</i>	<i>Network Topology</i>				
<i>Regular</i>					
	Star	Bus	Mesh	Ring	Grid
<i>Hybrid</i>					
	Snowflake	Tree	Hybrid Mesh		
<i>Complex</i>					
	Random	Small-World	Scale-Free		

Regular networks are recognized basic structures like bus, star, ring, in addition to lattice networks as a mesh and grid. In hybrid networks, more than two regular networks are combined to produce new structures such as a tree (star-bus), snowflake (extended star), and hybrid mesh (Sterbenz et al., 2013). The complex networks have a large number of nodes and links with the randomness of connectivity and complexity of structuring, for example, scale-free, small world, and random networks (Fan et al., 2014), as illustrated in Table 2.2.

Although there was no consensus definition of complex networks when reviewing the significantly related literature, however, Alderson (2005) lightly defined the complex network as *"a network system with a large number of components with complicated relationships among them and has many degrees of freedom in the possible actions of these components"* (Lade & Peterson, 2019).

The conception of networking evolution added to the definition by Boccaletti et al. (2006) to become *"networks whose structure is irregular, complex and dynamically evolving in time"* (Louzada et al., 2013). Manoj et al. (2018) described it as a *"network presenting properties and characteristics observed in real-world networks, with a topology that evolves over time"* (Senovsky et al., 2019).

On the other hand, the network characteristics of CIIs describe outer, individual, changeable attributes of the network, comprise architecture, behavior, reliance, and configuration (Setola et al., 2017). Initially, the heterogeneous configuration related to the diverse components' arrangement processes connected smoothly with the different setups in the same environment, conversely, the homogenous network (Chowdhury et al., 2020). From the cyber view, the profound heterogeneity between ICS-based and ICT-based infrastructures lies in networking and communication protocols (Li et al., 2018).

The ICS-based networks operated by protocols compatible with differential equations in continuous systems, while ICT-based networks used protocols working with events in discrete systems (Sirika & Mahajan, 2016). Nevertheless, both types of infrastructures apply the same standard protocols for connecting with each other, providing web services, and surfacing the internet (Manzoor et al., 2020).

In the second place, the network's reliance deals with network interactions. The network

infrequently appears in independent status (Almoghathawi et al., 2019). However, the relationship scenarios in a dependent network focus on the node in one network supported directly by the node in another network (Holden et al., 2013). In contrast, the nodes linked across different interdependent networks affect bidirectionally. In particular, there are five dimensions, four classes, three categories, and two approaches for studying the interdependency of critical information infrastructures (Barker et al., 2017).

Thus, CIIs are in constant interdependencies with their environment, using and transforming inputs to provide outputs to the same environment (Sarwat et al., 2018). These interdependencies can be characterized into five dimensions: (1) Economic concerns shaping production scheduling and business agreements (Shah & Babiceanu, 2015). (2) Political views, regulations, and policies affect infrastructure growth or bind the operating environment (Stanley et al., 2016). (3) Technical requirements control modes of operation (Goldbeck et al., 2019). (4) Safety regulations affect the operation of associated infrastructures (Blokus & Dziula, 2019). (5) Social factors stimulate infrastructure operators' operational decisions (Barker et al., 2017).

The four classes of interdependencies include (1) Physical class: an infrastructure is physically interdependent if the state of its operations is dependent on the material outputs of another infrastructure and vice versa through a functional and structural linkage between the inputs and outputs of two infrastructures (Huang et al., 2011). (2) Cyber class: an infrastructure has a cyber-interdependency if its operation state depends on information and data transmitted in both directions through the information infrastructure via electronic or informational links. Outputs of some information infrastructures are inputs to the other infrastructures, and the material passed among the infrastructure assets is information (Tundis et al., 2017).

As well, (3) Geographic class: infrastructure assets are geographically interdependent if a local

environmental event can create changes in the state of operations in all of them (Yang et al., 2015). (4) Logical class: an infrastructure is logically interdependent if its state of operations depends bidirectional on the state of another infrastructure via a mechanism that is not a physical, cyber, or geographic connection. Logical interdependency is attributable to human decisions and actions and is not the result of physical or cyber processes (Mo et al., 2017).

In addition to the four classes of interdependencies, the connections among critical information infrastructures are multidimensional, adding to their complexity as the following: (1) Upstream interdependencies: dealing with the inputs of the products or services provided to one infrastructure by another external infrastructure that is necessary to support its operations and functions and vice versa (Nan et al., 2014). (2) Internal interdependencies: dealing with the interactions among the infrastructure's internal operations, functions, and missions. Internal interdependencies are the internal links among the assets constituting a critical information infrastructure (Wang & Ouyang, 2015). (3) Downstream interdependencies: dealing with the outputs or consequences on stakeholders of critical information infrastructures from the degradation of the resources provided by them (Rahnamay-Naeini & Hayat, 2016).

In general, however, two approaches can be taken when studying the interdependencies between infrastructure networks: (1) Top-down approach: the various networks are modeled generally in the same infrastructure designing with each network topology. The data model is inherent to the network. The complete critical data sharing between multiple networks of infrastructure is essential. It is a significant obstacle because most of this information is sensitive, like locations of infrastructures and types of technologies (Yin et al., 2018). The definition of the relationship rules between the different networks is very complicated. The interdependencies are parameterized and formalized within the infrastructure networks. The discovery process has

occurred in the conceptualization of these networks. This approach implies a higher level of abstraction in the modeling process (Bloomfield et al., 2017).

Also, (2) Bottom-up approach: the internal topology of each infrastructure network is studied at the finest available precisely. As a result, a very detailed model can be achieved within each network. It requires less data sharing between non-parameterized interdependencies; they can be discovered using the networks (Zio & Fang, 2017).

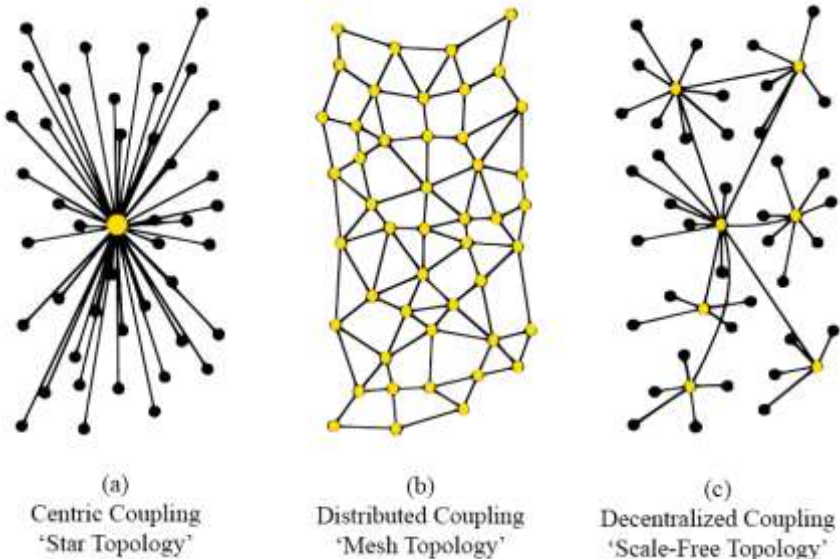


Figure 2.8: Comparison between Centric-Distributed-Coupled Architectural Couplings (Golnari & Zhang, 2015 modified)

The consequences of these interdependencies are obtained but not fully formalized. Therefore, a standard data-sharing model needs to be developed for information flow between networks. The failure is simulated within these networks, and then the results of that simulation are extended to other networks in the infrastructure to study cascading effects. It gives added flexibility to this approach (Seppänen et al., 2018).

The third characteristic of the network is Architectural Coupling, which is a complete structural design of established networking to provide an overall view of accessible resources in detail



whether the coupling is (a) centric, (b) distributed, or (c) decentralized, is considered a combination of the first two types (Bodeau & Graubart, 2013) as shown in Figure 2.8.

It is mandatory in centric coupling with star topology to access or pass information through the centralized node or giant vital component, but in distributed networking with mesh topology, one has to use a directly node-to-node connection rather than using a centric node (Cetinkaya et al., 2017).

Usually, the architectural couplings of the physical level of critical information infrastructures are centric or distributed, but at the cyber level, their architectural coupling is decentralized (Shoemaker et al., 2018). Centric coupling is easy to maintain, as there is only a single point of failure (Sterbenz et al., 2013). The decentralized coupling has moderate maintenance but still a finite number of failures. Distributed coupling is the most difficult to maintain with infinite points of failure (Buldyrev et al., 2012).

Furthermore, the centric coupling is low scalability with high instability; there will be chaos in the network when removing the central node (Brennan et al., 2019). In contrast, the distributed coupling is very stable with infinite scalability, and a single failure is not harmful. Despite the low to moderate scalability of decentralized coupling, recovery is possible through other hub nodes when removing the hub node (AlHamdani, 2020).

Moreover, the centric coupling is less complicated, created fast, and follows a single framework that applies everywhere in the network but has no diversity and evolves slowly. On the other hand, for distributed and decentralized architectural couplings, creating the moderate with lower-level details like resource sharing and communications, evolution is tremendous once the primary network is in place (Yamin et al., 2020).

Focusing on the interdependencies of coupled heterogeneous networks of critical information

infrastructures and their behaviors, the first classification of the interdependent relationships between CII is tight or loose, depending on the relative degree of coupling (Acheson & Dagli, 2016). The degree of coupling tightness or looseness influence the cyber resilience of CII when stressed under cyberattacks. To better understand the level of interdependencies and represent their relative impact, use a dependency matrix among CII (AlMajali et al., 2012).

Tight coupling represents CII highly dependent on one another such that any disturbance tends to propagate rapidly through and across them. Time-dependent CII with little or no slack usually characterize tight couplings (Cao et al., 2017). Additionally, tight coupling refers to disturbances in one infrastructure correlated closely to those in another tightly coupled infrastructure. Disturbances propagate rapidly through and across tightly coupled infrastructures (Golnari & Zhang, 2015). On the other hand, loose coupling represents CII relatively independent of each other with weak or no correlation between their statuses. In terms of time-dependency, short-term disturbances rarely affect other interdependent CII (Tian et al., 2015).

The second classification of the interdependent relationships among CII can be evaluated using the coupling order that indicates whether two CII are directly or indirectly connected with the latter achieved through one or more intermediate CII (Fotouhi et al., 2017).

The multiple connections of the feedback and feed-forward paths create a sophisticated scale-free topology capable of modeling disruptions, flows, and long-term impacts depending on other properties and characteristics of CII networks. As a result, they were incorporating these feedback loops into scale-free topology can represent how, where, and when disturbances propagate, leading to interdependent CII failures (Danziger et al., 2016).

Finally, network behavior characteristics are twofold, linear and nonlinear. The linear behavior causes the CII network to be intensely reliant on the required communication patterns with a lack

of flexibility. In addition, the nodes are resistant to crashing, and links sustain the operational level regularly (Broeders & Berg, 2020). Linear interactions are designed with few unfamiliar or unintended feedback loops like assembly lines carried out in sequences. Small changes in linear interactions can also result in a sudden and erratic impact; therefore, the linear behavior models cannot address such effects (De Florio, 2015).

Arbitrary communication patterns in geometric dimensionality usually support nonlinear behavior. Nonlinear interactions are those interactions with unfamiliar sequences, whether by design or inadvertently (Banescu et al., 2015), not visible or immediately comprehensible, and they can be subtle and difficult to detect. Such interactions can occur with branching paths, feedback loops, and jumps from one linear sequence to another (Kleij & Leukfeldt, 2019).

The nodes might depart or arrive within the network, and links might fail and recover based on the Cost, throughput, and routing paths. So naturally, the networks of CII and their interdependencies are predominantly nonlinear (Burla et al., 2016).

The failures of CII interdependencies are categorized as cascading, escalating, or common cause. (1) Cascading failures occur when a disruption in one CII subsequently disrupts another node or link in another CII. This type of failure is called the domino effect. The cascading failure effect can be linear or nonlinear (Başar & Zhu, 2012). (2) Escalating failures occur when disruption of one CII exacerbates an independent disruption on the second CII and intensified in the form of increased severity or recovery or restoration time for the second CII. This type of failure is called the snowball effect. The escalating failure effect can be linear or nonlinear (Pescaroli & Alexander, 2016). (3) Common failures occur when disruption of two or more CII networks are influenced simultaneously, typically due to physical or cyber interdependencies.

The typical failure of effect can be nonlinear (Brummitt et al., 2012).

Both coupling and behavior characteristics capture how critical information infrastructures handle a disruption like cyberattacks to one or more of their interdependencies (Tyra, 2012). Complex interdependent relationships are characterized by multiple connections between heterogeneous infrastructures (Wu et al., 2018). The connections create detailed feedback and feed-forward paths, branching topologies that transmit failures across different critical information infrastructures (Ventresca & Aleman, 2015).

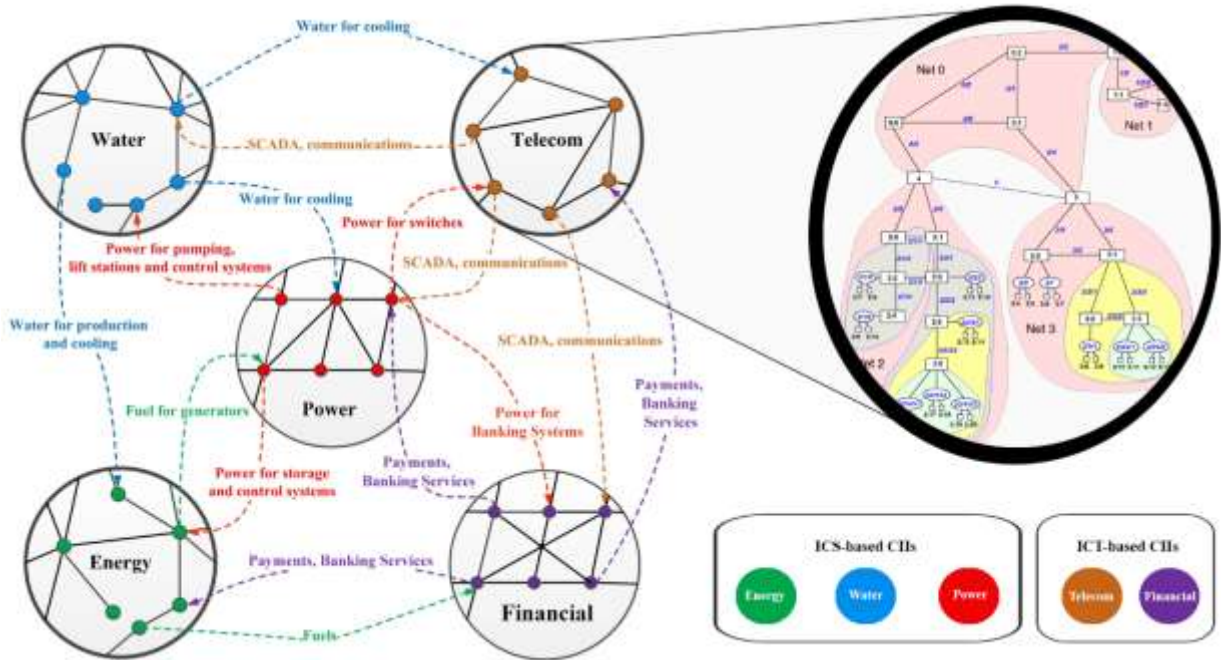


Figure 2.9: Cyber Interdependencies among Heterogeneous CII (Canzani, 2016 modified)

An example of the failure impacts on the cyber interdependencies among ICS-based and ICT-based infrastructures would be simulated a substation breaking down in a particular area caused by cyberattacks that interrupt the power service provided by energy infrastructure for 6 hours (Fang & Sansavini, 2018), as shown in Figure 2.9.

The information is passed onto a water infrastructure that estimates the areas where no water will be delivered to telecom infrastructure, calculates the effects on the landline and cell phone networks (Canzani, 2016). Then, this information passed onto the breakdowns in banking systems in financial infrastructure has local-wide consequences; likewise, the traffic lights will disrupt the transportation infrastructure that affects millions of people (Canzani, 2017).

In such cases, the disruptions of cyber interdependencies are contained within given critical information infrastructures; based on that, more or less well-defined functions or services are affected (Thorisson et al., 2020).

### **2.1.2 Cyber Vulnerability Analysis of CII's Scale-Free Topology**

The vulnerability research frames the offensive and defensive motivations over the past two decades through three primary areas: vulnerability discovery, exploit development and exploit mitigation (Nistor et al., 2019). The goal of an aggressive cyber attacker covers the first and second vulnerability areas that were increasing the capabilities continuously on the target CII. Conversely, the cyber defender's goal covers the first and third vulnerability areas that mitigate the exploit development techniques cyber attackers will use, not necessarily rooting out vulnerabilities and fixing them (Reniers & Zhang, 2018).

It is commonly understood that impractical to attempt to find and fix all of the vulnerabilities exhaustively. Thus, exploit mitigations act as a defensive force-multiplier significantly raises the bar for exploiting all vulnerabilities within interdependent CII's (Seppänen et al., 2018).

As the first component of cyber risk management, cyber vulnerability has a central role in supporting decision-making for ensuring adequate dynamic cyber resilience of CII's. The concept of cyber risk is mature, whereas that of cyber vulnerability is still evolving (Beyza et al., 2019).

Risk analysis as a formalized subject has existed for almost four decades and has reached a wide

range of applications to reveal and identify potential failure modes in systems and operations so that they may be correct before they manifest (Danziger et al., 2016).

For CIIs, the term cyber risk may include the frequency of loss of service with its resulting consequences, while cyber vulnerability seen as a global CII degree embeds three sub-degrees: the degree of losses due to the impact of cyber threats; the degree of exposure to cyber threats, and degree of cyber resilience (Kumar et al., 2020).

The critical information infrastructures generally are legacy, costly, carry out complex interactions in real-time, and have a long operational lifetime, whether ICS-based or ICT-based, leading to three types of vulnerabilities at disparate extents: design, operation, and administration (Hong et al., 2012).

Indeed, the priorities of CII administration are conflicting between sustained performance operation and maintained integral cyber protection. Operationally, the internal bugs usually existed in the standard operating systems used to run the industrial control systems or the information and communication systems such as SCADA and SWIFT. Some of them still operate with low-level networking protocols that manipulate communication messages with simple plain text and lack encryption, designed to work in isolated environments (Ferreira, 2019).

The topology design of CII networks is scattered geographically with multiple access spots, seeing as backdoors that are not safeguarded well against failure. The topology vulnerabilities describe network connectivity's possible loss because of random incidents like natural hazards or intentional disruptions such as cyberattacks (Oliva et al., 2019). Therefore, the deep understanding of CII complex networks' cyber layers, particularly the scale-free topology, serves as a backbone for the components of these heterogeneous layers and their dynamics at the level of all related cyber protocols (Xu & Masys, 2016).

The complexity of CII topology caused by the network multiplexing means the networks of CII cyber layers handle a massive quantity of logical connections through minimal physical links (Cao et al., 2017). In contrast, the network topologies of CII physical layers are simpler, where generally could be hybrid or regular such as the star, ring, grid, or tree topologies (Gamboa et al., 2020).

Thus, the numerous studies in CII research, including those related to cyber resilience, focus on the topologies of complex networks and their expected failures when exposed to disturbances resulting from the interactions with other interdependent CII networks (Karabacak et al., 2016).

Besides that, the growing research area of complex networks differs in three main aspects from traditional networking research: concentrating on real-world networks with non-trivial topologies, understanding evolutionary networks over time, and looking for network behavior dynamics (Pescaroli & Alexander, 2016).

These aspects are enabling deep insights into the vulnerability of CII network topologies that expansively studied by Holme et al. (2002), Dekker and Colbert (2004), Tanizawa et al. (2005), Dall et al. (2006), Estrada (2006), Paul et al. (2006), Grubestic et al. (2008), Herrmann et al. (2011), Schneider et al. (2011).

Recently, scholars in the field of complex networks have made some works on localized cyber failures. For example, Shao et al. (2015) studied network percolation under localized failures, modeled by removing a randomly selected node, nearest neighbors, next-nearest neighbors and reaching some failure intensity. They are strictly called topological failures (Reniers & Zhang, 2018).

Berezin et al. (2015) also modeled failures in a diluted square lattice by removing all nodes within a certain Euclidean distance from a random location, which is only a simple form of

spatial failure. Moreover, these purely topology-based studies usually produce vulnerability results with weak correlations to those results obtained when Ouyang (2013) and Cavalieri et al. (2014) consider the infrastructure flow properties. To this end, it is crucial to understand and analyze the cyber vulnerabilities of the topology of critical information infrastructures specially provided by the scale-free networks (Gatchin & Sukhostat, 2019).

The term scale-free refers to the lack of an intrinsic scale regarding the expected degree of a randomly chosen node in the network, resulting from the extensive range in node degrees seen in scale-free networks (Hansen, 2019). The interest in scale-free networks began in the late 1990s with the reporting of discoveries of power-law degree distributions in real-world networks such as the World Wide Web (WWW), the network of Autonomous Systems (AS), some networks of Internet routers, protein interaction networks, email networks, etc. (Gao et al., 2016).

Most of these reported power laws fail when challenged with rigorous statistical testing, but the more general idea of heavy-tailed degree distributions, many of these networks genuinely exhibit, is very different from what one would expect if links existed independently (Tian et al., 2015). Barabási et al. (1999 - 2003) introduced the concept of scale-free networks. Barabási-Albert's (BA) preferential attachment model is commonly used for generating scale-free networks (Barabási, 2016).

A  $k$ -linked scale-free graph grows by incrementally adding nodes and connecting each new node by  $k$  links to existing nodes where  $k$  must be at least two to guarantee connectivity (Cao et al., 2017). A network is named scale-free if its degree distribution, i.e., the probability that a node selected uniformly at random has a certain number of links, follows a particular mathematical function of the power-law that implies the degree distribution of these networks without a characteristic scale (Holden et al., 2013).



In a network with a scale-free degree distribution, some nodes have a degree of orders of magnitude larger than the average; these highly connected nodes act as network hubs, efficiently providing connectivity within the network (Hayel15). However, such hub nodes are vulnerable to targeted cyberattacks to fracture the network quickly because these critical nodes have the highest degree and have thus been implicated in the spread of failure in cyber networks like interdependent critical information infrastructures (Goebel et al., 2018).

For this reason, scale-free networks are described as the hub-spoke networks that exhibit a non-random pattern of node degree with hub nodes exhibiting very high connectivity while most connected spoke nodes have relatively low numbers of links (Tipper, 2014).

Hub nodes also interact internally between network clusters, providing target and quick inspection opportunities. Thus, hubs are not the most obvious targets only, but they also are complex enough to contain the kinds of redundant critical information infrastructure networks that may make for a quick recovery (Johnston et al., 2014).

The hub nodes become highly focused points of interconnection and more critical to protecting critical information infrastructures; the loss of a hub node located at the center of the scale-free network may result in the complete failure of the connection (Hayel & Zhu, 2015). Such concepts have applied to the vulnerability of internet backbones as well as interdependent critical information infrastructures (Zhu & Chen, 2020).

The hub-spoke network design has served well for several forms of cyber connections, but it is evident, now that cyber resilience issues heightened, that the exposure of large fractions of interactions to passage through a few hub nodes or along a single path requires assessment in terms of cyber threat and probability of failure (González et al., 2016).

Any cyber risk situation combines the probability of failure and frequency of occurrence and the

likely cyber consequences of that failure. Cyber risk and cyber consequences are also highly likely to be interdependent, especially for cyber threats, as it is very probable that cyberattacks would prioritize the highest valued targets (Goebel et al., 2018).

However, links are also critical to the interconnection of two network clusters. An issue that has also been relatively under-examined in the context of hubs is that the resulting sparse and efficient network provides an obvious shortest path but pays no attention to the availability of backup routes (ICS-based CII hub and spoke network's added vulnerability is a lack of redundant alternatives. It is also effortless to use the assignment variables to know links will be busy and interactions flow. Thus, it could make targeted disruption of essential connections relatively easy (Yin et al., 2018).

Most methodological analysis and modeling approaches are used to assess cyber interdependency's criticality and evaluate scale-free topology within the CII hub-spoke networks (Faramondi et al., 2020). For example, a cyberattack at a spoke node chosen at random would most likely do minor damage because of its low degree, but a deliberately concerted effort to disable one of the very high degree hub nodes could be devastating (Panzieri et al., 2019).

The primary modeling paradigms found in the literature provides insights on the maturity level of each quantitative approach that include network analysis, system dynamics, and agent-based modeling as the follows: (1) Network analysis is a research method that lays the foundations in many different disciplines and mathematical models (Zhu & Chen, 2020). The development of advanced network analysis led to the new science of networks in almost every scientific domain (Ottenburger et al., 2020). An intuitive way to cope with CII's interdependency is to use network theory concepts. Single CII's can be seen as networks, where nodes are different components of the CII (Nistor et al., 2019).

Similarly, networks in each node representing CII describe interdependencies between CII (Holden et al., 2013). In general, modeling criteria for interdependent networks of CII account for infrastructure topologies (topology-based methods) or services delivered by CII (flow-based methods) (Goldbeck et al., 2019).

In the case of disruptive events, the CII's performance is evaluated by using different metrics such as the number of failed nodes, path length, connectivity loss, redundancy ratio, and network clustering when considering topological features and node heterogeneity (Pedroni et al., 2015). Time-dependent characteristics of the nodes, such as duration of CII unavailability and lost service hour, are modeled to analyze system-level functionality. However, topology-based methods fail in providing information about the flow performance of CII (Scala et al., 2016).

The so-called network flow models capture flows of commodities between CII. For instance, Oh et al. (2010) propose a disaster impact analysis based on two measurement factors: level of service and inter-relationship level. The first assesses the damage of the disrupted infrastructure; the latter identifies how industries depend on adjacent infrastructure for sustaining their activities (Divakaran et al., 2017). However, network flow models do not consider dynamics within a single node in the CII (Chowdhury et al., 2020).

Studies based on network flow principles often consider a limited number of CII due to the complexity of modeling each infrastructure's detailed operation mechanisms (Wu et al., 2018). An example is the connectivity model Svendsen and Wolthusen (2007) proposed to capture the production and consumption of power grid, telecommunication, and gas infrastructures.

However, several assumptions made in the previous studies limit the network analysis method used towards the cyber-resilient CII. One limitation is the use of network structural properties to assess resilience. The performance of CII is interconnected intuitively to their structure or

topology (Francis & Bekera, 2014). Nevertheless, focusing on structural properties does not fully capture the concept of cyber resilience, as defined for this work. Cyber resilience focuses on the ability of CII to maintain desired capabilities following disruptions (Graubart & Bodeau, 2016). While CII structure and connectivity likely contribute to these capabilities, many other factors may determine the provided capabilities. Ignoring these possible factors and assuming that connectivity directly translates to capability can be misleading when designing CII. Concentrating on structural properties also assumes a static view of resilience (Manzoor et al., 2020).

The cyber resilience of CII is determined by the capabilities maintained in the presence of cyberattacks and the capabilities recovered following the disturbance, with consideration of the time elapsed during this entire process (Graubart & Bodeau, 2017). Using network structural properties to evaluate cyber resilience does not fully consider this aspect since there is no time consideration when determining a removed node's effect on network structure (Masood et al., 2016). These studies also do not consider CII adaptation and reconfiguration. The ability of resilient CII to adapt to potential cyberattacks is a defining characteristic that distinguishes them from robust CII. Accurately, these studies are more described as network robustness (Mitchell & Chen, 2016).

(2) System dynamics is a top-down approach to explore interdependent complex adaptive systems such as CII. System dynamics models built stock-and-flow diagrams that capture the aggregated system behavior through a set of differential equations underlying the model (Kiss et al., 2015). It allows decision-makers to analyze what-if scenarios, causes of disruptions, design effects, and evaluate recovery using continuous-time simulations (Balchanos, 2012).

This methodology is used to study systems' complex behavior because flows and accumulation

of flows change over time by interacting variables within nonlinear feedback loops (Canzani, 2017). Vugrin and Camphouse (2011) focus on cyber resilience assessment of critical information infrastructures through control design. However, data access problems and the inability to analyze network topology changes and component-level dynamics are significant limitations of the system dynamics approach (Klein & Klein, 2019).

However, the related studies maintain many of the same issues limiting other CII's cyber resilience studies for designing cyber resilient networked CII's. These studies focus on the structural properties and do not consider the adaptation (Schwind et al., 2016).

(3) Agent-based modeling is a bottom-up decentralized and interaction-oriented modeling approach. It is used widely to analyze the complexity of CII's that assumes complex dynamics arise from single interactions among CII components (Thompson et al., 2019). It means that infection dynamics result from various events determined by single agents' behavior. The agent-based approach enables the analysis of scenarios with all interdependency types among CII's via discrete-event simulations (Dibaji & Ishii, 2015).

However, this approach is more dedicated to robustness since the CII's can still adapt once cyberattacks occur. Furthermore, the robustness measure also does not consider the time aspect of cyber resilience, i.e., how quickly CII's lose capabilities and how long they recover following cyberattacks (Dong et al., 2013).

Ventresca and Aleman (2015) propose a more vigorous defense against cyberattacks by allowing CII's to add new links following each cyber-attack. Their method more closely considers cyber resilience by incorporating adaptation, but their analysis still focuses on the topology structure of the CII's following each cyber-attack (Johnson et al., 2018).

This approach does not account for the actual CII's capabilities to evaluate node removal's

robustness. Robustness is a capability-based measure, but this measure is used only to study CII bottleneck as the operational environment changes (LaRocca, 2014).

### **2.1.3 CII Failure under Concurrent and Consecutive Cyberattacks**

For lifeline networks like smart grids, banking transactions, transportation systems, emergency services, and information and communications technology need to be at almost full functionality during disruptive times (Sano et al., 2016).

A focus on global cyber threats as the second component of cyber risk management led to changes in viewpoints on the importance of CII network protection for a functioning society (Wang, 2019). In particular, external cyberattacks consider the most popular and dangerous vectors of cyber threats. Furthermore, the definition of cyberattacks has been evolving over the years due to changing cyber threat perceptions (Zhao et al., 2017).

Some extreme impacts of cyberattacks' significance have altered the thought process incorporated into the CII networks in recent years. Moreover, monitoring and safeguarding against cyberattacks arising from different sources (Castillo et al., 2019). As such, there has been an increased understanding that it is not possible to protect every possible CII network against every cyberattack and eliminate all cyber vulnerabilities (Hayel & Zhu, 2015).

The cyber risk management against cyber-attack-based correlated multiple and catastrophic failures is a topic that has not been paid much attention in the literature so far despite always being a top priority (Johnson, 2015). Therefore, this research targeted researchers and practitioners from both academia and industry interested in cyber resilience issues to new and future CII networks' architectures.

On the basis of the literature review, there are more than 30 cyber threat models. However, most of them are sub-models or customized forms of a few main cyber threat models that are split into

two dimensions: Attack-Defend Dimension (ADD) and Static-Dynamic Dimension (SSD) (Conti et al., 2018). Further, Attack-Defend Dimension (ADD) is divided into attack modeling that focuses on cyber attacker's actions and vulnerabilities of systems; and defense modeling that concentrates on cyber defensive aspects, such as detection, reaction, responses, and prevention (Tabansky, 2011).

The Static-Dynamic Dimension (SSD) is divided into dynamic formalisms that take temporal aspects, such as dynamics, time variations, and cyber interdependencies between considered actions like order or priority, into account. Simultaneously, static approaches cannot model such cyber relations (Rusi & Lehto, 2017), as shown in Figure 2.10.

Both Attack Tree and T-MAP models fall in the first Quadrant I with cross-over Attack-Dynamic dimensions. The Attack Tree model comprises conceptual diagrams with a tree-like structure (Viswanathan et al., 2017). The tree structure represents the different ways that the CII's attacked. The tree leaves represent the underlying attack tasks that need to compromise the specific cyber threat higher up in the tree (Petukhov et al., 2019).

Such a model is only helpful when the CII's are pretty well-known. Furthermore, the model assumes that if all cyberattacks on the CII's are understood, they could likely design the appropriate countermeasure (Shevchenko et al., 2018). Therefore, the model does not provide guidelines for identifying the CII's architecture. Besides, it does not provide guidelines for assessing sub-goals and tasks (Strom et al., 2017).

Finally, it relies on cyber estimation for assessing the actual cyber threat of one, particularly sub-goal, and heavily on analysts who know the cyberattacks quantifying or the damage it may cost (Thorisson et al., 2020). Thus, it knows how difficult it might be for the cyber attacker or the likelihood of apprehension for the cyber attacker (Xiong & Lagerström, 2019).

However, the Attack Tree model does not require knowing the aspects of the CII; the cyberattack’s specifics suffice. Another usefulness of the Attack Tree lies in providing a tool for modeling the overall cybersecurity for decision-making (McCollum et al., 2018). When all information is known about cyberattacks, the model is an excellent map for understanding the cyber threats and their assumptions (Shevchenko et al., 2018).

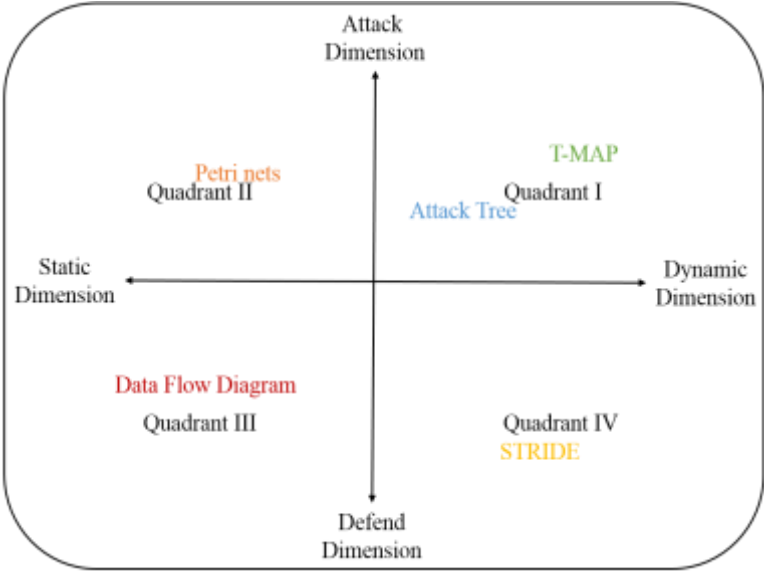


Figure 2.10: Quadrants of Key Quantitative Cyber Threat Models

A common outcome is that many cyber threats and countermeasures are vastly overestimated effectiveness. A famous example is that of the commonly proposed encryption countermeasures. By thinking in attack trees, countermeasures are compared, communicated effectively, and made logical decisions (Creese et al., 2011).

Moreover, Threat Modeling Attack Paths (T-MAP) analysis is a novel quantitative cyber threat model that assesses cyber threats by calculating the total severity weights of relevant cyberattack paths (Conti et al., 2018). T-MAP describes a comprehensive cyber threat quantification, several underlying formulas, and weighing techniques used to quantify the overall cyber threat level of



cyberattack paths described (Viswanathan et al., 2017).

Attack paths are conceptual representations of the CII's architecture in four layers. These are the firewall, the Commercial off the Shelf (COTS) tools, the critical information infrastructure, and the organization's core values (Sterbenz et al., 2013). The four layers together are described in terms of 22 attributes. The Common Vulnerability Scoring System (CVSS) developed by Cisco, Microsoft, and other large industry giants inspired these attributes (Fang & Sansavini, 2018).

The T-MAP weighting system used severity ratings for each of the above attributes and summing up all the calculated cyber-attack paths, the overall threat known (Tonhauser & Ristvej, 2019). Then, evaluate any new countermeasures with the cyber-attack paths it might eliminate for more efficiency within the T-MAP framework and implement within the organization (Sansavini & Fang, 2016).

In the second Quadrant II, intersect Attack-Static dimensions, Petri-Nets for cyber threat modeling is suggested alternative to the Attack Tree model (Harrison et al., 2011). It allows representing the CII's network in terms of critical components such as places or states, transitions nets or actions, mapping functions or directed arcs between cyber interdependencies, simulated as the flow of tokens through the CII networks (Sterbenz et al., 2012).

Many tokens move around the Petri-Nets from place to place via the arcs, and the distribution of tokens among the places represents the dynamic state of the entire modeled CII networks through various types of asynchronous and concurrent processes cyberattacks that need representation from different sources at the same time (Moraitis et al., 2020). Additionally, the model is designed to reconcile the knowledge from different resources into one cyber threat model by working with generic places and transitions, and suitable for a distributed CII networks setting, where concurrent actions need to be undertaken to execute successful cyberattacks (Xiong &

Lagerström, 2019).

However, the Petri-Nets model assumes such actions or transitions without breaking or altering the CIIs' components. It is most appropriate as a retrospective model to evaluate how cyberattacks could have occurred from a high level (Johnson et al., 2018). Furthermore, the model assumes that no central ownership of the components in the cyberattack points of the CIIs, i.e., the specific places and transitions do not have to be within one CII network (Shevchenko et al., 2018).

Furthermore, Data Flow Diagram (DFD) for cyber threat modeling in the third Quadrant III cross Defend-Static dimensions. It is a graphical representation to display four generic data flow elements through CIIs (Nistor et al., 2018). DFD consists of the external entity, the data flow, the data store, and the complex processes modeled in the analysis, while the trust boundaries drawn to show related data flows move from one CII to another CII (Scala et al., 2016).

However, DFD is used for applications where cyber threats are mainly in the CII networks and operate using the IP protocol by providing an overview of all components and processes that can be a cyber-threat and focus primarily within their trust boundaries (Singh et al., 2016). Finally, limited information about the element itself is shown, such as the data type or details about the processes (Wu et al., 2018).

Likewise, Activity Diagram (AD) as an alternative for Data Flow Diagram (DFD) is a UML 3.0 workflow model of CIIs used in existing cyber threat modeling (Conti et al., 2018). To compare the evaluation of the AD effectiveness against DFD for threat modeling, Johnstone (2010) has used a standard case to show AD cyber threat modeling is more expressive because the guard condition for the activity element, while DFD has no analog for this element (Tabansky, 2011). It is the same for similar activities, while DFD provides no explicit notation within the UML

framework (Viswanathan et al., 2017).

However, AD has fewer expressive elements for data stores of databases, possibly further hampering the cyber threat modeling process (Björck et al., 2015). The extra elements in AD could model a more complex situation and make the diagram unnecessarily complicated (Haque et al., 2018). Finally, as with DFD, the AD seems to have similar steps, such as defining boundaries, differentiating between different CIIs, and addressing components and their functions and dependencies. It does not assume all cyberattacks but instead assumes a complete overview of the target CII (Moyer et al., 2016).

Finally, the intersection of Defend-Dynamic dimensions in the fourth Quadrant IV shows the STRIDE cyber threat model. It stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of privilege. The model used for identifying these common types of associated cyber threats to the CIIs was once described (Behal & Kumar, 2016).

Each cyber threat type of the STRIDE mnemonic is standing what sets for it exactly. Spoofing is seen as the act of misrepresenting itself as the receiving party or the sending party in a communication line (Georgiev et al., 2017). Tampering focuses on modifying data in data stores. Repudiation is when the authentication cannot be verified, assured, or accounted for. Information disclosure describes a data breach (Wright et al., 2016). Denial of service focus on overloading a communication line and making it unavailable. Last, the Elevation of Privilege happens when privilege levels are changed or removed (Mosharraf et al., 2015).

The six types of cyber threats in the STRIDE model provide starting points for developing cyberattack scenarios depending on several factors such as the scale of the war-gaming details, the scope of cyber risk assessment, defensive cyber technologies, business functions posture, and

the CII's evaluated environment (Bhuyan et al., 2015).

For example, when the cyber attacker remotely controls the SCADA distribution management system, the disconnection of several substations for hours and the failure cascade across more areas (Dan-Suteu & Gânsac, 2020). Once failure begins, the CII network's failure may directly affect physical devices' status due to the coupling effect, thus aggravating the cascading (Wang, 2019).

Table 2.3: Classifications of the Cyberattack Scenarios  
(Kochedykov et al., 2020, Hayel & Zhu, 2015 modified)

<i>Scenario</i>	<i>Vector</i>	<i>Scale</i>	<i>Target</i>	<i>Effect</i>	<i>Objective</i>	<i>Scope</i>	<i>Reliance</i>	<i>Failure</i>	<i>Example</i>
<i>Adverse</i>	Concurrent	Small & Large	Function & Data	Interruption/ Interception/ Degradation/ Modification/ Fabrication/ Exfiltration	Availability, Confidentiality & Integrity	Infrastructures & Services	Dependent & Interdependent	Common	DDoS
<i>Historical</i>	Consecutive	Large	Function	Interruption/ Interception/ Degradation	Availability & Confidentiality	Infrastructures	Dependent	Escalating	Zero-day
<i>Postulated</i>	Regular	Very Small & Small	Data	Modification/ Fabrication/ Exfiltration	Confidentiality & Integrity	Services	Interdependent	Cascading	MITM

Table 2.3 shows the classifications of three types of cyberattack scenarios with related cyber-attack vectors, scale, and examples. Besides, the cyber effect within C.I.A. triad and cyber reliance on the scope with the failure influence on the target (Tsochev et al., 2019) as the following:

(1) Adverse cyber scenarios can range in scale from small to large scale of concurrent cyberattacks that target two or more interdependent critical infrastructures or services simultaneously (Bhuyan et al., 2015). The concurrent cyberattack as a popular vector in this type of scenario common causes in CII's affects the related cybersecurity objectives of availability, confidentiality, and integrity (Yong et al., 2016).

The Distributed Denial of Service (DDoS) cyberattack is a good example that can be generalized

in terms specific to the target CIIs environment in a real-world event (Wang, 2019). OSI Layer-3 DDoS cyberattacks on the CIIs networks rely on too high volumetric data, including ICMP, SYN-ACK, and UDP floods, to slow down the performance and consume large amounts of bandwidth, make excessive connection requests without responding to confirm the connection, and eventually degrade access for legitimate services. In addition, it typically affects the availability of information resources and differs in success relative to the CIIs environment (Georgiev et al., 2017).

(2) Historical cyber scenarios focus on the large scale of consecutive cyberattacks with escalating effects across the dependent infrastructures' functions to serve as the starting point for a failure tree analysis (Heinbockel et al., 2013). Scenarios focus on availability and confidentiality through interruption, interception, or degradation of the given functions. In addition, they widely explored zero-day cyberattacks in deployed technologies on specific critical infrastructures (Zhao et al., 2017).

A zero-day cyberattack exploits potentially severe vulnerabilities of the interdependent CII networks' critical functions. A zero-day attack gets its name from the number of days the cyber defender has detected the targeted vulnerability and rushed to resolve to limit cyberattacks' failure effects (Tran et al., 2016).

A zero-day cyberattack involves spyware, malware, and worms using known vulnerability backdoors to exploit unauthorized access to sensitive data and interrupt services (Cazorla et al., 2016). Such cyberattacks' propagation models exhibit widely differing cyber behaviors digital signatures that define them and are likely to circumvent conventional detection mechanisms easily (Zheng & Albert, 2019).

For example, based on the Random Constant Spread (RCS) model of the zero-day cyberattack of

the Code Red worm, a two-factor model was developed to capture the effect of countermeasures against worm spreading and the impact of an active worm on internet traffic and critical information infrastructures (AlMajali et al., 2012). In addition, existing research on the propagation of zero-day cyberattacks and their models provides the foundation for additional research in this area (Han et al., 2016).

(3) Postulated cyber scenarios could be very small or small in scale. These scenarios aim for data confidentiality and integrity in the interdependent services on shared infrastructures (Wicks et al., 2018). The exploitation of Man-in-the-Middle cyberattack in widely deployed technologies in such scenarios or on specific essential services causes cascading effects across the CIIs (Yamin et al., 2020).

Man-In-The-Middle (MITM) cyberattack is a form of active eavesdropping in which a cyber-attacker can target two coupled nodes in the interdependent CIIs, believing that they are communicating directly with each other when in fact, the connection is controlled by the cyber attacker (Castillo et al., 2019).

Therefore, it is used merely to access the transmitted data or modify the messages before retransmitting those. Compromised links of CII networks are a perfect place for executing MITM cyberattacks. Especially hub nodes are excellent targets for cyber attackers since most network traffic in the CIIs, pass through these links (Mauthe et al., 2016). When a cyber-attacker can control such a link, it is quite simple to perform some malicious operation to capture or modify it. Even if some secured protocol is used, there are still valuable ways to get into the link session (Cetinkaya et al., 2017).

The differences in the cyberattacks landscape of these three types of cyber attacking scenarios can be categorized into five levels based on the adversary seriousness degree (Brtis et al., 2013),

as shown in Table 2.4. In the details, the advanced cyberattacks have the highest seriousness with fifth-degree. This is because these cyberattacks are very sophisticated, well-resourced, and generate opportunities to support concurrent, consecutive, and successful cyberattacks (Bodeau & Graubart, 2013).

Table 2.4: Cyberattack Levels based on Seriousness Degree  
(Bodeau & Graubart, 2016, Strom et al., 2017 modified)

<i>Seriousness Degree</i>	<i>Adverse Level</i>	<i>Cyberattack Capability</i>	<i>Cyberattack Intent</i>	<i>Adverse Target</i>
5	Advanced	very sophisticated	All aspects of the CII mission	Functions & Data
4	Significant	sophisticated	Some aspects of the CII mission	Functions & Data
3	Moderate	moderate	Shared resources of CII	Functions
2	Limited	limited	Critical functions of CII	Functions
1	Unsophisticated	very limited	Critical data in CII	Data

In this level, the cyber attacker analyzes information obtained via the reconnaissance stage to target a specific CII persistently with great determination to impede severely and destroy all aspects of the high-value mission by exploiting a presence in the interdependent CII (Strom et al., 2017).

Less than that degree, the significant cyberattacks have a sophisticated level of expertise, with significant resources and opportunities to support multiple successful coordinated cyberattacks (Heinbockel et al., 2013). The cyber attacker focuses on some critical aspects of mission-critical information while maintaining his accessibility to the CII in the future. The adversary is very concerned about minimizing their cyber tradecraft disclosure, particularly while preparing for future cyberattacks (Laderman et al., 2015).

The third degree of seriousness is the moderate cyberattacks, which have appropriate resources, expertise, and opportunities to support multiple successful cyberattacks (Bodeau et al., 2016). It seeks to obtain or modify critical information to disrupt the shared cyber resources by

establishing a foothold in the CII, particularly when carrying out cyberattacks over long periods. The cyber attackers at this level are analyzing publicly available information and willing to impede the critical positions of CII knowingly to achieve these ends (Mitra et al., 2010).

Moreover, the adversary has limited resources and expertise in the second adverse level by using publicly available information to target a class of high-value information and actively seeking targets of opportunity within that class to usurp critical functions and does so without concern about the detection of them cyberattacks (O'Halloran et al., 2017).

Lastly, the lowest seriousness of the cyberattacks is unsophisticated ones with minimal expertise and opportunities to support successful cyberattacks that may or may not target any critical data in specific CII and deface the information without concern revelation them (Sano et al., 2016).

Based on the above cyberattacks' adverse level, the consequence effects of the common cause, escalating, and cascading failures indicate that the disruption in one node of CII causes the subsequent disruption in the connected node of another CII (Abdelgawad et al., 2019).

A cyber failure in one node can initiate cascading effects within interdependent CII or, in the worst case, cause cyber failures in other interdependent CIIs, possibly disrupting vital services. Such cascades of failures could disrupt both function and data flows (Kiss et al., 2015).

So far, a great diversity of methodologies has proposed modeling the three types of cyber failures. However, no existing approach can capture all mechanisms during cyber failures (Lyn, 2015). Moreover, each model has its concentration and advantages, while only limited research has been proposed to study the interdependent models due to the complex mechanisms and difficulties invalidation in reality (Pipyros, 2019).

The coming brief presents the critical review of interdependent models for cyber failure analysis based on their different characteristics; these models can classify into threefold: complex



network-based interdependent model, interdependent Markov chain model, and flocking-based hierarchical cyber-physical model (Bloomfield et al., 2017). Furthermore, each model may have characteristics involved in other models, while its main contribution and features only classify it (Guo, 2010).

(1) Complex network-based interdependent model: interdependent CII are common in many real-world networks and have been widely studied using complex network theory (Beyza et al., 2019). For example, Buldyrev et al. (2012) introduced interdependent models, analyzing the robustness of interacting networks subject to cyber failures. The model used real-world data from CII networks and an internet network implicated in cyber failure (Torres et al., 2013). An analytical solution has illustrated that removing the critical nodes would lead to cyber failure and the complete fragmentation of two interdependent CII networks (Li et al., 2018).

Shah and Babiceanu (2015) have improved the model based on multiple random support-dependent relations and analyzed CII networks' robustness. The results proved consistent with those simulated on other single networks (Tran, 2015). However, this model's disadvantage is that it fails to consider enough cyber property while focusing only on purely topological parameters (Wu et al., 2018).

Schneider et al. (2013) have proposed another model that showed how to mitigate cascading failure in a coupled network by selecting a minimum number of autonomous nodes. Later on, he has presented a new coupling model that consisted of three subnetworks (Ventresca & Aleman, 2015). A sensitivity analysis was performed to evaluate the mitigating method in the model. The model has simulated a load control, focusing on load factor and interdependence degree (Milanović et al., 2018).

More recently, a more comprehensive model has proposed a mesh network that considers cyber

network characteristics (Louzada et al., 2013). Moreover, bidirectional links are modeled, including data uploading and command-downloading channels. These links were supposed to connect all cyber network nodes and a corresponding physical node (Ghanbari et al., 2018). The fragility of the coupling model has been studied under various cyberattacks, like DDoS. Load shedding and relay protection have been involved in the model (Vespignani, 2010).

(2) Interdependent Markov Chain (IDMC) model: it provided a probabilistic framework of cyber failure analysis to capture the effects of interdependencies among physical networks and cyber networks (Rahnamay-Naeini & Hayat, 2016). The IDMC model enabled a cyber-level prediction of the interdependent coupled networks with trackable details of the CII. Furthermore, it assumed that the coupled network was more vulnerable when a failure occurred, thus increasing failure probability in the CII (Sarwat et al., 2018).

On the other hand, when physical network components fail, they may also trigger cyber networks with a given probability (Blokus & Dziula, 2019). The IDMC model demonstrated that interdependencies between two coupled networks could significantly affect each other on failure distribution sizes (Balchanos, 2012). The simulation illustrated that coupled networks with exponentially distributed failure sizes tend to be less robust, as evidenced by the scale-free power-law distributed failure sizes for both coupled networks in the CII (Hadjsaid et al., 2010).

(3) Flocking-based hierarchical cyber-physical model: a multi-agent cyber network model based on the flocking theory presented (Kalala, 2017). The model considered dynamic nodes and local cyber-controller (Etigowni et al., 2016). The related parameters were involved in the cyber networks were regarded as physical parts, and local cyber-controller served as cyber elements (Eldosouky, 2019). The model concentrated on control strategies for coupling networks' cyber resilience (Hui et al., 2014).

## **2.2 Dynamic Cyber Resilience**

The assumption is that advanced cyberattacks, particularly against critical information infrastructures, cannot be stopped easily because the ongoing stresses of a persistent cyberattack will succeed in the end (Shalamanov, 2019). For that reason, CIIs must ensure that their essential functions have cyber continuity capabilities despite these adverse conditions (Teodorescu & Pickl, 2016).

While the cybersecurity concept focuses on keeping adversaries out, it is designed to ensure that the confidentiality, integrity, and availability of CIIs are achieved at acceptable levels (Siddiqui et al., 2019). Therefore, dynamic cyber resilience quickly emerges as a critical component in any effective cyber protection strategy (Choudhury et al., 2015). Since it assumes that good cybersecurity capabilities are already in place and then build cyber continuity capabilities to withstand and rapidly recover from deliberate cyberattacks occurring to critical cyber resources of CIIs (Vugrin et al., 2014).

Additionally, there have been some studies on cyberattacks in coupled networks; long-lasting cyber networks may be resilient to inevitable cyberattacks, but as time passes after the CII networks fielded, changes in the operating environment may make the networks less resilient to both old and new types of cyber threats (Wang et al., 2017). Most of these works have taken a static view of cyber threats. A common assumption among previous studies is that the cyberattacks are independent and consecutive attacks will not happen simultaneously (Cai et al., 2018).

### 2.2.1 Core Principles of Dynamic Cyber Resilience

The evolution towards cyber resilience thinking is far from trivial; cyber resilience as a concept is more dynamic, it is non-linear and cross-linked, complex, so to say, and it embraces uncertainty (Chmutina et al., 2016). Current thinking on cyber resilience is the product of theoretical and practical constructs that have been refining and reshaping the paradigm of cyber risk management over the past three decades (Rehak et al., 2018).

Several researchers present ten top-level principles or sub-principles extracted from many literature sources that constitute the core of cyber resilience for enabling critical information infrastructures (Lin & Bie, 2016) to (1) Anticipate and possibly avoid cyber-attacks (Carlson et al., 2012). (2) Survive an encounter with cyberattacks (McGill, 2011), or (3) Recover from an encounter with cyberattacks (Linkov et al., 2013).

These core principles are necessary to develop concrete solutions and suffice for dynamic cyber resilience purposes and can be divided into two categories, scientifically accepted principles and the other based on experience, commonly called heuristics (Marchese et al., 2020). Although all principles in both categories may apply to interdependent CII, certain ones will stand out as being more critical, primarily those described in terms of technological aspects (Raab et al., 2015).

The summary of the first set of the five scientifically principles are as follows: (1) Coupling: states those failures in loosely networked CIIs should not be allowed to propagate from node to node, as Perrow (1999) says, *“loosely coupled systems, whether for good or ill, can incorporate shocks and failures and pressures for change without destabilization”* (Laishram et al., 2018). (2) Absorption: states that the CII should be capable of withstanding cyberattacks within its design limit (Karakoc et al., 2019). The sub-principle of limit degradation states that absorption capability should not be allowed degrading because of aging or low maintenance. Woods (2006),

who adds margin, describes it as a separate principle.

Also, (3) Redundancy states that the CII should consist of at least two or more identical parts physically or have two or more different segments functionally (Yin et al., 2018). (4) Reorganization: states that the CII should be capable of restructuring itself in the face of cyberattacks (Shalamanov, 2019). (5) Repairing: states that critical information infrastructure should be capable of being repaired (Dupont, 2019). This principle reflects a capability, is standard in most CII networks (Helfgott, 2018).

On the other side, the summary of the second set of the five heuristic principles are as follows:

(6) Complexity: states that the number of components and interfaces in a CII should be reduced to a minimal level (Setola et al., 2017). (7) Localizing: states that the functionality of the CII should reside in the distributed hub nodes of the coupled networks (Ouyang, 2017). Sometimes uses the term modular capability, as Perrow (2011) called. (8) Layering: states that the CII should not have a single point of failure (Mitra et al., 2010). This principle depicts cyberattacks passing through multiple layers of defense; each layer represents a different defense layer. The lesson is that more layers increase the cyber resilience of the CII (Dunn Caveltly et al., 2015).

Also, (9) Interacting: states that every inter-node of a CII should be capable of communicating, cooperating, and collaborating with other nodes (Häring et al., 2016). This principle was particularly crucial in the CII and other interdependent principles because it is a significant factor in several case studies to reduce the hidden interactions (Das et al., 2020). In other words, every action made by inter-node should assure that there are no unexpected interactions among other nodes of a CII that may be detrimental to the functionality of the whole CII (Choras et al., 2015). Moreover, Perrow (1999) discusses hidden interaction extensively and attributes many system failures to this principle.

(10) Correcting: states those corrective measures should be taken when the CII is drifting towards the boundary of its cybersecurity limit (Brown et al., 2010). Drift correction in CII networks can be divided into two categories: real-time drift correction and latent drift correction (Liu et al., 2016). Real-time drift correction occurs when cyberattacks are approaching a CII (Almoghathawi et al., 2019). Latent drift correction pertains to flaws that have lain undetected until a catastrophe occurs (González et al., 2016). Drift correction in a technological context occurs when risk increases; however, it is just as valid in CII networks (Vugrin et al., 2014).

It is crucial to consider the inherent interdependencies among most coupled CII, offer different services to the modern communities (Bodeau & Graubart, 2016). Such dependency on cyber resilience between these communities and CII has been widely recognized in the scientific literature and is depicted in the cyber resilience maturity matrix of interdependent CII networks (Laderman et al., 2015).

In this respect, Gilligan (2016) presented the mapping of the relationships as a matrix for cyber resilience maturity for interdependent critical information infrastructures in explored five levels vertically across four capabilities of cyber resilience horizontally that divided into cybersecurity and cyber continuity categories as well as described by MITRE (2015).

The matrix demonstrated cyber resilience types and levels that need to incorporate CII interdependencies to be cyber resilient, considering the cyber failures through coupled CII networks (Strom et al., 2017), as shown in Table 2.5.

At level one, the cyber resilience maturity is essential and characterized by the inconsistent deployment of basic cybersecurity controls that led CII to be susceptible to very limited cyberattacks without any capability to mitigate, recover, or normalize to cyber failures (Shoemaker et al., 2017). In addition, Gilligan (2016) speculated that many legacy CII

nowadays are at level one with has no cyber resilience (Strom et al., 2017).

The following two levels consider the static type of cyber resilience, whereas level two, performed, involves implementing foundational cybersecurity controls that provide more or less cyber protection against limited cyberattacks (AlHamdani, 2020). Unfortunately, the CII's at this level have inconsistent responses to mitigate the effect of cyberattacks with very late recovery and mission normalization uncertain (Johnson, 2015).

Table 2.5: Cyber Resilience Maturity Matrix of Interdependent CII Networks (Gilligan, 2016 modified)

Types of Cyber Resilience	Cyber Resilience Maturity Levels		Cybersecurity Capabilities		Cyber Continuity Capabilities	
			Withstanding Capability	Mitigation Capability	Recovery Capability	Normalization Capability
Dynamic Cyber Resilience	Level 5	Resilient	Operate through a very sophisticated cyberattack	Integrated response to anticipate cyberattack	Real-time recovery	Mission assurance focused
	Level 4	Developed	Able to absorb sophisticated cyberattack	Continuous reaction to cyberattack	Rapid recovery	Mission focused
Static Cyber Resilience	Level 3	Managed	Cyber protected against moderate cyberattack	Slow respond to cyberattack	Recovery after fact	Partially mission-focused
	Level 2	Performed	Some cyber protection against limited cyberattack	Inconsistent response to a cyberattack	Very late recovery	Mission uncertain
No Cyber Resilience	Level 1	Essential	Susceptible to very limited cyberattack	No mitigation	No recovery	No normalization

Cyber resilience capabilities for coupled CII networks in level three are managed and protected against moderate cyberattacks with monitored cybersecurity controls in place endlessly (Carias et al., 2019). Besides, level three's mitigation capability delivers a slow response to cyberattacks and recovery after failure, partially focused on the coupled CII's mission (Liu et al., 2016).

Levels four and five are considered dynamic types in establishing cyber resilience (Alcaraz, 2018). Upon that, level four referred to the ability to absorb a sophisticated cyber-attack with the continuous reaction as a developed baseline based on CII's mission information and needs (Schwind et al., 2016). Level 4's recovery is rapid, with a mission-focused critical function normalization (Vugrin et al., 2014).

Finally, level five is the highest level of cyber resilience maturity in the matrix, and the coupled CII networks are described as resilient (Conklin & Kohnke, 2017). Interdependent CII's are

operating at this level exhibit anticipation of cyberattacks and can operate through a very sophisticated cyber-attack (Siddiqui et al., 2019). Operate with real-time recovery and mission assurance that assume an augmented baseline (Ormrod & Turnbull, 2019).

Furthermore, the static and dynamic types provided that help in cyber resilience for disruptive recovery of interdependent in CII networks against cyberattacks are establishing the capabilities (Ani et al., 2019) as the following:

(1) Static cyber resilience: support improving the long-term recovery behavior of the CII networks after disruptions (Tundis et al., 2017). Primarily the focus is to quantify the disruptive response that is time-independent and only concerned with the long-term capabilities of coupled networks to rearrange itself (Balchanos, 2012). Thus, the link taken towards recovery is irrelevant, and the only driving factor for cyber resilience is withstanding the capability to the initial disruptive impacts regarding quantifying such cyber resilience (Sirika & Mahajan, 2016).

The static cyber resilience is a time-independent probabilistic and cannot be used in real-time for decision making because the capabilities of withstanding, mitigation, recovery, and normalization are not considered to the actual impacts and dynamics of different types of cyber failure events; therefore, the CII remained to have the same behavior results over the timeline (Balchanos, 2012).

Furthermore, the static cyber resilience does not capture the importance of CII structure, and interrelationships between CII components do not capture interactions between CII behavior and the failure event and ignore the complex dynamics of CII response (Carias et al., 2019).

Additionally, it cannot assess how capable the CII is to absorb the disruption and cannot include the ability of the CII to deliver a partial level of service (Thorisson et al., 2020). While static cyber resilience measures are more appropriate for assessing pre-disturbance CII vulnerabilities,



they cannot capture the recovery process dynamics. They cannot identify when the CII will recover to a normal functioning state (Sansavini & Fang, 2016), as shown in Figure 2.11.

(2) Dynamic cyber resilience: when the short-term recovery behavior of interdependent CII networks needs to be improved, it involves understanding the link the network takes from the onset of disruption until any given time (Alcaraz, 2018). Such behavior shows properties that indicate dynamic cyber resilience (Balchanos, 2012). Furthermore, the quantification of the dynamic responses helps establish effective cyber resilience measures (Lyn, 2015).

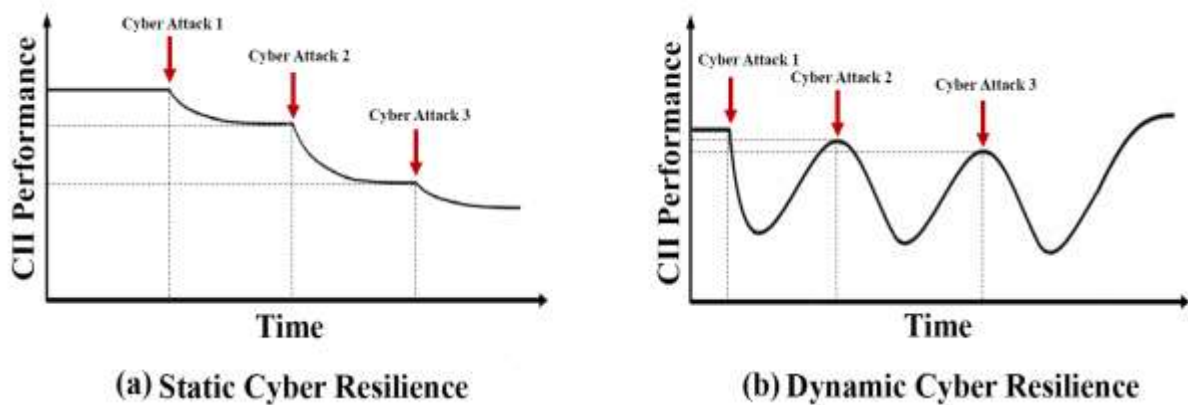


Figure 2.11: CII Performance Changing after Consecutive Cyberattacks  
(a) Static Cyber Resilience. (b) Dynamic Cyber Resilience. (Alcaraz, 2018 modified)

The dynamic cyber resilience can be used in real-time to evaluate proactive and reactive concepts because it is varied based on the cyberattacks' impact to provide all capabilities of withstanding, mitigation, recovery, and normalization during the different cyber failure events (Carias et al., 2019). It also captured the consequences of various feedback within the CII produced by interdependencies of CII components, future unknown CII states, and the importance of spatial and temporal CII scales (Liu et al., 2016).

The dynamic cyber resilience is achieved by implementing the above four capabilities that enable the CII to adapt to the cyber failure impacts and enhance its components to function during the

cyber failure (Rasouli et al., 2014). In addition, these capabilities help the CII components cope with and recover from disturbing events to return to a pre-disturbance level of performance as rapidly as possible (Villate, 2014).

Static and dynamic cyber resilience drive interdependent networks' responses and fundamental measures (Schwind et al., 2016). In establishing an improved response leading to strengthened cyber resilience, there is also scope for incorporating new measures that help the CIIs withstand further impacts and update their response to future disruptions (Barker et al., 2017).

### **2.2.2 Standard solutions of Dynamic Cyber Resilience**

Today, critical information infrastructures' operating environments are becoming unstable and complex (Cai et al., 2018). Therefore, cyber resilience engineering must address the core principles of dynamic cyber resilience that stem from the research observations of cyber resilience thinking by technology solutions of multi-faceted capabilities can be developed (Dimase et al., 2015).

Cyber resilience engineering, in particular, has seen much research progress in recent years and emerged as a new discipline within CIIs to cope specifically the various challenges of absorption, mitigation, recovering from, and adaptation to cyber failures with maintaining an acceptable level of service in the face of cyberattacks to normal operations (Häring et al., 2016). This level affects how to access information when needed, provide end-to-end communications, and ensure smooth distributed functions over CIIs (Laderman et al., 2015).

Cyber resilience engineering research streams have two key strategies: soft and hard (Mo et al., 2017). The soft strategy is widely used due to its economic and technical costs because it focuses on the topological shortest path between the source node and the destination node passing through the hub nodes in CII networks that lead to traffic congestions and less cyber resiliency

(Sansavini, 2017).

This fact consequently motivates to improve the efficiency of the soft strategy dynamics, especially in the complex heterogeneous CII networks, by spreading the traffic among the hubs according to the nodes' degree (Kleij & Leukfeldt, 2019). Moreover, creating early warnings, handling the delivery of traffic capacity, and estimating the projected waiting time along with the average shortest path lengthening (Chowdhury et al., 2020).

On the contrary, the hard strategy means the topological structure is appropriately changed so that there is an underlying relation between cascading dynamics and the congestion of traffic (Başar & Zhu, 2012). Cascading dynamics involve that small failures can trigger breakdown on a global scale on hub nodes through cascading (Du et al., 2015).

Hence, these dynamics can be optimized by removing specific hub nodes or highly congested interlinks from different kinds of existing CII networks to become more operationally convenient, consistently increasing, and economical in real production environments (Fernando et al., 2017).

The hard strategy usually helps to enhance dynamical synchronization, redistributes traffic loads, and mitigates the cascades of overloading on coupled scale-free networks, and easy to be implemented at a low cost, while adding interlinks or rewiring hub nodes is more costly than the soft strategy (Hayel & Zhu, 2015).

Based on both soft and hard strategies, several standard solutions of dynamic cyber resilience were developed, implemented, and optimized from the mid-1980s until nowadays to deal with the challenges of cyber failures of the CIIs and adapt to disturbing events (Grafenauer et al., 2018). As such, they continually adjust the behavior of the CIIs to change conditions in a risk-managed fashion (Hromada et al., 2018).

In general, a set of characteristics might be available in the technology solution to be ideal for

dynamic cyber resilience as the following: (1) Adaptive solution to the topology dynamics of CII networks (Zio & Fang, 2019). (2) The solution makes limited network broadcasting reduce traffic collisions (Divakaran et al., 2017). (3) The solution provides fast network convergence (Goldbeck et al., 2019). (4) Loop-Free and time-sensitive solution (Holden et al., 2013). (5) The solution utilizes network resource usage (Yazdanparast et al., 2018). (6) A localized solution means that it should be thoroughly networking distributed (Ouyang, 2017). (7) The solution supports the Quality-of-Service for the performance level of CII networks (Herrera & Maennel, 2019).

This section demonstrates the features and limitations of the three standard solutions. These solutions include Distance-Vector solution, Link-State solution, and Path-Rule solution (Sirika & Mahajan, 2016). Each standard solution is an integrated suite of algorithms, protocols, and mechanisms based on the layer-3 OSI model that supports the requirements of the four capabilities for dynamic cyber resilience that applied in the different environments of critical information infrastructures (Hadjoannou, 2015) as the following:

(1) Distance-Vector solution: a technological suite of algorithms and protocols developed before four decades practically for computer network routing then enhanced with mechanisms to patch the cybersecurity holes exploited by the cyberattacks (Rak, 2015). Lately, it has improved to meet the dynamic cyber resilience capabilities for dealing with the cyber resiliency requirements in different operational environments of critical information infrastructures (Malik & Sahu, 2019).

The first capability of dynamic cyber resilience in the distance-vector solution is the withstanding capability supported by the neighbor authentication with two types of plain text and Message-Digest Algorithm Type 5 (MD5) that ensures received information from trusted neighbors (Bao

et al., 2014). Furthermore, it certifies each neighbor of hub nodes' authenticity and the integrity of its shared secret key to validate each routing update (Manzoor et al., 2020).

Correspondingly, it protects secure data and peering sessions from cyberattacks such as unauthorized peer insertion or removal of authorized ones, injection of false data or modification of legitimate information, or session reset attempts (Mohammad et al., 2017).

Further mechanisms for withstanding are access control techniques such as Infrastructure Protection Access Control Lists (iACLs) that shields the CII networks from internal and external cyberattacks. It is designed to permit explicitly authorized control and management traffic bound to the CII networks while denying any other traffic directed to the address space (Masood et al., 2016). iACLs protect hub nodes from DDoS cyberattacks by preventing the establishment of unauthorized sessions and by reducing the chances for session reset, preventing the injection, modification, or removal of information (Behal & Kumar, 2016).

Route filtering is another vital tool to secure the CII networks divided into two topologies: hub and spoke; the first form filters the information exchanged between the hub nodes (Glesk et al., 2016). The second form filters the information exchanged between the stub nodes, where the spoke nodes direct all traffic to a hub distribution node (Ullah et al., 2018). The stub configuration helps control the propagation of routing information from the spoke node, preventing the distribution of false data and manipulating trusted routes (Ottenburger et al., 2020).

The stub node is configured to permit static, connected independently, and summary routes (Turnquist & Vugrin, 2012). In this case, a bogus node is installed in the stub network, assuming the bogus node establishes a peering session effectively. Thus, the stub node will learn any routing data originating from the bogus node, but it will not pass it onto other nodes, shielding

the rest of the routing infrastructure from the potential injection of incorrect data (Yuan et al., 2016).

Consequentially, cyberattacks' success scenarios are handled by mitigation capability with nodal redundancy using the Gateway Load Balancing Protocol (GLBP) (Yin et al., 2018). This protocol attempts to overcome the limitations of existing redundant nodes by adding basic load balancing functionality and allows a weighting parameter to be set priorities on different hub nodes (Mode, 2020).

Another redundancy protocol is Hot Standby Router Protocol (HSRP) to establish a fault-tolerant between network nodes to achieve failover if the hub nodes become inaccessible (Bao et al., 2014). As well, Rapid Spanning Tree Protocol (RSTP) is implemented loop prevention technology, despite its shortcomings, still a very commonly used protocol (Yang et al., 2015).

The recovery capability sustained by Resilient Ethernet Protocol (REP) provides a basis for constructing a faster alternative to Spanning Tree Protocol (STP) (AlHamdani, 2020). In addition, REP controls the loops of CII networks, bridges the link failures, supports load balancing, and improves convergence time (Dsouza et al., 2013).

Besides, Fast Reroute upon Multi-homed Domains (FREMD) is a fast recovery technique using a pre-established path between the hub nodes (Sano et al., 2016). When links fail, the hub node could fast react to failure with an alternative path. The convergence is invoked if the link failure is not restored for a certain period (Uday, 2015). Once the CII network converges to another stable state, the FREMD path is withdrawn, and the CII network comes back to normal forwarding (Yong et al., 2016).

Finally, dynamic cyber resilience's normalization capability is managed by dynamic routing protocols (Hadjioannou, 2015). These layer-3 broadcast protocols' main characteristics are the

distance that identifies its distance to the destination CII network from the source-based total on a metric including the hop depends, value, bandwidth, and delay (Manzoor et al., 2020). Moreover, the vector that specifies the subsequent-hop node or exit interface route reaches the destination (Malik & Sahu, 2019).

Also, it collects statistics of the records of the routing desk of its neighbors. Determine the better direction, adding the metric cost acquired as the routing facts happen from one node to another. The alternate topology updates consist of periodic updates of the tables (Masood et al., 2016).

For example, the Routing Information Protocol (RIP) is based on the Floyd-Warshall algorithm using hop-counting metrics (Dinitz & Itzhak, 2017). It has advantages in small CII networks, is easy to understand, configure, is widely used, and is supported by almost all nodes. However, RIP is limited to 15 hops, updates every 30 seconds, is inappropriate for large CII networks, and has less efficient convergence without support for multiple paths (Zhao et al., 2017).

The classful RIPv1 (1988) and classless RIPv2 (1994) are working with regular Internet Protocol (IPv4), but RIPng (1997) is working with a new version of the Internet Protocol (IPv6) (Dünner et al., 2018). IPv6 specifies a new packet format designed to minimize packet header processing by network routers (Kalala, 2017). Because the headers of IPv4 and IPv6 packets are significantly different, the two protocols are not interoperable. However, IPv6 is a conservative extension of IPv4 (Yu, 2013).

Likewise, another dynamic routing protocol is Enhanced Interior Gateway Routing Protocol (EIGRP), developed by Cisco in 1993 based on the Diffusion Update Algorithm (DUAL), was an enhanced version of the Interior Gateway Routing Protocol (IGRP) published in 1985 based on Bellman-Ford algorithm (Singh & Tripathi, 2018). EIGRP worked with IPv4 and IPv6 and was mostly deployed in massive CII networks with quicker convergence, ease of configuration,

and maximum hops of 255 (Kalpana & Tyagi, 2017).

There are three tables to make routing selections in EIGRP. Those are the routing table, the neighbor table, and the topology table (Zhao et al., 2017). Therefore, all information stored can quickly adapt to alternate routes (Dünner et al., 2018). EIGRP used bandwidth, delay, reliability, load, and MTU as the metrics to determine the best route from the source to the end. In addition, the variable-length subnet mask reduces time to CII network convergence and increases scalability (Wang, 2018).

(2) Link-State solution: is a technological suite like a Distance-Vector solution in terms of their being from one family of Interior Gateway Protocols (IGP), but they are different regarding algorithms and protocols (Hadjioannou, 2015). The development of the Link-State solution started in 1990, i.e., after the Distance-Vector solution about a decade, and the improvement continued to these days (Malik & Sahu, 2019).

This chance allows studying the previous limitations and attempting to cope with the shortcomings of the Distance-Vector solution in dynamic cyber resilience for critical information infrastructures (Glesk et al., 2016). In addition to neighbor authentication and load balancing between several hub nodes, the capability of withstanding has been handled in the Link-State solution using the default passive-interface (Sirika & Mahajan, 2016). It protects the nodes from DDoS cyberattacks by controlling the propagation of routing updates, but at the same time, it prevents neither the insertion of unauthorized nodes nor the insertion, modification, or removal of information (Bhuyan et al., 2015).

Moreover, a distributed list is a unidirectional technique that controls the acceptance or rejection of the route information in the CII networks based on the suite of standard criteria (Hui et al., 2014). A distribute-list filter affects all outgoing updates sent or received between hub nodes and



information derived from redistribution (Shevchuk, 2019).

The redundancy concept applies to the mitigation capability in this dynamic cyber resilience solution through the Automatic Protection Switching (APS) protocol to remove hub nodes when they fail by new ones immediately taking over (O’Kelly, 2015). In addition, APS protects against cyber failures between the particular hub node and one or more others and between multiple links in the same hub node (Başar & Zhu, 2012).

Furthermore, the Virtual Router Redundancy Protocol (VRRP) is designed to increase the master hub nodes’ availability on the same subnet of the CII network (Rozorinov et al., 2017). Furthermore, this protocol achieved reliability by advertising a virtual hub nodes group as an abstract representation of master and backup hub nodes acting as a group instead of one physical hub node (Bergström et al., 2015).

Another redundant technique used in well-designed CII networks is Level 1-2 hub node areas to be isolated from each other in the case of cyber failure occurring in one area (Anne et al., 2018). For example, if the Level 2 adjacency fails on the first Level 1-2 hub node, installing a default route points to the second Level 1-2 hub node. It will re-flood the area with updates of the Level 1 hub nodes in the same area, remove their default route to the first Level 1-2 hub node, and replace it with a default route to the second Level 1-2 hub node (Fan et al., 2014).

According to the recovery capability, several protocols are serving this capability of dynamic cyber resilience, such as the Shortest Path Bridging (SPB) protocol, which is designed to replace the Spanning Tree in providing loop prevention and load sharing between links by advertising both topology and logical network membership (Sapundzhi & Popstoilov, 2018). Additionally, the Resilient Packet Ring (RPR) protocol is a standard designed for the optimized transport of data traffic for providing cyber resilience over CII networks to increase the efficiency of IP

services (Rak, 2015).

Additionally, Link-State Information Refreshing (LIRP) protocol is a remaining lifetime that must refresh periodically by each originator hub node that has a checksum; if the checksum is deemed incorrect by the receiving hub node, the database purged, and a new one is requested from the originating hub node (Shoemaker et al., 2017).

Similarly, the Reliable Flooding Protocol (RFP) checks any change in the point-to-point links among hub nodes, which means that the updates need to be resent to the whole CII network to update other hub nodes' changed topology (LaRocca, 2014). Newer updates are tagged with a more significant sequence number and recognized by the other hub nodes (Liu, 2016).

Correspondingly, the typical hub nodes used the adjacency-processing technique to handle the half-broken links that flap between adjacency states by so-called hold timer to delay artificially bringing up a link (Bashan et al., 2011). Links that have flapped frequently will have a higher hold timer value than links that have not experienced flapping (Wang et al., 2017). Thus, the CII network is not overwhelmed by frequent updates resulting from a flapping link (Hayel & Zhu, 2015). Another behavior technique that affects recovery capability against failures is network liveness detection (Burla et al., 2016). Frequent message timers sent by hub nodes allow fast detection of lost adjacency state is possible (De Florio, 2015).

Finally, the normalization capability in the Link-State solution is popularly administered by two dynamic routing protocols; Open Shortest Path First (OSPF) protocol and Intermediate System to Intermediate System (IS-IS) protocol (Dinitz & Itzhak, 2017). Both multicast protocols based on the Dijkstra shortest path algorithm calculate the path costs to distribute the information over the CII network (Singh & Tripathi, 2018).

They create a complete view of the network topology by gathering statistics from all nodes to

choose the first-class path to all destination networks inside the topology (Herrmann et al., 2011). Therefore, the hierarchical design and fast convergence of CII networks are essential (Cetinkaya et al., 2017). Furthermore, these protocols do not use periodic updates, but instead of that, each hub node independently calculates its significantly shorter direction of the CII network's destiny (Sterbenz et al., 2013).

OSPF protocol is more common in smaller CII networks and has better cyber-physical support than IS-IS protocol (Hadjioannou, 2015). The structural design of CII networks for IS-IS is different from that used in OSPF. IS-IS does not have a single CII network like OSPF (Manzoor et al., 2020). Instead, several hub nodes in different CII networks form a coupled network by IS-IS (Malik & Sahu, 2019). In contrast, CII networks built using OSPF have a spider-web style topology, where the edge networks are attached to the core CII network (Glesk et al., 2016).

The OSPF protocol was introduced by Internet Engineering Task Force (IETF) and released in three versions; the last one was in 1999 and compatible with IPv6 (Sirika & Mahajan, 2016). It continuously determines the loop-free routes, routinely updates any adjustments, and helps multiple hub nodes for a single trip advertisement with low bandwidth usage (Chen, 2016).

On the other hand, IS-IS protocol for routing datagrams in the Connectionless Network Service (CLNS) using Network Service Access Point (NSAP) type of addresses on layer-3 of the OSI model (Ventresca & Aleman, 2015). It has two versions, the first one developed in 1990 for IPv4 and the second version published in 2000 to support IPv6 correctly (Hadjioannou, 2015). IS-IS determines the best paths for datagrams to follow across a packet-switched network by dividing the network into separate areas, storing the topology information in each hub node, and exchanging it with others (Cetinkaya et al., 2017).

(3) Path-Rule solution: a technological suite consisting of integrated sub-solutions and supports

dynamic cyber resilience capabilities between coupled networks. The solution was developed after Distance-Vector and Link-State solutions in 1995 (Fotouhi et al., 2017). It belongs to the Exterior Gateway Protocols (EGP) family, is not based on specific algorithms like standard solutions but depends on rule sets and local policies according to the different aspects of the CII environment (Dünner et al., 2018).

The withstanding capability covers by Secure Border Gateway Protocol (S-BGP) to protect the leading edges of CII networks through three significant features (Manzoor et al., 2020). Initially, strong authentication verifies the hub nodes in the coupled networks (Schneider et al., 2013). In the Second place, Public Key Infrastructure (PKI) cryptography authorizes ownership and validates the information (Vasilyev et al., 2017). Finally, IP Security (IPSec) protocol using for communication confidentiality (Dupont, B. (2019).

Similarly, the Secure Origin BGP (So-BGP) was introduced as a lightweight alternative to S-BGP for bleeding edges of CII networks to verify two information issues: the authoritative and the advertising hub node has at least one valid path to the destination (Hadjoannou, 2015). It utilizes three types of certificates for the required verification of the topology database and validates received information (Manzoor et al., 2020).

Furthermore, the path-rule solution used TTL Security Check to protect hub nodes from multi-hop cyberattacks. It allows the configuration of a minimum acceptable TTL value for the information exchanged between two hub nodes (AlHamdani, 2020). When enabled, both transmit all their traffic to each other by establishing a secure session only if another hub node sends a TTL value equal to or greater than the TTL value configured for the secure session (Johnson, 2015). Otherwise, the mechanism resets unauthorized sessions to prevent DDoS cyberattacks (Wright et al., 2016).

As well, the First Hop Redundancy Protocol (FHRP) and Virtual Router Redundancy Protocol (VRRP) are an essential part of the mitigation capability of dynamic cyber resilience that is widely implemented and played a vital role in access CII networks as well as service providing (Yin et al., 2018). Both protocols allow for transparent failover at the first-hop hub node and enable two or more hub nodes to work together in a cluster, sharing a single and virtual IP address (Rozorinov et al., 2017).

Regarding mitigation capability again, the demand controlling technique is used by Control Plane Policing (CoPP) to enforce hub nodes by the policies of Quality-of-Service (QoS) for regulating to permit, block, or rate-limit the network traffic handled by the CII networks (Chmutina et al., 2016). Furthermore, CoPP separates this traffic into multiple classification schemes based on relative importance and traffic type to mitigate the failure effects caused by the range of cyberattacks like DDoS (Georgiev & Nikolova, 2017).

The recovery capability in the Path-Rule solution enhanced by fast reroute compatible Fast Recovery technique upon Multi-homed Domains (FREMMD) to support the CII network comes back to normal forwarding after cyber failure (Ghanbari et al., 2018). Another recovery technique used is the Path Computation for Resilient Networks (PCRN) (Liu et al., 2016).

It also provides backup paths selected randomly and finds a suitable backup path (Wang et al., 2017). This technique rebuilds the current path from a given hub node or replaces an existing path with another one from the set of backup paths generated in the beginning to have a different hub node in each search process (Sapundzhi & Popstoilov, 2018).

Additionally, the Path Diversification Mechanism (PDM) selects multiple paths between a given ingress and egress hub node using a quantified diversity measure to achieve maximum recovery flow. The paths chosen will not experience correlated failures (Mitchell & Chen, 2016). To this

end, a measure of diversity quantifies the degree to which alternate paths share the same hub nodes and links (Mosharraf et al., 2015).

Lastly, the normalization capability is dealing with the Border Gateway Protocol (BGP) or internal Border Gateway Protocol (iBGP) (Manzoor et al., 2020). Formally, BGP is routing the network traffic between independent CII networks known as Autonomous Systems (inter-AS), but iBGP is routing the network traffic inside the CII network (Marais & Uday, 2015). Both unicast protocols are crucial to sustain neighbor relationships and keep the connectivity updates within the CII network or other CII networks (Chowdhury et al., 2020).

These protocols support the core routing decisions by maintaining a table of IP addresses that designate the CII networks' reachability (Hadjioannou, 2015). They described path-rule protocols because they make routing decisions based on path, network policies, or rule sets (Glesk et al., 2016). For this reason, they are more appropriately termed reachability protocols rather than routing protocols (Mohammad et al., 2017).

The above three technology solutions have common limitations based on their operating environments of critical information infrastructures that summarized as the following:

(1) The different compatibility of technology solutions with architectural couplings of CII networks (Wilner, 2017). The Distance-Vector solution is ideal for small-centric, simple, and non-hierarchical CII networks (Shoemaker et al., 2017). Link-State solution for large decentralized, complex, and hierarchical CII networks, while independent and distributed CII networks use Path-Rule solution (Brennan et al., 2019).

(2) The diverse adaptation of technology solutions with topology dynamics of CII networks (Glesk et al., 2016). The Distance-Vector solution is perfect for dealing with the star topology changes, and the Link-State solution is proper for handling with mobility of scale-free topology

over time (Cao et al., 2017). In contrast, the Path-Rule solution has typical actions to address the breakage of paths for the mesh topologies of the CII networks (Tian et al., 2015).

(3) The distinct convergence of technology solutions with interdependency updates of CII networks (Almoghathawi et al., 2019). The Distance-Vector solution has fast convergence with multiple network broadcasting modes for updating, but sometimes the neighboring transmitter prevents the broadcasts (Buldyrev et al., 2012). In comparison, the Link-State solution uses network multicasting to explore the hidden sub-clusters in the CII networks, slowing down the convergence for the traffic collisions (Francia et al., 2018). The Path-Rule solution stores the tables of stable paths that are automatically updated by network unicasting; therefore, its convergence is slow in unstable paths (Dong et al., 2013).

(4) The various recovery of technology solutions with failure effects of CII networks (Brown et al., 2010). The Distance-Vector solution effectively reduces the effects of cascading failure of Distributed Denial of Service (DDoS) cyberattacks to increase performance recovery (Liu et al., 2016). However, the Link-State solution manages the escalating effects efficiently because the hub nodes are extremely attractive and vulnerable to this pattern of cyberattacks (Vugrin et al., 2014). It enhances the CII networks to be recovered to the equilibrium state (Wright et al., 2016). Nevertheless, the Path-Rule solution actively treats the common failures of the CII networks caused by DDoS to achieve maximum recovery with minimum adverse effects to reach an acceptable performance level (Georgiev & Nikolova, 2017).

### **2.2.3 Quantification of Dynamic Cyber Resilience**

Understanding and analyzing the high disruptive dynamics of CIIs' cyber resilience is a vital research area when studying cascade effects between interdependent infrastructures, which are increasingly targets of cyberattacks (Fotouhi et al., 2017). The cyber-resilient CII account for

maintaining desired capabilities of withstanding, mitigating, recovering, and normalization quickly and smoothly transitions from degraded to recovered states to mission success (Nan et al., 2014).

The observations in the literature of cyber resilience engineering noted the importance of evaluating cyber resilience to enable design trade-off studies (Häring et al., 2016). These observations were used to satisfy the established requirements for selecting the approach to quantify the dynamic cyber resilience of critical information infrastructures (Nan & Sansavini, 2017).

The selected approach should provide a set of quantification metrics to evaluate dynamic cyber resilience capabilities that derive from specific criteria summarized as the following: quantitative, capability-based, dynamic, time-dependent, and failure-dependent (Moraitis et al., 2020). Therefore, various approaches for quantifying dynamic cyber resilience have been proposed in the most representative stream of relevant literature, as shown in Table 2.6.

At a glance, Vugrin et al. (2010) provide the system resilience approach as a quantitative method partially for evaluating cyber resilience (Balchanos, 2012). However, this approach directly accounts for CII capabilities through systemic impact calculations but does not provide detailed quantitative calculations to differentiate how CII absorbs, recovers, and adapts to cyberattack (Guo, 2010).

Instead, the characterization of these cyber resilience capacities is limited to qualitative comparisons. Over time, performance and cost measurements account for dynamic CII behavior (Creese et al., 2011). However, smooth capability transitions are not accounted for since integration removes some capability data dynamics (Camphouse & Vugrin, 2011).

Besides, the approach is limited in quantitatively comparing the resilience of multiple CII designs



(Brown et al., 2010). Integrating CII performance and cost concerning time provides quantitative values for comparison but makes it difficult to differentiate between CIIs with similar integrated values yet vastly different dynamic behaviors (Bodeau et al., 2013).

The authors extend this approach with a stochastic optimization model but only consider three methods of improving resilience: overdesigning CIIs and providing redundancy, ignoring potential adaptation methods (Chen, 2016).

Table 2.6: Comparison of Quantification Approaches for Dynamic Cyber Resilience

<i>Year</i>	2010	2010	2012	2013	2014	2015	2018	2018	2019
<i>Author(s)</i>	Vugrin et al.	Sterbenz et al.	Balchanos	Simonovic & Peck	Francis & Bekera	Tran	Bodeau et al.	Haque et al.	Ellingwood et al.
<i>Approach</i>	System Resilience	ResiliNets	TIRESIAS	System Dynamics	Resilience Factor	Complex Networks	MOEs	CRAM	IN-CORE
<i>Criteria</i>									
<i>Quantitative</i>	Partially	Partially	Yes	Partially	Yes	Yes	Yes	Partially	Partially
<i>Capability-Based</i>	Yes	Yes	Yes	No	Yes	Yes	No	No	Yes
<i>Dynamic</i>	Partially	Partially	Partially	Yes	Partially	Yes	Partially	Yes	Partially
<i>Failure-Dependent</i>	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
<i>Time-Dependent</i>	No	No	Yes	Yes	Yes	Yes	No	No	Yes

Moreover, Sterbenz et al. (2010) propose the ResiliNets approach as a cyber-resilience state space to evaluate the cyber resilience of a potential CII facing a given cyber-attack (Bodeau & Graubart, 2016). Desired capabilities are used as the state space’s service parameter (Mitra et al., 2010). The state-space provides a dynamic consideration of CII performance by tracking how the CII behaves throughout an engagement (Linkov et al., 2013).

However, there is no suggested quantification of the various capacities of cyber resilience or the ability to provide smooth transitions from degraded to recovered states (Bhuyan et al., 2015). It is mainly limited to an assessment approach, with conceptual suggestions for improving CII cyber resilience (Wang & Ouyang, 2015). Additionally, the authors focus on assessing the cyber resilience of static CII topologies without considering how a CII might adapt to improve its cyber resilience (Guo, 2010).

Furthermore, Balchanos (2012) presents TIRESIAS as a quantitative approach for assessing CII cyber resilience (Wang & Ouyang, 2015). This approach extended by adding quantitative metrics to characterize how well the CII absorbs and recovers from a failure (Bodeau & Graubart, 2013). These metrics allow a more redefined comparison between potential CII that also considers the dynamic behavior of a CII following a failure (Tran, 2015).

However, these metrics are limited in their ability to characterize the smoothness of capability transitions and adaptation to repeated cyberattacks and focus on assessing CII cyber resilience rather than designing resilient CII networks (Kiss et al., 2015). They provide limited guidance on how CII networks should be defined structurally and incorporate adaptation to achieve cyber resilience (Chen, 2016).

Additionally, Simonovic and Peck (2013) developed an approach to quantify the dynamic cyber resilience through system dynamics simulation in understanding the dynamic behavior of CII, thereby enabling a more integrated approach to increase their cyber resilience (Häyhtiö & Zaerens, 2017).

The approach allows for the understanding of factors contributing to cyber resilience in the context of cyber vulnerability and exposure and gives a more systematic assessment of various measures to increase cyber resilience (Di Pietro et al., 2017). However, it is limited to cost-benefit analysis, whether for direct or indirect quantitative measures for cyber resilience of CII networks (Chen, 2016).

Besides, Francis and Bekera (2014) define a system resilience factor that extends other cyber resilience metrics by explicitly considering recovery time factors to capture temporal aspects of cyber resilience, in addition to recovered and degraded performance levels of CII (Nan & Sansavini, 2017).

They also account for uncertainty in event occurrences by considering event probabilities (Nazir et al., 2017). Hence, their approach enables design comparisons and aids decision-making processes by providing a single value for CII's cyber resilience and can be seen as a cyber-resilience based on risk assessment (Kiss et al., 2015).

However, there is limited guidance on calculating recovery time and recovered performance levels for CII's facing multiple threats with volatile data (Marais & Uday, 2015). Besides, their cyber resilience metric does not consider the intermediate variation of CII performance during recovery or the ability to adapt to multiple disruptions over time (Wang & Ouyang, 2015).

Correspondingly, Tran (2015) presents a novel approach to complex networks that includes a quantitative mechanism for the life cycle framework of cyber resilient CII networks (McCollum et al., 2018). This framework enables quantitative comparisons of potential topology structures and suspected vulnerabilities to their integrated cyber resilience metrics, cyber resilience metric  $R$  for identified single failure, and total cyber resilience metric  $R_{total}$  for multiple failures (Beyza et al., 2019).

These metrics are capability-based, time-dependent, and calculated by a set of cyber resilience factors, consider the framework's primary contribution, and apply them to ICS-based and ICT-based infrastructures (Sepúlveda-Estay et al., 2020).

The cyber resilience factors include the performance factor that accounts for the total performance maintained by the CII's over time (Patrman et al., 2019). The recovery factor accounts for the end state of the CII's (Liu et al., 2016). To end with the absorption factor that accounts for the ability of the CII's to absorb the effects of failures (Yong et al., 2016).

A volatility factor accounts for the ability of the CII's to smoothly transition from degraded to recovered state (Canzani, 2016). Finally, a normalized recovery time factor accounts for the CII's

response's temporal aspects by calculating the time required to reach the following steady-state failures (Sansavini & Fang, 2016).

However, there are limitations to this approach; firstly, CII networks are defined to be homogeneous for individual CII properties, although many CIIs are heterogeneous with varying properties (Rehak et al., 2018). In addition to the assumption that nodes have global knowledge of the complete topology of the CII network at any given time (Cetinkaya et al., 2017).

Due to the large scale and geographic dispersion of many CIIs, this assumption may not always be accurate (Cao et al., 2017). Besides, focusing on single-layered CII networks with the attention that CIIs are usually characterized by multi-layered alongside interdependencies would extend the consideration of failures in one layer affecting the behaviors occurring in other layers (Burla et al., 2016).

Similarly, Bodeau et al. (2018), funded by MITRE Corporation, presents an approach of cyber resiliency measures of effectiveness (MOEs) for providing different angles of cyber resilience study and a lack of clear explanation of the quantitative resilience metrics formulation (Gasser et al., 2019). The approach defines, evaluates, assesses alternative cyber resiliency solutions, and identifies improvement areas of cyber resiliency to evaluate the extensible scoring methodology (Haque et al., 2019).

However, this approach's main limitations are that it is most suitable for ICT-based infrastructure rather than ICS-based infrastructure (Hromada et al., 2018). Moreover, comparing metric values across CIIs requires consistency in assumptions about the context in which the metric is meaningful (Igor & Aleksandr, 2018). Finally, in addition to combining cyber resiliency metrics for CIIs supporting functions, it is similar to that for cybersecurity metrics for other areas in CIIs' properties, and behaviors are emergent (Goldbeck et al., 2019).

Likewise, Haque et al. (2018) propose a comprehensive approach of the Cyber Resilience Assessment Model (CRAM) for ICS-based infrastructures using the R4 framework comprises four broad metrics of cyber resilience, are Robustness, Redundancy, Resourcefulness, and Rapidity (Kamissoko et al., 2019). They decompose the cyber resilience metric into several sub-metrics hierarchies; each can be analyzed independently (Mbanaso et al., 2019). The approach derives directions in the ICS-based analysis and assessment process using the quantitative metrics for cyber resilience (Hromada et al., 2018).

However, these metrics are organized in a tree structure that captures data depending on the effective functioning of all aspects, not limited to cybers but physical security, organizational practices, and technologies implemented in the ICS-based infrastructures (McCollum et al., 2018). Additionally, it focuses on the experts' and operators' technical opinions to periodically assess the ICS-based environment's changing issues (Panzieri et al., 2019).

In addition, Ellingwood et al. (2019) from the National Institute of Standards and Technology (NIST) provide an approach of Interdependent Networked Community Resilience Modeling Environment (IN-CORE) for improving the cyber resilience of CIIs (Kamissoko et al., 2019). This approach identifies detailed guidelines of five functions that organize cyber resilience at the highest levels: identify, protect, detect, respond, and recover (Kumar et al., 2020).

The authors define the necessary measures to make ICS-based infrastructures resilient (Mbanaso et al., 2019). IN-CORE has already laid the groundwork for understanding the factors that make the ICS-based infrastructures resilient, assessing the likely impacts of cyber risks on them, and developing risk-informed decision strategies that optimize planning and recovery from failures (Potii & Tsyplinsky, 2020). However, it does not provide an approach to quantify the cyber resilience metrics of ICT-based infrastructures (Selifanov et al., 2020).

## **2.3 Findings of the Literature Review**

A systematic review reveals two literature streams selected and analyzed to provide substantial theoretical foundations for this research (Singh et al., 2016). Furthermore, these streams' specific findings meet with the research gaps observing the understanding of interdependent CII networks and the availability of technology solutions for their cyber resilience (Xiong & Lagerström, 2019).

The first stream is the well-established section of critical information infrastructures, which offers valuable insights on three composite subsections of coupling behavior across interdependency, cyber vulnerability analysis of scale-free topology, and failure under concurrent and consecutive cyberattacks (Banerjee et al., 2018).

The majority of studies focus on handling the issues of physical resilience and cyber-physical resilience rather than cyber resilience (Hansen, 2019). Therefore, limited studies on critical information infrastructures compared to critical infrastructures (Lewis, 2019). In addition to the widespread scientific efforts that consternate homogeneous CII networks' cyber interdependency, there is a lack of research on heterogeneous ones (Ottenburger et al., 2020).

Furthermore, the familiar works discuss the technical vulnerabilities of CIIs, such as operating systems, legacy characteristics, and administration issues (Staggs & Shenoi, 2019). In opposite, the dearth one deals with the scale-free topology vulnerability of coupled CII networks (Lazari, 2014).

Besides, the recent research discussions are dedicated to the single or multiple cyberattacks with spaced time intervals and cascading failures only. However, there is a shortage of discussions on the concurrent and consecutive cyberattacks against CII networks that cause common, escalating,

cascading failures (Martin, 2020).

The second stream of the literature review is a deep-rooted section of dynamic cyber resilience that presents most of the research community's studies to address three integrated subsections: core principles, standard solutions, and quantification of dynamic cyber resilience (Carias et al., 2019).

However, to the best of the author's knowledge, no research papers were published concerning the comprehensive technology solution of dynamic cyber resilience for interdependent critical information infrastructures using cyber zero-trust engineering (Linkov & Kott, 2019). Generally, the existing ones tackle cyber risk management, cybersecurity, and cyber resilience in critical infrastructures using cyber trustfulness engineering (Siddiqui et al., 2019).

In particular, this thesis focuses on the ICS-based and ICT-based infrastructures in heterogeneous environments (Chowdhury et al., 2020). It accounts for its decentralized architectural coupling and vulnerability of complex scale-free topology (Fotouhi et al., 2017). Furthermore, emphasis on the complex network modeling of cyber interdependency with agent-based modeling (Thompson et al., 2019).

Moreover, studying the non-linear behaviors of hub nodes in the CII networks under concurrent and consecutive cyberattacks of DDoS by considering the Petri-Nets and STRIDE cyber threat modeling of Attack-Static and Defend-Dynamic dimensions, respectively (Xiong & Lagerström, 2019).

Additionally, examining the impacts of common cause and escalating failures throughout adverse and historical cyber scenarios with two levels of significant and advanced cyberattacks that target the function and data in the CII networks (Zheng & Albert, 2019). Likewise, exploring the resilient and developed levels based on the maturity matrix for cyber resilience (Storm et al.,

2017).

Furthermore, investigating the standard solutions' features and limitations involves Distance-Vector, Link-State, and Path-Rule solutions (Bao et al., 2014). The comparisons between these layer-3 suited solutions and the proposed solution in this research (Rak, 2015).

Besides, the complex networks approach quantifies dynamic cyber resilience capabilities because it meets the criteria of the quantification requirements (Tran, 2015). The secondary data collected from the previous literature benefited the remaining chapters of the thesis differently, especially Chapter 4 Design and Methodology and Chapter 5 Results and Discussion.



## **CHAPTER 3. THE PROPOSED SOLUTION**

Dynamic cyber resilience has become an essential topic on the protection research agenda of the cyber space's critical information infrastructures (Kalashnikov & Sakrutina, 2019). However, there is no holistic technology solution over the literature reviewing to bridge the gap by combining cybersecurity and cyber continuity concepts (Mikhalevich & Trapeznikov, 2019).

This Chapter is a potential attempt to establish a novel proposed solution to fulfill the research gaps and utterly consistent with the problem statement for achieving the research goal. Several components comprise the proposed solution's structure and its conceptual framework in this situation.

Additionally, the prototype was developed in the primary phase, and the proposed solution was improved in the optimized phase. These mechanisms involve primary and optimized algorithms, coding and recoding, and layering integration.

### **3.1 The Paradigm Shift of Dynamic Cyber Resilience**

Considering the universal nature of critical information infrastructures are an ever-increasing demand in daily life to ensure regular functions by handling the adverse effects of disruptive cyber events (Shafqat & Masood, 2016). Currently, all technology solutions of dynamic cyber resilience focus on the conceptual frameworks of cyber trust engineering to reduce the likelihood of CIIs' malfunctions and mitigate the consequences of undesirable cyber events (Spirin et al., 2020).

In contrast, the novel proposed solution adopts the paradigm shift of dynamic cyber resilience based on the cyber zero-trust approach (Kizza, 2020). Furthermore, recent adverse events against interdependent CII networks in cyberspace are more intelligent, sophisticated and demonstrate

that not all are preventable (König & Rass, 2017).

This section is organized twofold. The first part of the paradigm shift of dynamic cyber resilience for this research centers on the new perspective of cyber risk management. This perspective consists of typical cycle states, dynamic cyber resilience capabilities, cyber-efficiency-effectiveness management, and cybersecurity and cyber continuity concepts.

The second part concentrates on the fundamental concepts and competitive advantages of the novel proposed solution based on cyber zero-trust engineering to enhance the paradigm shift of dynamic cyber resilience compared to standard solutions built on trustfulness engineering in cyberspace.

### **3.1.1 New Perspective of Dynamic Cyber Resilience**

The four capabilities of dynamic cyber resilience, i.e., withstanding, mitigation, recovery, and normalization, can be obtained grounded on the ten core cyber resilience principles. These capabilities are at the center of the principles (Brennan et al., 2019). They are linked with the various states of the typical cycle of dynamic cyber resilience (threshold state, bottom state, an equilibrium state) to reduce the chances of cyberattacks shocks and absorb them when they recover quickly and re-establish the acceptable performance CII (Carias et al., 2019).

The withstanding capability refers to the degree to coupled CII networks can anticipate disruptive events, recognize unanticipated events, survive cyber aggressions, and absorb the cyber shocks of major disruptions with considerable efforts before reaching the threshold state (Ullah et al., 2018). In practice, though, it is a management feature depending on configuration, controls, and operational procedures. Robustness and reliability are prototypical pre-disruption characteristics of resilient CII (Zio & Fang, 2019).

While withstanding capability is the ability to absorb cyber perturbations, the mitigation

capability is coupled with CII networks’ ability to adjust to undesirable situations and avoid performance to drop to the bottom state by undergoing some changes on its non-essential attributes and localizing the redundant resources (Golnari & Zhang, 2015). Also, minimize escalating consequences and maintain the critical functions of CIIs during cyberattacks within acceptable degradation parameters to resist internal drifts and cascading failures (Schneider et al., 2015).

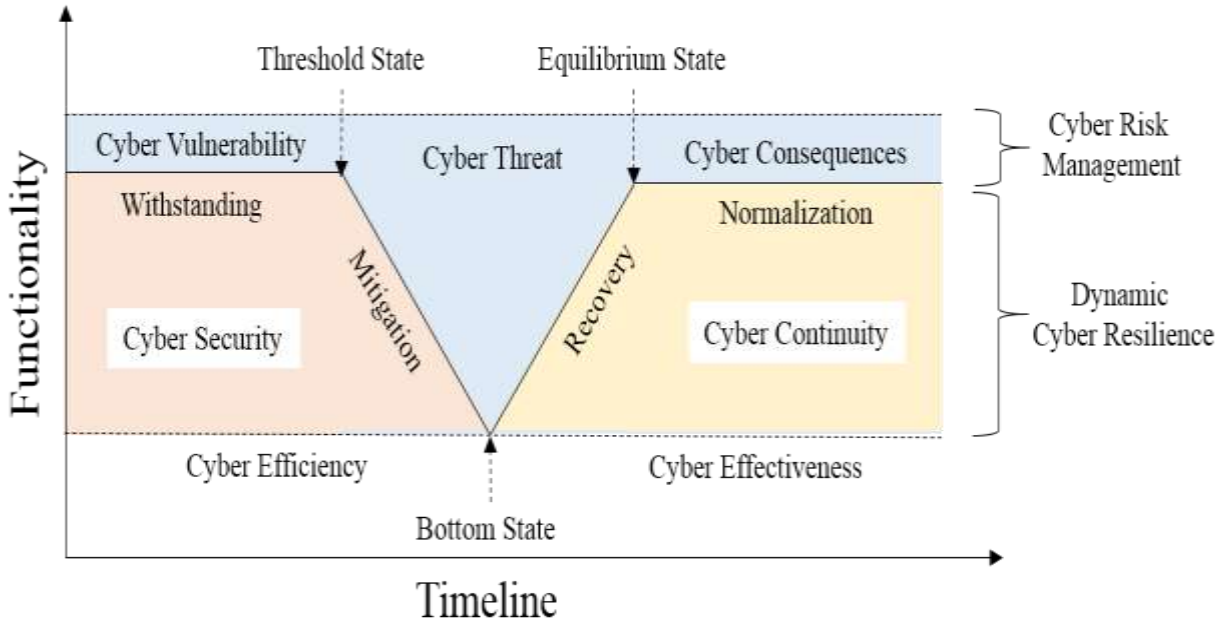


Figure 3.1: New Perspective of Dynamic Cyber Resilience

A recovery capability is enhanced by coupled CII networks’ ability to self-healing and re-organize the resources after the occurrence of an adverse event and general preparedness for cyberattack events (Liu et al., 2016). Besides, rebuilding structural properties and critical functions within an acceptable time and composite costs to recover the equilibrium state (Vugrin et al., 2014).

The normalization capability of resilient CII networks is often characterized by the rapid return to

normal or improved operations and performance reliability (Sukach et al., 2020). It supports the restorative capacities that should be assessed against a defined set of requirements derived from a desirable level of services or controls, as shown in Figure 3.1.

The dynamic cyber resilience constitutes a bridge between the proactive concepts in the cybersecurity part and the reactive concepts in the cyber continuity part (Strom et al., 2017). These two parts integrate to present an all-inclusive solution that orchestrates the four capabilities of dynamic cyber resilience: withstanding, mitigation, recovery, and normalization for sustaining the acceptable level of functional performance within a specific timeline of interdependent critical information infrastructures (Gisladottir et al., 2017).

Abstractly, cybersecurity refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. The cybersecurity part consists of three concepts, the so-called C.I.A. triad: Confidentiality, Integrity, and Availability (Maglaras et al., 2018).

The confidentiality concept aims to restrict undesired users from authenticating the CII functions (Vasilyev et al., 2019). It prevents function exfiltration throughout unauthorized transmission or removal of information from the CII network by determining the credentials and categorizing the permissions (Gamboa et al., 2020), and also avoiding data interception via obtaining access to reach sensitive data within or transmitted to or from the CII network (Dimase et al., 2015).

The integrity concept maintains the data's accuracy, trustworthiness, and consistency against modification in existing information or fabrication of new information into CII networks by setting the access controls and encrypting the data within its life cycle in the CII cyber environment (Han et al., 2016).

The availability concept emphasizes keeping up the CII functions against interruption of any

ability to use CII services or degradation in the effectiveness or performance of CII by internal and external threats through performing repairs, upgrades, and backups rigorously (Cai et al., 2018).

These three cybersecurity parts are included in the withstanding and mitigation capabilities, representing the cyber efficiency of dynamic cyber resilience (Nazir et al., 2017). The withstanding capability is the ability to absorb the cyber disturbances caused by the changing circumstances by monitoring the quality of CII and assessing the vulnerability of topology and fragility of interdependency to ensure robustness and reliability (Ottenburger et al., 2020). It is measured by the absorption factor of designed mechanisms to avoid potential failures and prevent negative impacts on other parts of substructures (Bodeau & Graubart, 2016).

The mitigation capability is to provide and operate a replica of the core functions to reduce the undesired effects after cyber failures by maintaining regular redundancy and exceeding the structure capacities (Golnari & Zhang, 2015). It is measured by the volatility factor of in-depth mechanisms in the CII that balanced the cyber efficiency to save the extra resources and the cyber effectiveness to accomplish the functionality goals (Haque et al., 2018).

The cyber continuity attempts to maintain the core functions' vitality and smooth operations of critical network systems severely influenced and suffered during and after the unplanned failure has occurred (Tran et al., 2016). The cyber continuity part consists of three concepts: resourcefulness, response, and restoration in cyberspace (Almoghathawi et al., 2019).

The resourcefulness concept explores the available opportunities to innovate the control mechanisms for mobilizing, relocating, and optimizing the limited resources in cyber risks to ensure determining both desirable and feasible levels of CII fundamental functions be deemed recovered (Yazdanparast et al., 2018).

The response concept also provides a quick reaction to facilitate recovery processes by using available resources to transfer the CII critical tasks from the degradation to the equilibrium within the complacency scope of time and performance while handling the cyber risks (Viswanathan et al., 2017).

The restoration concept seeks to recompense various cyber functionalities lost, repair problematic parts, reset the original data settings, enhance the necessary resources for returning CII to its former state before failure conditions, and run smoothly (Chowdhury et al., 2020). These three concepts of the cyber continuity part included the recovery and normalization capabilities, representing the cyber effectiveness of dynamic cyber resilience (Vugrin et al., 2014).

The recovery capability is the ability to adapt and respond to failures by quickly transforming the relevant information and resources within all parts of the infrastructures based on the recognized trust interdependencies (Zio & Fang, 2019). The self-organized mechanisms' recovery and recovery time factors are measured to reduce emerging impacts and effectively enhance communications for the cyber continuity of core functions (Marais & Uday, 2015).

The normalization capability is the ability to regain and recalibrate the original level of the critical functionality by scanning the uncovered gaps and keeping up with the translation of new information and activities into action (Sukach et al., 2020). It is measured by the performance level factor of active feedback mechanisms to reassess the design requirements of CII and overcome the current challenges (Bhuyan et al., 2015).

The threshold state plays a role in whether a critical information infrastructure has enough robustness to be able to absorb the shocks of continuous cyberattacks (LaRocca, 2014). However, when a threshold has been exceeded, the bottom state must identify the maximum degradation cost that CII suffers after failure (Fan et al., 2014).

In contrast, the equilibrium state assesses the CII alternatives that regenerate the performance to regain stability (Rose, 2019). These three states' relationship determines the cyber efficiency and cyber effectiveness for CII (Shalamanov, 2019). Thus, cyber efficiency is bounded between the threshold state and the bottom state, and cyber effectiveness is bounded between the bottom state and the equilibrium state (Kott & Linkov, 2019).

### **3.1.2 Novel Proposed Solution based on Cyber Zero-Trust Engineering**

Today, critical information infrastructures that mainly have the highest cybersecurity level are denoted as cyber trustworthiness (Severson et al., 2018). Nevertheless, even such a level has historically been proven inadequate by revealed sophisticated cyberattacks against susceptible targets worldwide (Bao et al., 2014). Perfect cyber trustworthiness is impossible because CIIs must have full resilient capabilities to resist various cyber risks (Kalala, 2017) robustly and continuously.

Cyber trustfulness is an abstract, subjective, and multifaceted concept crucial for CIIs to rely on resources and provide services (Dünner et al., 2018). An essential pillar and significant factor fundamentally describe a cyber-trustworthiness level (Zafar et al., 2017). Cyber trustfulness engineering refers to managing cyber trust in the CIIs environment, including defining cyber trust and identifying the hub nodes that establish cyber trust (Grachkov & Malyuk, 2020).

Furthermore, setting mechanisms for cyber trust computation, propagation, aggregation, storing cyber trust data, and provisioning cyber trust service enhancement to allow certain trust functionality to be implemented and supported using computing algorithms (Fan et al., 2020).

Upon that, cyber trustfulness engineering has a complicated and costly process that brings self-cyber risks to CIIs since relying on trust involves the necessity of a centralized node or nodes for cyber trust granting, which is considered single or multiple hub nodes that are easily targeted by

sophisticated cyberattacks and consequently lead to the cyber trust dilemma (Etzioni, 2019). This dilemma reduces the efficiency and effectiveness of cyber resilience capabilities (Stafford, 2020). Moreover, it has significant negative impacts on the heterogeneous coupling networks formed by interdependent CIIs collaborating to conduct cyber actions on each other's decentralized infrastructures to manage the shared resources and achieve the mutual objectives (Kolokotronis et al., 2019).

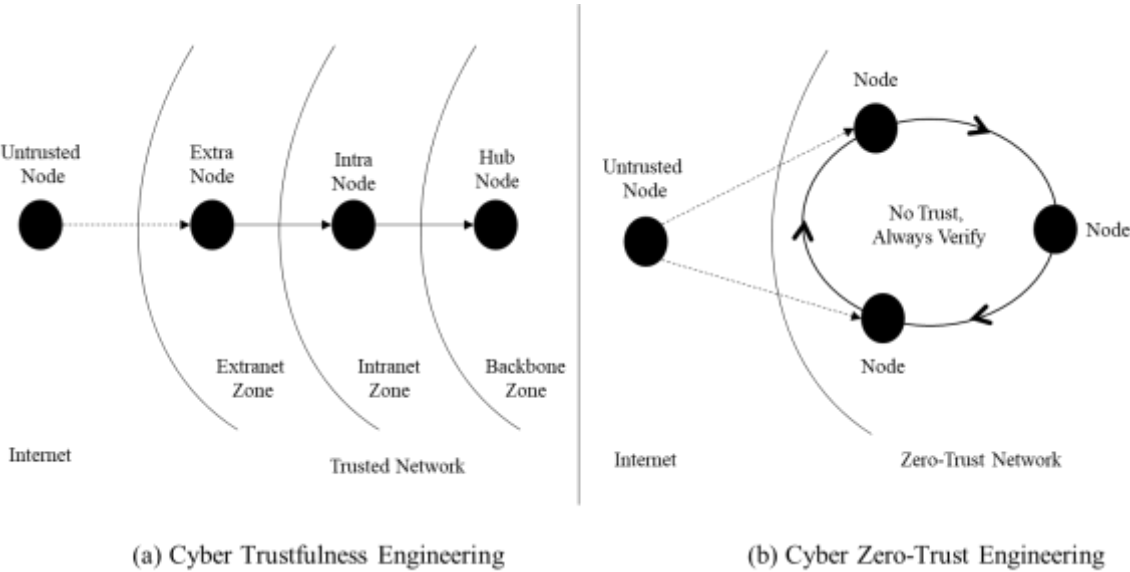


Figure 3.2: Cyber Trustfulness Engineering vs. Cyber Zero-Trust Engineering

In order to resolve the cyber trust dilemma in such a context, numerous algorithms and mechanisms are developed based on the trustfulness concept by the standard solutions for dynamic cyber resilience, including distance-vector, link-state, and path-rule solutions (Xie & Li, 2017).

However, these standard solutions have common limitations for cyber trustfulness discussed amply at the end of section 2.4.2 in this thesis and summarized thus the different compatibility of architectural couplings, the diverse adaptation of topology dynamics, the distinct convergence of



interdependency updates, and the various recovery of failure effects for decentralized CII (Yuan et al., 2017).

Therefore, the imperative demand is to provide a technology solution of dynamic cyber resilience to solve the cyber trust dilemma by revoking the need for centralized node existence to grant cyber trust where the peer hub nodes in scale-free CII networks can collaborate in cyberspace without trusting each other (Gilman & Barth, 2017).

This research proposed a novel technology solution adopting cyber zero-trust engineering at network layer-3 OSI model introduced by John Kindervag in 2010, the principal analyst for Forrester Research, to resolve the inherent cyber trust dilemma in CII networks and aim for meaningful perceived and actual cyber trustworthiness towards both data and functionalities (Rose et al., 2018).

The cyber zero-trust engineering assertions assume that the CII networks have fine-grained rules and dynamic technologies from as many functions and data flow sources as possible because the locality is not adequate for decisive cyber trustfulness (Kindervag, 2016). Besides, the CII environment is always hostile due to acknowledging internal and external cyber threats exist at all times, so never inherent trust for anything (Vanickis et al., 2018).

Cyber zero-trust engineering has been a common theme from a new perspective of cyber risk management (Stafford, 2020). It continues verification, monitors, and maintains logs of all network traffic for the workload, workforce, and workplace of the CII coupled networks (Boumhaout et al., 2018).

Moreover, this engineering manages a complete and active lack of trust in the entire lifecycle over cyberspace and cyber collaboration issues (Liu et al., 2016). It considers even the inherent cyber resilience constraints against offensive cyberattacks implemented by each involved

interdependent CII on the other side (Zaheer et al., 2019).

The novel proposed solution reconceptualizes the dynamic cyber resilience of interdependent CII networks because the nodes in the zero-trust network can interoperate among themselves without a centric hub node for cyber trust granting (Kolokotronis et al., 2019).

Whilst in the trusted network, the centralized hub node in the backbone zone grants cyber trust for untrusted nodes in other network zones (Kindervag, 2010). Moreover, as it usually happens, the cyberattacks are targeted the hub nodes in the trusted networks, causing the single hub node failure (Scott, 2018), as shown in Figure 3.2.

Cyber zero-trust engineering designed in the proposed solution requires all hub nodes' participation, as a one coupled group, to enable them to make cyber actions and share their goals using decentralized cyber consensus to determine conclusions (Zaheer et al., 2019).

In such coupling CII networks, no given node will be exceptional, and no single node separately or even cluster nodes can ensue cyber actions in isolation from the rest nodes (Eidle et al., 2017). As a result, any hub node can be up and removed anytime and anywhere in the entire network. Therefore, a single hub node vulnerability is handled (Kerman et al., 2020).

In the proposed solution, the participating hub nodes do not have to be trusted in any way precisely (Zimmer, 2018). Nevertheless, simultaneously, each hub node makes self-serving, cooperates honestly with all the other nodes to calculate hashes accurately, commits transactions, acts appropriately of the whole, and aligns correctly with the dynamic cyber resilience capabilities (Gilman & Barth, 2017).

Every such node is a vital part of coupling CII networks that establish and utilize cyber trustless resources and play a decisive role in determining cyber actions (Scott, 2018). The proposed solution demonstrates a technology stack consisting of several algorithms that have been built

with comprehensive concepts to enhance the capabilities of dynamic cyber resilience for interdependent critical infrastructures and coping with both the cyber trust dilemma and limitations of the standard solutions (Rose et al., 2019).

These concepts comprise decentralized registry, encrypted transmission, delegated peers, consensus rules, hubs coupling, end-to-end service quality, and dynamic routing that support scalable, resilient, and accessibility by each peer hub node within CII networks (Kerman et al., 2020).

### **3.2 Optimization of Proposed Solution**

The optimization phase in this research focuses on improving the primary proposed solution after evaluation to enhance the dynamic cyber resilience capabilities of interdependent CIIs. The new improvements foster the optimized proposed solution by advancing knowledge of the primary proposed solution's strengths and weaknesses. *See Appendix E: Primary Proposed Solution.*

It was, furthermore, redesigning the proposed solution's optimization alternatives and their relations to each other to become more efficient and effective. It also enables handling the potential escalating and cascading failures of concurrent and consecutive cyberattacks and increasing dynamic cyber resilience to excel the standard solutions.

#### **3.2.1 Optimized Conceptual Framework**

On the basis of the primary phase results of the proposed solution compared to standard solutions, the conceptual framework of the proposed solution was optimized by adding three new fundamental concepts to the primary conceptual framework.

Currently, the optimized conceptual framework of the proposed solution has seven fundamental integrated concepts, as shown in Figure 3.5. This framework and the improvements on the

optimized technology stack of the proposed solution were re-evaluated based on the iterative four-objective cycle in this research, which is described in section 1.4 within Chapter 1. The analysis and discussion of the optimized results of the proposed solution compared to standard solutions. *See Appendix F: Primary Results Analysis and Discussion.*

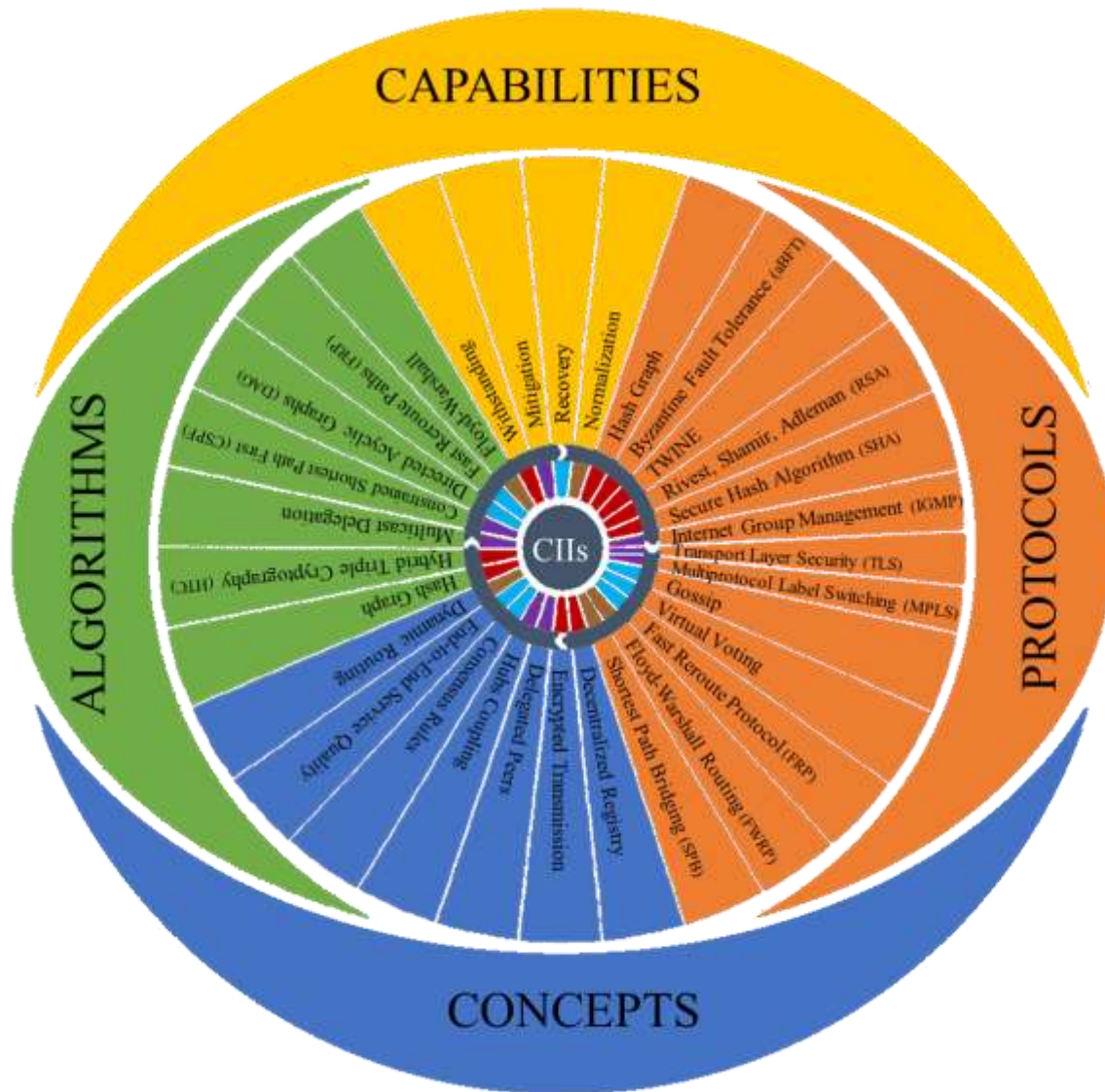


Figure 3.5: Optimized Conceptual Framework of Proposed Solution

The optimized conceptual framework in Figure 3.5 consists of three integrated circles; the outer

circle has four colored parts, the gold part represents the dynamic cyber resilience capabilities, the opposite blue part stands for the correlated optimized fundamental concepts. Likewise, the left green part demonstrates algorithms that support these capabilities and concepts, while the facing right orange part comprises protocols working with their associated algorithms together.

The middle circle presents the four gold slices; each slice shows the capability of dynamic cyber resilience. This color code is applied to the other slices in the middle circle, where the seven blue slices display the fundamental concepts of the primary conceptual framework, as well as the seven green slices that exhibit the cyber zero-trust algorithms. At last, the eight orange slices expose the protocols used in the technology stack of the proposed solution.

The inner circle also contains four colors with the core circle of CIIs: each color links every capability with its concept, algorithm, and protocols. Thus, for example, the red color slice of withstanding capability is linked with the concept of decentralized registry, hash graph algorithm, in addition to the protocols of the hash graph and byzantine fault tolerance (aBFT). In the same way, it applies to the rest colored slices in the inner circle. All details of the concepts, algorithms, and protocols for the primary conceptual framework have been elaborated in this section.

*1. The first fundamental concept in the optimized conceptual framework of the proposed solution is the decentralized registry.*

It manages the withstanding capability of dynamic cyber resilience. This concept enables a decentralized serial tables-based registry to determine what data records payload when transmitted, distributed, and routed over interdependent CII networks.

The decentralized registry contains the necessary entry information such as attached and remote network IDs, subnet mask, forwarded next-hop, outgoing interface, data payload, host routes, and default metrics matched with the origin and destination's best paths (El Ioini & Pahl, 2018). This

registry is maintained, updated, and guaranteed by coupled hub nodes dynamically using layer-3 consensus-based protocols to exchange records corresponding to cross the surrounding network topology (Galar, 2018).

The proposed solution's concept of a decentralized registry uses a Hash Graph algorithm. This algorithm is a decentralized data structure that maintains growing data tables, improving collaboration and operating escalation among the hub node peers (Luykx & Baird, 2020). Furthermore, it is secure, fast, fair of access, chronological ordering, and time stamping with high throughput (James et al., 2019).

Every hub node sends a signed newly created record and receives it from other peers by attaching an additional pair of hashes containing the last two hub nodes (Baird, 2016). The peers update the state changes applied to that record, build a new serial-table, aggregate the records into it, and then share the replication with others (Lasy, 2019). Further, each hub node determines if a new serial-table is valid or not based on all network hub nodes' consensus within the CII network guarantees resistance from cyberattacks (Hoxha, 2018).

The data is stored as an input in a serial-tables hash graph containing timestamped records signed by its hub node creators (Junfeng et al., 2020). This comprehensive process continues until all hub nodes view all serial-tables created or received initially and maintain hash graphs representing serial-tables sequences in the decentralized registry (Rauchs et al., 2018).

As a result, the coupled hub nodes must obey the statutes group to preserve this registry (Lasy, 2019). Any hub node can create signed records at any time repeatedly (James et al., 2019). All other hub nodes immediately have a complete and exact copy (Baird, 2016). Also, guarantee a timestamped consensus on those ordered records by multiple directed paths passing through enough connected hub nodes (Crary, 2020).

Moreover, if one hub node sent a record to another, the latter should create a serial-table, sign, and contain hashes of the prior and the upcoming serial-tables (Suciu et al., 2018). These two serial-tables are called the self-parent of the newly created serial-table (Lasy, 2019). On creation, the hub node puts its local time into the created serial-table as the timestamp (Green, 2019).

The decentralized registry contains any serial-table created by the hub node and timestamps used to track the validated records (Luykx & Baird, 2020). Thus, it is difficult for a cyber-attacker to unfairly influence the predefined accurate order of records chosen as the consensus; even trying to forge the timestamps, the hash graph algorithm detects it (Junfeng et al., 2020).

*2. The second fundamental concept that has been added to the optimized conceptual framework of the proposed solution is the encrypted transmission.*

It enhances the withstanding capability of dynamic cyber resilience, together with the concept of the decentralized registry. Furthermore, this improvement fosters the proposed solution's optimized results because it increases the coupled network robustness for reaction to cyber disturbances and resists cyber failures to sustain its stability.

Encryption is a complex process that employs mathematical formulas with cipher codes to secure, integrate, and authenticate the data (Giri et al., 2020). The central pillar of cryptography is based on the concept of a key. Therefore, there are three types of cryptography: symmetric, asymmetric, and hashing. Each has a wide range of algorithms used for many purposes (Kessler, 2016).

Symmetric cryptography uses one key to encrypt and decrypt data. As for asymmetric type needs two keys, a public key to encrypt data and a private one to decrypt it, while hashing uses no keys with one-way encryption and message digests (Smart, 2016).

As a rule, in cryptography, cyber protection increased whenever the crypto algorithm complexity

increased, resource consumption increased, network delay increased, and computational performance decreased (Dowling et al., 2020). Therefore, balancing is recommended between the encryption advantages to secure CII networks against the disadvantages of cyberattacks' potential costs and implementing cybersecurity measures (DhivyaShree & Sandhiya, 2016).

In this context, end-to-end encryption is the most secure data encryption process at the end hub node that operates independently of any other encryption processes used (Suzaki et al., 2011). Data is end-to-end encrypted only while transmitted, existing as non-encrypted on the sending and receiving hub nodes (Sinha et al., 2020).

End-to-end encryption is implemented through standards at the network layer-3 in the OSI reference model responsible for routing and connectivity between two end hub nodes (Suzaki et al., 2013). Besides, depending on each end over the communication path between the identified source and destination hub nodes without the detailed transmission medium (Koutsoukos & Sundaram, 2013). The proposed solution's encrypted transmission uses a Hybrid Triple Cryptographic (HTC) algorithm. It combines all three cryptography types to form a secure end-to-end transmission comprising optimized features for each type.

For example, symmetric cryptography is ideally appropriate for encrypting data providing confidentiality. The sender generates a session key to encrypt the data; the receiver needs it to decrypt it (Angelo, 2019).

Likewise, asymmetric cryptography theoretically is a key exchange application for non-repudiation; if the receiver obtains the public key encrypted with the sender's private key, only this sender could have sent it. Also, the private key values are computed faster than the public key values (Choras et al., 2015).

On the other hand, hashing cryptography is well-suited for data integrity to a high degree of



confidence; any change made to the data calculated different hashing values in the receiver than the one placed in the sender's transmission (Gamboa et al., 2020).

In the hybrid triple cryptographic algorithm, the sender uses the private key to encrypt the session key, randomly generating each session. The sender then encrypts the session key using the receiver's public key. The encrypted session key and encrypted data together form the encrypted record. Upon receipt, the receiver recovers the encrypted session key using the private key and then decrypts the encrypted data (Karabacak et al., 2016).

The encrypted record is formed in two stages. First, the sender computes the hash value of data; next, the sender encrypts the hashing values with the private key. Upon receiving the encrypted record, the receiver recovers the hashing values calculated by decrypting the encrypted record with the sender's public key (Smart, 2016).

The receiver applies the hashing function to the sender's original data, which the receiver has already decrypted. If the resultant hashing values are not the same as the sender's values, the receiver knows that the data has altered; if the hashing values are the same, the receiver believes that the data received is identical sender sent (Vasilyev et al., 2019).

The hashing cryptography provides non-repudiation since it proves that the sender sent the data; if the hashing values recovered by the receiver using the sender's public key proves that the data has not altered, the sender created the encrypted record. If the receiver correctly decrypts the data, it should have decrypted the session key correctly, meaning it has the correct private key. Thus, the receiver has proof that it is the intended receiver (Giri et al., 2020).

The session key is used once for a single session every time. Even if it is attacked, only one session is compromised. The session key is not constructed on the previous sessions' keys in the next session. The hybrid triple cryptographic algorithm supports the perfect forward secrecy;

losing one session key due to compromising prevents losing all of them (Kessler, 2016).

*3. The third fundamental concept in the optimized conceptual framework of the proposed solution is the delegated peers.*

It manages the mitigation capability of dynamic cyber resilience. This concept enhanced hub nodes' redundant layout to deal with the expected cyber structural failures and serve route requests on short paths in the overlay CII networks to establish a new functional local routing quickly. Delegated peers commonly select multiple neighboring hub nodes and mutually open redundant cyber connections via the underlying CII networks. The additional low-cost links save information proactively on replication neighbor peers for fallback. The delegated peers for the replica are somewhat deliberate and not explicitly chosen. Even after some delegated peers have cyber failed, functions are replicated, and data is stored redundantly on different hub node peers, leading to higher response retrieving the breakdown of CII services.

The proposed solution's delegated peers use a Multicast Delegation algorithm. It guarantees the cooperative process of distributed problem-solving consistency by using a decentralized collection of network sources located in different processor hub nodes (Afanador et al., 2020).

Moreover, it controls the task decomposition to keep the delegated peers from conducting subtasks twice or executing errors in a particular sequence of interactions through the synchronization mechanism (Tsikin & Melikhova, 2016).

The multicast delegation algorithm also enables a set of delegated peers to harmonic cooperate in decentralized CII networks through three roles: determination, delegation, and execution (Wang et al., 2011). However, Hub node peers can carry out these roles in the scale-free CII coupling network depending on the nodal reliability and topology complexity (Dibaji & Ishii, 2015).

In detail, a delegation set can contain any number of coupled heterogeneous peers. The cohesive

relationship among them is neither as strong as a team nor as weak as a crowd (Godán et al., 2016). All initial route requests of delegation communication that are received are passed to the delegation set in the coupling CII network. The peers negotiate the three possible roles (Wang et al., 2010).

Firstly, the determination role governs hub node peers' capabilities to ensure having adequate resources and concrete capabilities like processing speed, connection bandwidth, scalable coordination, storage pace, and localized views to handle the given tasks as potential contractors. Simultaneously, it verifies that the preconditions to route requests are satisfied (Wu et al., 2011).

Secondly, the delegation role decomposes the route requests into subtasks, generates tactics covering slots for actions, coordinates the corresponding cooperation efficiently to and from reliable hub node peers in the same set, and ensures proper task execution. This role requires a high synchronization to avoid having some peers implement the identical subtasks that others had not implemented yet (Afanador et al., 2019).

Lastly, the execution role eventually performs the analogous subtask process after contracted to particular hub node peers with associated constraints or delegates other peers' recursively to execute the rest of subtasks until completing the entire initial task to prevent possibly taking a longer execution time for the whole task (Tsikin & Melikhova, 2016).

*4. The fourth fundamental concept that has been added to the optimized conceptual framework of the proposed solution is the hubs coupling.*

It enhances the mitigation capability of dynamic cyber resilience, together with the concept of delegated peers. This improvement boosts the optimized results of the proposed solution because of maintaining regular redundancy among hub nodes and providing a replica of their core functions in CII networks to cut down the undesired effects after cyber failures occurred

(Koutsoukos & Sundaram, 2013).

This concept reduces the structural fractions of coupled nodes between heterogeneous CII under different cyberattacks, increases support-interdependency multiple relations, suppresses numerous levels of synchronization amongst hub nodes that appeared in scale-free networks, and expands the resistance to the cyber fragility of the single hub node failure in the presence of cyber interdependency (Pereira, 2010).

The concept of the hubs coupling in the proposed solution uses a Constrained Shortest Path First (CSPF) algorithm. It runs after the violation of a given set of constraints such as end-to-end delay, hops limitations, specified minimal bandwidth guaranteed that required per cyber link, the maximal number of inter-links crossed the CII network whether it include or exclude coupled hub nodes; in order to resolve dynamic routing queries by discovering the best route among hub nodes (Kalpana & Tyagi, 2017).

The CSPF algorithm keeps a local copy of constraint-based traffic information in the serial-table within the decentralized registry to generate a multicast routing architecture for each query. This local copy stores two types of information: the shortest path tree and tentative hub nodes (Lozano & Medaglia, 2013). Configurable caching of full source routes minimizes the calculation time for inter-links redundancy, switching protection, fast restoration, and high availability across hub nodes' failures (Shi et al., 2017).

In detail, the constrained shortest path first algorithm collects the attributes information of the inter-links to connect each hub node, then floods this information to other hub nodes and combines each one to each inter-link respectively. Thus, forming the topology structure of the whole coupled network and calculating constrained paths to protect it (Masood et al., 2018).

There are three policies for path first selection: random, total, and least remaining bandwidth rate.

The random selection rule places an equal number of each inter-link; one of the remaining paths is selected, nevertheless of the available bandwidth rate (Kempf et al., 2011). The entire selection rule fills an inter-link before choosing the alternative inter-links; the lowest minimum bandwidth rate available is preferred. In the end, the minor selection rule equalizes the reservation on each inter-link; the most considerable minimum bandwidth rate available is desired (Olszewski, 2012). The CSPF algorithm processes begin at the login hub node with bandwidth rate parameters to reach the final destination. First, it checks the hub node for maximal hop counts metric starting with configured constraints; skip the verification if the end hub node is already visited. If not, check the inter-link for static, re-servable, or available bandwidth metrics (Sapundzhi & Popstoilov, 2018).

The traffic data contained in the serial-table have to be the same across all coupled hub nodes. The inter-link is removed from the serial-table when it fails to meet the bandwidth constraints; if it passes, select the inter-link with the nearest hub node's shortest path, hop to the next inter-link, and repeat these steps for all hub nodes. In the case of none shortest path found, then indicate retry after a particular interval. (Pramudita et al., 2019).

*5. The fifth fundamental concept in the optimized conceptual framework of the proposed solution is the consensus rules.*

It manages the recovery capability of dynamic cyber resilience. This concept is a suite of rules that consider an essential pillar in cyber zero-trust engineering to characterize the cyber functions of heterogeneous hub nodes and govern their proper functioning in the coupled network. This suite is a decision-making process for the set of hub nodes, where it constructs cyber works and sustains the cyber actions that best for the rest of them. It is a form of resolution where coupled hub nodes need to support the majority of better outputs that benefit them all and solve data

synchronization, which has a higher difficulty value to win for the decentralized CII network.

The consensus rules describe the necessary conditions required for hub nodes' collaboration, do not trust each other to reach a specific consensus, and define the reliable operations between them that should be performed under a single fault caused by cyberattacks.

As a method to decide within a set of coupled hub nodes, the consensus rules depend on certain principles, including (1) Agreement: the rules gather all the set's agreements as much as they can to accomplish a collective agreement. (2) Cooperation: every hub node aims toward a better agreement that results in the set's interest as a whole, and every one of them works as a team and put its interest aside. (3) Participation: every hub node's participation is essential and has the same value. No hub node is left out or stays out without participation. (4) Responsibility: every hub node inside the network is equally active, and no one with more responsibility in the coupled network.

The concept of consensus rules in the proposed solution uses a Directed Acyclic Graphs (DAG) algorithm. A seamless graph shows that data structuring, storing, and compressing get processed topologically through side-sequence from earlier to later to find the best navigation route (Herrmann et al., 2019).

In general, all records resemble a flow chart where all hub nodes are explicitly headed in one direction to conduct autonomously on parallelized records to reduce the time and cost of creating, hashing, and validating decentralized registry across the CII network (Benčić & Žarko, 2018).

Moreover, the DAG algorithm bundles the new record of information to the older record graph into an established registry sequentially with immutable and chronological order to validate the record by record according to the previously validated records (Herrmann et al., 2019). Also, replicating and keeping up to date with the records added over all the hub nodes simultaneously

makes the entire coupled network safer, faster, scalable, and more robust (Webster-Clark & Breskin, 2020).

Furthermore, it is acyclic, i.e., the cyber attacker's chance to find the hub node is zero as it is a reverse tree-like, not a loop of coupled nodes, branching out from one to another so on (Crary, 2020). As a final point, it stands for a shared registry for registered records and significantly tracks any record stored in the decentralized registry (Gissibl & Klüppelberg, 2018).

The directed acyclic graphs algorithm works in-depth; every hub node has multiple records layers. When a record is registered in the hub node, it first needs to verify two other records before its record has been verified. Those two records were chosen upon the DAG algorithm (Benčić & Žarko, 2018). Besides, the hub node has to check if the two records are not conflicting and benefit decrease unnecessary verification (Bhattacharya et al., 2020).

*6. The sixth fundamental concept that has been added to the optimized conceptual framework of the proposed solution is end-to-end service quality.*

It enhances dynamic cyber resilience's recovery and normalization capabilities, together with consensus rules and dynamic routing concepts. This improvement leverages the proposed solution's optimized results because it handles resource reservation to different data flows between connected hub nodes, and controls functionality requirements, and provides traffic prioritization to guarantee an overall performance level for the coupled network.

End-to-end service quality is an overall quantitative description to control optimal performance levels among heterogeneous CII networks, especially after cyber failures. Several quality aspects of CII services are essential typically, such as the actual traffic rate or throughput metric and end-to-end delay or latency metric (Qiu et al., 2019).

The concept of end-to-end service quality in the proposed solution uses a Fast Reroute Paths

(FRP) algorithm. It aims to reduce the CII network traffic loss for local protection while hub nodes converge after a scale-free topology change against single hub node failure or link failure within the shared risk link group (O’Kelly, 2015).

In order to keep CII services running despite failure, rapid single failure repair is accomplished using safe loop-free alternates through precalculated backup next-hops of label-switched path tunnels. In addition, the loop-free alternates maintain recovery paths in the decentralized registry to reduce the recovery time (Jarry, 2013).

The FRP algorithm creates a one-to-one backup detour at each potential point of local repair and bypass tunnel to protect a potential failure point (Pereira, 2010). This local repair of tunnels differs from traditional schemes of dedicated path protection where network traffic is rerouted near a single failure point that speeds up the process to resend the lost network traffic (Papán et al., 2018).

The local network traffic detours, with a recovery path from the last reachable hub node with a failed link along the destination hub node’s original path until the decentralized CII network’s convergence process is completed without requiring support from other hub nodes coupled network. Consequently, the protection delay is crucial for the CII network; otherwise, it suffers from a vital recovery latency (Seppänen et al., 2018).

The event of a single failure is more extensive than alternates intended to repair, the looping traffic redirection onto backup tunnels that have the same constraints of end-to-end service quality as original paths (Herrera & Maennel, 2019). Therefore, these constraints used for the backup paths along data is rerouted typically involve the end-to-end service quality in the FRP algorithm (Qiu et al., 2019).



7. *The seventh and last fundamental concept in the optimized conceptual framework of the proposed solution is dynamic routing.*

It manages the normalization capability of dynamic cyber resilience. This concept is a networking approach that provides optimal data routing in CII networks and enables hub nodes to select routes logically according to the real-time network topology changes. Besides, it allows scalability since the cyber routes do not have to be configured manually, and there is less administrative overhead and error-prone involved than static routing.

Dynamic routing is considered an essential pillar in any technology solution for dynamic cyber resilience, in other concepts interact together based on it. The concept of dynamic routing in the proposed solution uses Floyd-Warshall's algorithm. It allows hub nodes to share information about the CII networks with other nodes to select the best routes to reach a destination (Triana & Syahputri, 2018).

Floyd-Warshall's algorithm generates a series of matrices by successfully counting new hub nodes that give each node pair the truly shortest route (Arai, 2020). Consequently, it computes as inputs all-pairs shortest routes in a directed weighted network upon time frequently for all pairs of hub nodes that exist on the CII network, not just the shortest route from a particular single source of hub node (Kumar & Reddy, 2020).

Floyd-Warshall's algorithm initiates by discovering all the minimal distances between hub nodes' pairs without passing across intermediate nodes (Djojo & Karyono, 2013).

The minimum values of distances are registered in the decentralized registry. Comparisons with the previous values determine the minimal distances between hub nodes' pairs (Kulkarni et al., 2015).

Any change in the scale-free topology of CII networks dynamically updates the decentralized

registry with new minimum distance values. The first hub node does these sequence steps up to the last hub node (Ajila & Chang, 2017); Floyd-Warshall's algorithm process is repeated using the previous values for comparisons and calculate the weights of the positive and negative links to avoid negative route cycles (Swathika & Hemamalini, 2017).

Moreover, Floyd-Warshall's algorithm is a dynamic programming variant for solving an optimization problem. The algorithmic technique breaks the routing problem down into routing sub-problems (Mirino, 2017). The shortest route solution is generated as an interconnected decision formed from the route sub-solutions to its route sub-problems. It depends on the fact that the overall route problem can be more than one optimal route solution (Singh & Mishra, 2014).

### **3.2.2 Heuristic Improvements of Proposed Solution**

In light of advances in the heuristic optimization method that its formulation procedure is executed iteratively investigates each alternative proposed solution's feasibility depending on the problem statement until an optimal one will be found. After that, the evaluated results of each one are compared, and the better is adopted (Bradley et al., 2015).

Usually, there is a tradeoff between unconstrained effective functionality maxima and afforded efficient resources minima; thus, a robust, flexible, and optimal solution emerges. Nevertheless, such a problem-specific becomes intractable and cannot be solved (Chowdhury et al., 2020).

The heuristic improvements aim to reach an optimum or near-optimum proposed solution and provide optimized results compared with standard solutions of dynamic cyber resilience for CII networks. This method has been implemented as a powerful instrument applied in designing experiments, analyzing the collected data, performing interactive tasks, and processing the optimization choices to handle the research purpose step-by-step, guaranteeing that an optimal proposed solution is developed (Martí & Reinelt, 2011).

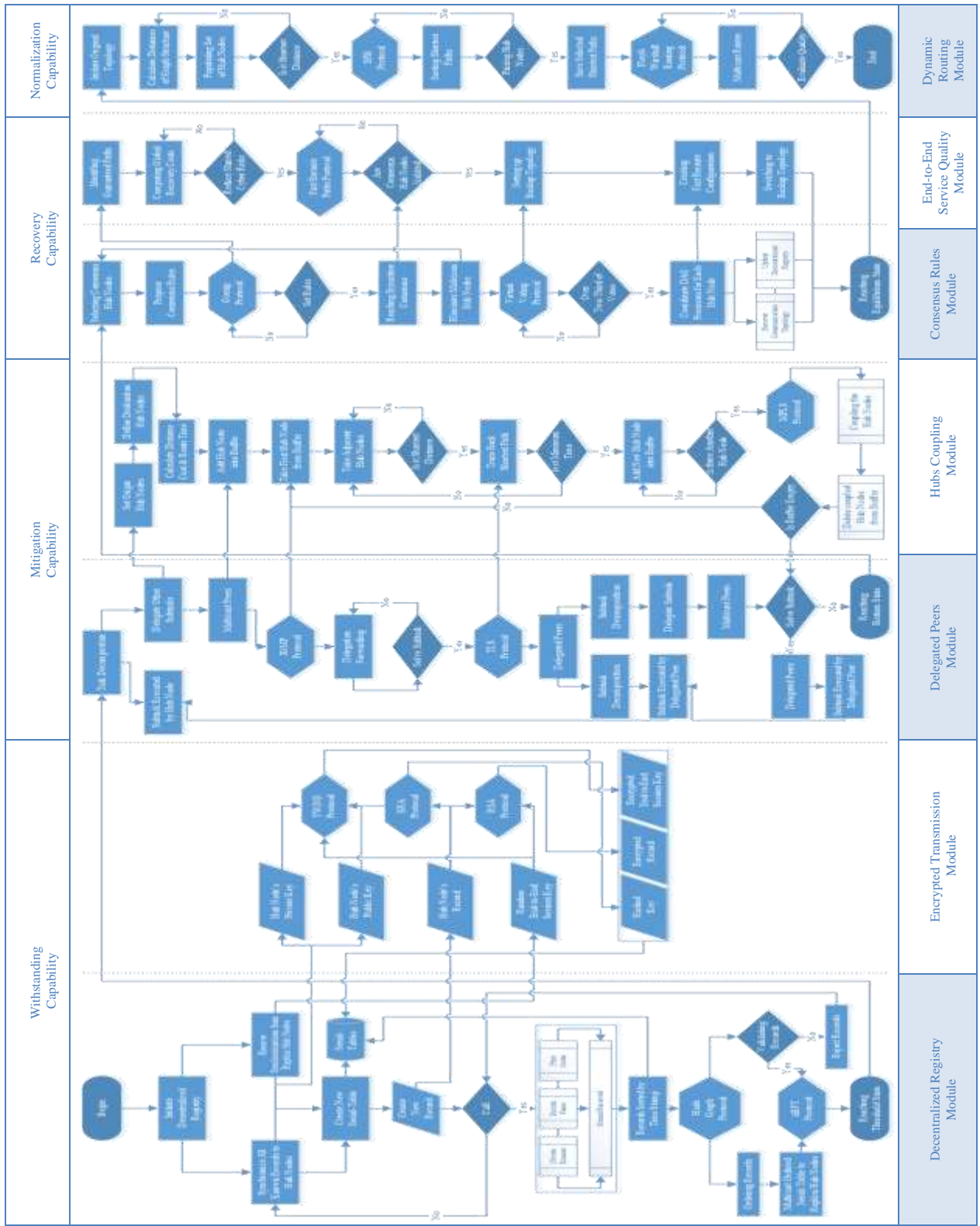


Figure 3.6: Flowchart Diagram of Technology stack for Optimized Proposed Solution

The improvements scheme is harmony combined based on the theoretical requirements indicated in the literature and the empirical observations obtained from the primary quantitative results and analyzed during the primary evaluation phase in this research (Davendralingam & DeLaurentis, 2013).

As shown in Figure 3.6, the optimized technology stack has a set of three modules integrated precisely with highlighted four modules implemented in the primary technology stack on top of each other. Each module combines one algorithm and a collection of correlated protocols based on cyber zero-trust engineering in line with the relevant fundamental concepts of the optimized conceptual framework.

- 1. The first module in the optimized technology stack is the decentralized registry module that includes the hash graph algorithm presented in section 3.2.1 and the Hashgraph protocol and asynchronous Byzantine Fault Tolerance (aBFT) protocol.*

The hashgraph protocol is the central part of the hash graph algorithm to manage the decentralized registry's information. The information contained by the serial-tables is mostly a validated data storage of the records made in a given time with the timestamp, in addition to both regular parent hashes of the latest table and the previous one (Luykx & Baird, 2020).

That means all hub nodes in the hashgraph protocol can create new records into the decentralized registry that are potentially scaled; other hub nodes have to confirm, counting the entire coupled network in this process almost in real-time (Hoxha, 2018).

As a result, the hashgraph protocol is able to build secure and fast cyber zero-trust functionality and resistance to cyberattacks in the CIIs environment (Gilman & Barth, 2017). Additionally, it provides a high bandwidth usage efficiency, handles multi-thousands records, and verifies over a hundred serial-tables with measured time in seconds (Green, 2019).

The data flow diagram of the hashgraph protocol establishes multiple lines and circles by the interactions among all interconnected hub nodes within the coupled network (Schueffel, 2017). Each hub node has its circles representing records when it exchanges information with neighboring hub nodes. Whenever such connections occur, hub nodes mark their records and link them with the serial-table's preceding record (James et al., 2017).

Thus, the decentralized registry represents a complete and consistent history of how the hub nodes in the coupled network sent and received information to each other and guaranteed paths for records spread and reconstructed the whole hashgraph locally if cyberattacks proceeded (Green, 2019). Moreover, it prevents malicious nodes like DDoS botnets that are trying to block transited records shared between the hub nodes or flood the CII networks with fabricated records (Wang, 2019).

The other protocol in this module is an asynchronous Byzantine Fault Tolerance (aBFT) protocol. It allows the limited number of hub nodes to order the valid messages to the total ordering and convey the data independently without exchanging the finalized records to be delayed or lost altogether (Baird, 2016).

The hub nodes perform computations over asynchronous communications on the basis of the local copy of the decentralized registry for increased security against DDoS cyberattacks, high scalability, and latency with entirely trustless. As such, the aBFT protocol is resistant to a single hub node of failure (Gałol & Świętek, 2018).

If it is the first generated record of any hub node, it is termed a root record. The root record must be connected to the older ones and be known by at least two-thirds of other hub nodes (Lamport et al., 2019). In addition, any record contains at least the record history, timestamp, signature, and hash references (Micali, 2018).

Similarly, the serial-table stores the partial records' order from the next record to another root record based on timestamp for topological ordering (Baird, 2016). At long last, the total ordering values of records are computed locally regarding the number of connections from a record to other root records (Lamport et al., 2019).

The hub nodes exchange information by creating root records at a specific time and resharing copies of the referenced records' information to their peers (Micali, 2018). The hashes of the owner hub node sign these records with its peers (Gałol & Świętek, 2018). The aBFT protocol sets the rules via a cost function that governs the communication between hub nodes and determines that *one* selects others to broadcast (Baird, 2016).

*2. The second module is the encrypted transmission module that incorporates the hybrid triple cryptographic algorithm displayed in section 3.3.1 aforementioned and integrated three protocols: TWINE protocol, RSA protocol, and SHA protocol.*

Firstly, the TWINE protocol is the symmetric cryptography method with one key only used for encryption and decryption processes based on a lightweight block cipher length of 128-bit keys that are easy to implement and compatible with high-speed communications (Minematsu et al., 2011). Furthermore, this block cipher comprises procedures that restate parallel processing as the round functions (Suzaki et al., 2013).

TWINE block cipher tested successfully regarding cybersecurity level with the compressed implementation of combined encryption and decryption (Angelo, 2019). It creates numerous subblocks cipher compact with a decentralized characteristic leading to several encryption rounds, considering a significant improvement using the original cyclic shift (Smart, 2016).

As an independent encryption protocol developed by Nippon Electric Company (NEC) Corp in 2012, TWINE has many concrete design settings and updated encrypted keys with low memory

consumption and well-balanced performance against high consecutive and different cyberattacks that fully exploit the vital schedule of the encrypted keys (Schaub et al., 2016).

The second cryptographic protocol is RSA; this acronym comes from the initial letters of its developers Rivest, Shamir, and Adleman. The most widely asymmetric cryptography method used two distinct cryptographic keys to secure data transmission, the public key for encryption and the private one for decryption without exchanging a secret key separately (Giri et al., 2020).

RSA has 2048-bit keys typically long phased out by 2013 with variable size of the encrypted keys and small cipher blocks on the basis of the fact that factorize the problem of the immense size integers is a practical difficulty. Therefore, the encryption strength increases exponentially (Smart, 2016).

Simultaneously, the public encrypted keys contain two numbers; one is produced and published by multiplying large primary numbers and an additional value (Vasilyev et al., 2019). On the other hand, the private encrypted key is derived from the same dual large primary numbers throughout a dissimilar process and kept secret (Kessler, 2016). Thus, data is encrypted by any hub node via the public encrypted key but only decrypted by the hub node, which knows the primary numbers (AlHamdani, 2020).

The ideal example of the RSA protocol process involves the hub nodes over the coupled network that can distribute their public encrypted keys, and any hub node wishes to send the other hub node data to encrypt their data using these public keys. The sender hub node requests data from another hub node by sending its public key (Angelo, 2019).

The receiver hub node verifies and encrypts the requested data using the sender's public key and sends the encrypted data again. Lastly, the sender hub node receives and decrypts the data (Zakwan, 2015). Since the RSA protocol is asymmetric, no hub node except the sender hub node

can decrypt this data even if another hub node has the public key in the coupled network (Francia et al., 2018).

The third cryptographic protocol is the Secure Hash Algorithm (SHA), developed by the National Institute of Standards and Technology (NIST) at the end of 2013 (Giri et al., 2020). The SHA protocol produced hash keys based upon mathematical hashing functions with output size 512-bit cipher block length to secure data exchange pathways or store serial-tables of records (Kizza, 2020).

The hash keys are generated using complex calculations to turn a massive amount of data into a minimum representation with maintaining the data integrity verification in all sorting ways (Johnson, 2015). Furthermore, these keys are irreversible, i.e., once the data record is converted into the hash value, it is impossible to transform it back into the original one. Besides, it is unique that two distinct data records never generate identical hash keys (Rose et al., 2019).

The SHA hashing is not encryption since it is designed to be a one-way cryptographic function and fast to compute with twofold processes, compression, and modular additions (Sinha et al., 2020). These processes produce fixed-size records for any source record size different wholly from the original data records; a little bit of input change causes a significant hashing output change like the original length of the data record (Vasilyev et al., 2019).

The SHA protocol maintains data records secured against cyberattacks by detecting data tampering and providing robust characteristics, including pre-image, second pre-image, and collision resistance through the implicit record conversion to 512-bit cipher block by a hashing function (Kessler, 2016).

This complicated conversion calculates the required number of blocks, creates a 16-bit integer, takes four bytes from the data record for each of these integers, and left-shifts them within the



512-bit array proper quantity return into the 32-bit integer. The length in bits of the data record has to be attached in the last two integers of the final block of the last 64-bit integer (Suzaki et al., 2013).

3. *The third module in the optimized technology stack is the delegated peers' module that comprises the multicast delegation algorithm introduced in section 3.2.1, formerly and Internet Group Management Protocol (IGMP) and Transport Layer Security (TLS) protocol.*

The internet group management protocol plays a vital role in managing the dynamic multicast transmissions within integrated groups (Zakwan, 2015). The layer-3 dynamic multicasting allows incoming data streams to be transmitted to multiple hub nodes and handled by listening for joining and leaving periodic messages from the source hub node to a selected destination group of hub nodes (Chen & Atwood, 2018). Moreover, it permits the addition of hub nodes, removes them from the multicast group of the coupled network, and dynamically forwards the communication traffic to the group members only (Sargent et al., 2017).

The sending hub node initiates a one-to-many transmission sends a membership message to inform adjacent peers to join the multicast group (Liu et al., 2010). IGMPv3 creates a multicast group address and forwards it to multicast peers. The peering hub nodes are being added to the multicast group. All peers who wished to be group members of the coupled network send a joint message (Yonghui & Hu, 2012).

IGMPv3 continues sending membership queries to keep appropriate membership information updated. All hub nodes that want to remain in the group of the coupled network have to reply to these queries (Liu et al., 2010). If the group member does not reply to the inclusion request within a specified time, the IGMPv3 removes it from the group. Once all group members have left the entire coupled network, the multicast group address is removed (Yonghui & Hu, 2012).

The internet group management protocol has flexible transport and optimum routing capacities with optimized performance (Zakwan, 2015). Also, it is automatically implemented on all peers that support multicasting connections and operate efficiently to ensure selectable multicast source-specific information, besides securing transmissions since unknown peering sources cannot transmit the fabricated data (Sargent et al., 2017).

Without using IGMPv3 practically, each hub node sends a separate data stream to every receiving peer in the coupled network (Yonghui & Hu, 2012). This case has bandwidth consumed totally as all connected paths are occupied, leading to an overload quickly and difficulty with the CII services permanently available (Chen & Atwood, 2018).

The other protocol in this module is Transport Layer Security (TLS) protocol. It is well-designed to facilitate data integrity and end-to-end communications over CII networks, among other mechanisms, to detect data forgery, avoid eavesdropping, stop tampering, and improve mitigation performance capacities (Rescorla & Dierks, 2018).

The TLS protocol latest version 1.3, defined in 2018, is more helpful in performing reliable connections and preventing undetected data loss or checking message integrity during transmission between hub nodes through a well-defined TLS handshake sequence and examining the data records (Tschofenig et al., 2019).

The TLS handshake is carried out when a set of the hub nodes in the coupled network leverage attempt to connect, each hub node verifies that the other peers support TLS protocol (Turner, 2014). Then, all test the multidirectional connections using cryptographic parameters and negotiate in parallel by sending messages to each other (Dowling et al., 2020).

Once TLS handshaking has successfully proceeded, the peers decide to execute the procedure and use the established channels to exchange data records. Every time, the handshake process has

been followed based on the same mandatory steps (Polese et al., 2019). Otherwise, the TLS protocol launched triggers of error failure, preceded by alert messages for connections' termination (Tschofenig et al., 2019).

4. *The fourth module in the optimized technology stack is the hubs coupling module that consists of the constrained shortest path first algorithm proffered in section 3.3.1 above and one protocol called Multiprotocol Label Switching (MPLS).*

This layer-3 protocol-independent is a connection-oriented technique that establishes a virtual private network with highly efficient routes to underlying any technology contents over the intermediate hub nodes to its destinations in the coupled network (Masood et al., 2018).

The architectural key in MPLS protocol is the labels that provide additional short bit sequences more than the hub nodes before regular had (Olszewski, 2012). It tags the network traffic with predetermined identifier labels to distinguish the label-switched paths based on the specific criteria for setting the network traffic forwarding priorities (Kempf et al., 2011).

These paths are unidirectional, where the sent and received network traffic are transmitted via different paths. Each label contains four subparts: label value, experimental value, the bottom of the stack, and time to live. These parts hold all information for the hub nodes to decide where the network traffic is forwarded (Liu et al., 2016).

The hub nodes use the labels as indices into a serial-table to assign the same label-switched paths to forward the network traffic and attach it with a new label to the next hop (Tian et al., 2015). This operation is repetitive with the hub node at each hop until the original network traffic reaches the final destination (Li et al., 2015).

A different label is used for each hop, and all labels are comprised of an MPLS header. The hub nodes consistently handle the MPLS header with particular characteristics as long as they

examine the MPLS labels attached and direct the straightforward routes to the given label-switched paths chosen (O’Kelly, 2015). The hub nodes typically perform one or more of three examination actions on the labels. First, push to add a label. Swap to replace a label. Pop to remove a label (Pereira, 2010).

The MPLS protocol keeps connections genuinely intimate and scalable, reduces congestion, and recovers performance by mapping the real-time network traffic to low-latency hub nodes (Olszewski, 2012). Moreover, MPLS protocol is considered a secure and flexible transport mode with bandwidth utilization; therefore, it is not vulnerable to DDoS cyberattacks, although it does not provide encryption to the network traffic (Masood et al., 2018).

5. *The fifth module in the optimized technology stack is the consensus rules module containing the directed acyclic graphs algorithm represented earlier in section 3.2.1, Gossip protocol, and the Virtual Voting protocol.*

The gossip protocol is a decentralized process that uses vital and class peer-to-peer communications to propagate new data records periodically, rapidly, and ultimately to all group peers within dynamic, heterogeneous, and large-scale CII networks (Kalala, 2017). The gossip protocol’s core includes the bounded scope pairwise, regular aggregate, and fixed size of information exchanged during inter-process interactions between hub node peers, reflecting the state of changes to building a global map of the coupled network (Choi et al., 2020).

However, each hub node has to store this complete map and maintain its periodic updates consistently amongst the peers’ extensive group (Tetarave et al., 2015). The regularity of the local interactions is low than potential data records latency, so the gossip protocol has negligible costs and reliable communications (Ishii & Dibaji, 2017).

The gossip protocol spreads information continuously by multicast flooding the participating hub

nodes in the coupled network-wide until the data records are delivered (Tetarave et al., 2015). Upon that, each hub node identifies the blacklist of malicious peers in its view. Thus, each hub node's gossip with all-to-all peers is considered non-malicious only (Wang et al., 2020).

The gossip protocol lets each hub node know every data record transmitted over the coupled network. Besides that, the other protocol in this module is the Virtual Voting protocol. It ensures that all hub nodes agree on a linear order of the serial-table records depending on multiple rounds of pure voting messages sent across the peers to reach an overall consensus (Choi et al., 2020).

The hub nodes calculate each other peers' votes by locally looking at every one of their copies of the serial-table and applying internal votes calculations as a function of the previous records of the given record (Zhai & Wang, 2019). Thus, it guarantees that peers in the coupled network continuously calculate their votes concurring with the consensus rules (Dibaji & Ishii, 2015).

The virtual voting protocol process consists of three main steps: rounds division, fame decision, and order found (DhivyaShree & Sandhiya, 2016). The first step begins the virtual voting process by defining voting rounds and observers. Then, in the serial-table, the first record for a hub node is that hub node's first observer, launching the first round for that hub node (Wang et al., 2020).

All following records are the first round portion until a fresh observer is found when a hub node generates a new record that has to be able to recognize an obvious two-third of the recent round observers. Each record is added to the serial-table and assigned around (Zhai & Wang, 2019).

The second step is fame deciding whether an observer is well-known or not based on other observers' recognition if they can recognize it or cannot in the next round. If they recognize it, they calculate the vote to decide the observer's fame (Tetarave et al., 2015). Likewise, if other observers in the next round cannot recognize it, they vote and decide that the future observer is not considered famous (Li et al., 2015).

Later calculating the votes for all the observers around to be famous or not, the virtual voting protocol has proceeded as the third step to find the order (Benčić & Žarko, 2018). To conclude, it determines the records' order before the famous observer records by calculating the number of rounds and timestamp signature (Herrmann et al., 2019).

The number of rounds calculated for all records is still to be ordered after all famous observers' fame has been decided (Webster-Clark & Breskin, 2020). Later, the consensus timestamp is calculated using the ordered median of gathered records for the regular round's famous observers and signed. The hub nodes then analyzed and shared the serial-table to govern the consensus timestamp for all records (Bhattacharya et al., 2020).

6. *The sixth module in the optimized technology stack is the end-to-end service quality module encloses the fast-reroute paths algorithm described in previous section 3.3.1 with Fast Reroute Paths (FRP) protocol.*

The FRP protocol requires alternate routes with high throughput at each hub node to handle common cause, escalating, or cascading cyber failures when consecutive and concurrent cyberattacks are detected, leading to the functions delay and data records loss (Riaz et al., 2018).

Hence, it is fast since the network traffic immediately shifted to precalculated alternative paths next-hops are picked from the points-of-failures without discovering new paths or hop counts (Qiu et al., 2109). It has a minimum end-to-end convergence time delay because prime and alternate routes are the shortest. Also, recover the possible affected functions and normalize the performance of the CII services (Papán et al., 2018).

The FRP protocol is lightweight that computes and establishes prime and alternate topological paths before data records have been transferred on each hub node to avoid control overhead (Jarry, 2013). It finds at least one most suitable alternate route headed between every source hub

node and the destination one on the prime path through a definite intermediate hub node that is informed firstly (Bao et al., 2014).

The fast reroute paths protocol worked in a whole disjoint manner when the cyber failure occurred at any position every time on the prime route (Papán et al., 2018). In such a situation, the hub node detects the cyber failure ahead, shifting the network traffic to an alternate hub node and informing the cyber failure source (Riaz et al., 2018).

The prime and alternate routes have different hub nodes between the points-of-failures and the destinations with the need for elaboration tradeoffs (Jarry, 2013). The number of recoveries depends on the number of alternate routes. Therefore, it is reactive to coping with cyber failures and designed for mission CII (Qiu et al., 2019).

*7. The seventh and last module in the optimized technology stack is the dynamic routing module with the Floyd-Warshall algorithm shown in section 3.2.1 and Floyd-Warshall Routing Protocol (FWRP) Shortest Path Bridging (SPB) protocol.*

The Floyd-Warshall Routing protocol allows a maximum throughput and improves service quality, involving the required time of transmitting and retransmitting records from any hub node to the target one across the shortest paths in the coupled network (Azhar & Haroon, 2019).

The Floyd-Warshall routing protocol directly enhances the processing capacity of the hub nodes related to the transmitted time and the records queue length (Triana & Syahputri, 2018). The determined shortest path minimizes the required time for passing through them. It finds that the optimal routing between these peers depends on the combination of path communication capacity and hub node processing capacity (Swathika & Hemamalini, 2017).

That is, it is improving the weighted average based on the considered distance and the normalized load (Kumar & Reddy, 2020). Additionally, it is a value obtained to optimize the throughput and

service quality within Floyd-Warshall routing protocol and efficiently utilize all-pairs shortest paths computations by the other protocol in this module, Shortest Path Bridging (SPB) protocol (Azhar & Haroon, 2019).

The 802.1aq SPB protocol enables multiple active equal-cost paths, supports faster convergence and reconvergence times upon hub node failure, provides logical coupling with the head end (Pramudita et al., 2019). In addition, it transits layer-3 multicasting replication, simplifies networking configuration and segmentation, blocks redundant paths to prevent looping, and allows traffic load shares across all paths over the coupled network (Ashwood-Smith, 2010).

The shortest path bridging protocol also leverages routing activation and enhances dynamically adjusted topology changes between hub nodes. The SPB network traffic continually proceeds the most efficient shortest paths from the source hub nodes to the destination ones, guaranteeing failover and optimal performance (Nakayama & Oota, 2013). It is highly scalable and secure zones, extremely flexible, and comfortable troubleshooting supports virtualization, lowers costs, and deploys faster (Sapundzhi & Popstoilov, 2018).

The SPB protocol activates the encapsulation process, adding an identifier label to the traffic route forwarded to the destination across the selected paths among candidates with the exact cost (Kulkarni et al., 2015). Thus, the coupled network with SPB protocol looks like one hub for connected hub nodes that periodically share, store, and update the exact information of the global topology view within the decentralized registry (Swathika & Hemamalini, 2017).

The hub nodes configure themselves to carry traffic routes on the efficient path between each hub node to minimize convergence time after the given topology changes caused by cyberattacks significantly when recovery from the bottom state to equilibrium state moving toward the normalization of the CII functions and services (Sitti, 2015).



## **CHAPTER 4. DESIGN AND METHODOLOGY**

The research design and methodology build on the theoretical and empirical perspectives to assemble a set of selected methods, tools, and techniques appropriate to investigate and examine the capabilities of dynamic cyber resilience for the proposed solution compared with standard solutions in the environment of interdependent critical information infrastructures under concurrent and consecutive cyberattacks (Graubart & Bodeau, 2016).

As established earlier, it is a blueprint that reflects the ability of the thesis for accessing and gathering the primary data under observation, testing the hypotheses, and answering the questions in a way that is most likely to achieve the intended goal and objectives articulated in this Chapter through three sections include research design, research methodology, and research implementation (Bochkov et al., 2015).

In general, the first section of the research design includes the in-depth representation of the research roadmap that helps quest for a solution to the research problem, overview the structured evaluation metrics used to measure and reach the valid results; and develop the different scenarios with highlighted the operationalization procedures to provide trustworthiness when results are discussed (Yusta et al., 2011).

Moreover, the second section described the processes of the data collection like computing simulation, organized the levels of data analysis via analytical modeling in attempts to produce useful information and ensure that it is well-handled to meet the needs of the study, and outlined the practical tools of data validation such as emulated experiments (Deng et al., 2017).

Furthermore, it identified potential methodological choices, adopted various quantitative methods to conduct the study, and introduced the technical instrumentation constructed and utilized to

pursue the research objectives (Shevchuk, 2019). *See Appendix D: Research Methodological Choices.*

## **4.1 Research Design**

A research design is a strategic work plan for a study, employed as a guide based on the research rationale and motivation for collecting, validating, and analyzing the primary data (Cai et al., 2018). Therefore, it is crucial to identify the research purpose for establishing a suitable research design that is pursued (Shevchenko et al., 2018). Appropriate methods can be selected after a systematic investigation that caters to specific research objectives (Das et al., 2020).

This section describes all aspects of the three subsections that focus mainly on the selected methodological choices, the designated quantitative methods, and the detailed research roadmap to enrich the developmental research understanding and dynamic transitional process for the proposed solution (Seppänen et al., 2018).

### **4.1.1 Research Roadmap**

The roadmap is not an evidence-building plan only for bridging the research gaps. It is also essential for helping the research achieve its purpose and develop a technology solution optimized enough to enhance the dynamic cyber resilience of critical information infrastructures (Anne et al., 2018).

As illustrated in Figure 4.3, the roadmap explains that this research has started with a research work plan, identifies the sequential milestones, aligns with the primary and secondary data, and drives the general work plan's daily operations guided by the research questions. It consists of three essential parts, inputs, processes, and outputs (Divakaran et al., 2017).

The first part of the roadmap is the research inputs that comprise the problem statement, research

purpose, and literature review (Bergström et al., 2015). Next, it is conducted to understand the research gaps and envisions the next steps to construct a conceptual framework needed later and make a technology stack based on the secondary data (Dünner et al., 2018).

The research questions and hypotheses have arisen from the research work plan, where the formed conceptual framework fused into a prototype novel proposed solution and enriches the secondary data (Abdin et al., 2019). The result is developing the proposed solution and pinpointing the standard dynamic cyber resilience solutions (Labaka et al., 2017).

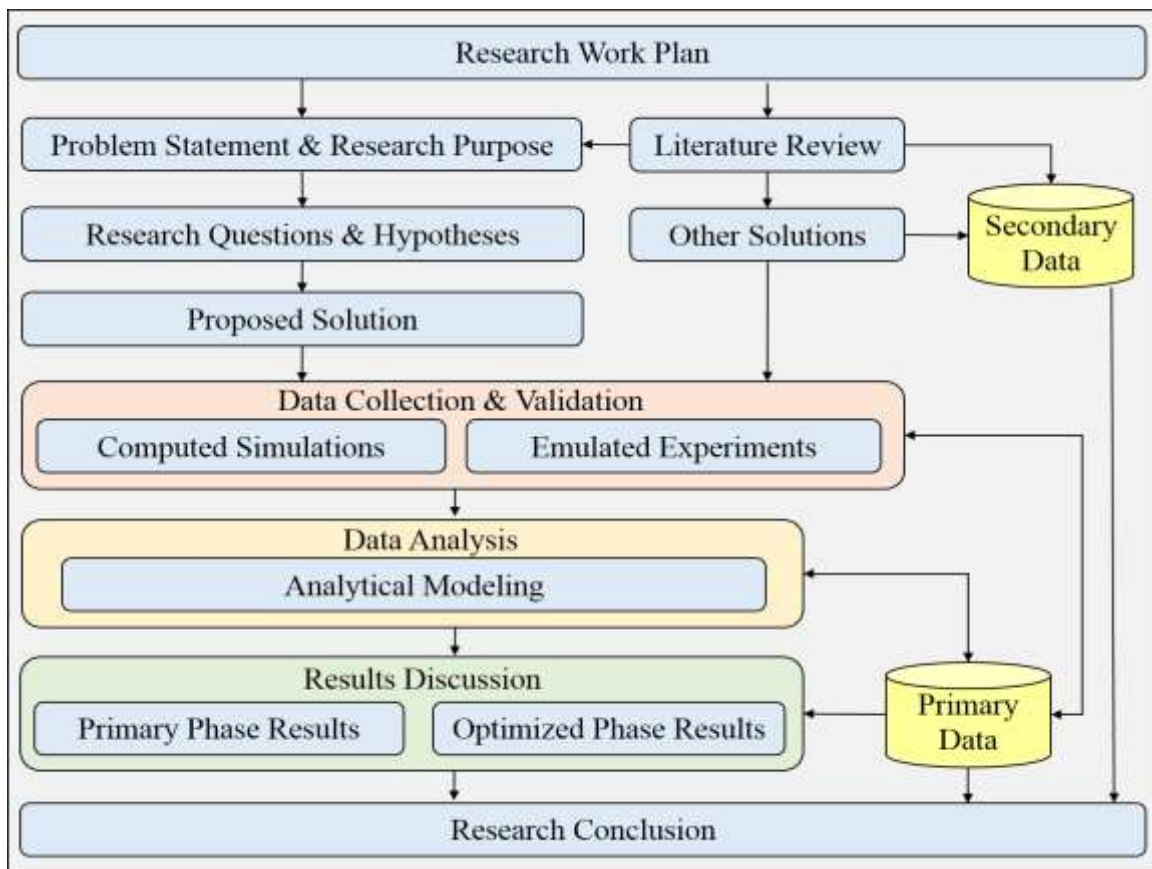


Figure 4.3: The Research Roadmap

Close readings of published research documents, related papers and books, performance diagrams, and reports of standard solutions of dynamic cyber resilience, and notes written by the researchers are valuable sources in this research for secondary quantitative data Caverzan &

Solomos, 2014).

The second part of the roadmap is the research process. It involves empirical data collection and validation using quantitative methods based on structured computing simulations and emulated experiments (Zafar et al., 2017). Then, the data analysis process through the analytical modeling method. In conclusion, these processes and methods create in exchangeable ways the primary data of this study is directed to the results (Moyer et al., 2016).

In this research, two phases of the plan were conducted to refine the data collection, validation, and analysis to develop related links between research questions and conceptual framework with formative clarification for the research design (Dsouza et al., 2013). In addition, the primary and optimized phases are a laboratory for detailing the proposed solution, allowing different scenarios for diverse experiments to observe raw outputs on a trial basis (Vasilyev et al., 2019).

These phases' scope covers methodological and substantive issues with a broader focus on the ultimate plan of final data collection and analysis (Haque et al., 2019). Additionally, this information is used for the ongoing literature review in parallel with the final research design to ensure that the actual results are significantly reflected in the conceptual framework (Ullah et al., 2018).

The third part of the roadmap is the research outputs, which entail the thesis's primary and optimized phases (Abdel-Razeq et al., 2018). The results have been discussed, the final findings interpreted, and the conclusion meets the hypotheses, answers the questions, and achieves the research goal and objectives (Nezamodini et al., 2017).

For further elaboration, a systematic review of the theoretical and empirical literature gathers the requirements and analyzes the potential cyberattacks for interdependent CII networks (Banescu et al., 2011). Besides, build the conceptual framework of the proposed solution for dynamic cyber

resilience (Labaka et al., 2016). As well, develop cyber zero-trust algorithms and protocols within the network layer-3 of OSI model through the conceptual framework and technology stack by using C++ object-based editor and network protocol software (Pitt-Francis & Whiteley, 2017). Moreover, define the quantitative metrics for dynamic cyber resilience capabilities evaluation (Linkov et al., 2013). Then, conduct several scenarios for the proposed solution using computing simulations and emulated experiments (Yamin et al., 2020).

The results' reporting is explicitly the essential source of lessons learned for research design and fieldwork procedures (Klein & Klein, 2019). In addition, these reports become robust prototyping for the final proposed solution (Grachkov & Malyuk, 2020).

Besides, analyzing the data through analytical modeling and comparing the proposed solution's results with standard solutions to optimize the proposed solution by improvements (Setola & Theocharidou, 2016). Finally, interpret the findings by representing the conclusion and recommendations for future works (Lade & Peterson, 2019).

#### **4.1.2 Evaluation Metrics**

Generally, the evaluation metrics are essential for any quantitative research to measure the algorithms or models' quality, efficiency, or effectiveness as a proposed solution (Linkov et al., 2013). In addition, using evaluation metrics is critical in ensuring that the proposed solution operates correctly and optimally by comparing predicted results with actual results (Bhuyan et al., 2015).

It is essential to understand the evaluation metric's definition to ensure it is aligned with the proposed solution's prediction goal. If the proposed solution improves prediction, the yield has a higher metric score (Nan et al., 2014). The improvements return the proposed solution metrics with the highest score. Sometimes, it is called a loss function in literature, where the goal is to

minimize the loss function (Mitra et al., 2010).

It is imperative to use multiple evaluation metrics to evaluate the proposed solution because the proposed solution may perform well using one measurement from one evaluation metric but may perform poorly using another measurement from another evaluation metric (Bodeau & Graubart, 2016). Likewise, they choose the wrong metric for evaluation, likely to choose a weak proposed solution, or in the worst case, be misled about the expected quality, efficiency, or effectiveness (Marais & Uday, 2015).

Choosing an appropriate metric is challenging because most of standard metrics that are widely used assume a balanced quality distribution; therefore, not all prediction errors are equal for imbalanced, and for this, there are many different types of evaluation metrics available for testing the proposed solution involves using a combination of these individual types (Haque et al., 2018).

In the context of the understanding of time-dependent evaluation for dynamic cyber resilience based on its capabilities such as recovery speed of coupled CII networks; i.e., a more resilient CII network can recover faster from a cyber failure than the others (Cai et al., 2018).

In addition to recoverability, dynamic cyber resilience quantified according to other capabilities includes withstanding, mitigation, and normalization (Francis & Bekera, 2014). These four capabilities enabled the description of dynamic cyber resilience in terms of the proportions of cybersecurity efficiency and cyber continuity effectiveness of the interdependent CII networks (Laderman et al., 2015).

In this research, the choosing of the evaluation metrics on the basis of the quantification ability that available to measure the capabilities of the single dynamic cyber resilience and the total dynamic cyber resilience for the interdependent critical information infrastructures against concurrent and consecutive cyberattacks using the proposed solution compared with the standard

solutions (Fotouhi et al., 2017).

Therefore, Tran (2015) introduced the metric  $R$  to measure the dynamic cyber resilience developed from the requirements set for a method to assess the established capabilities of dynamic cyber resilience (see section 2.4.3). This metric is based on the integration metric proposed by Vugrin et al. (2010) and the resilience factor proposed by Francis and Bekera (2013). The integration metric provides a quantitative method of capturing the total cyber resilience maintained by coupled CII networks throughout different cyber failure scenarios like the following:

$$R = \begin{cases} \sigma\rho[\delta + \zeta + 1 - \tau^{(\rho-\delta)}] & \text{if } \rho - \delta \geq 0 \\ \sigma\rho(\delta + \zeta) & \text{otherwise,} \end{cases}$$

Where  $0 \leq R \leq \infty$ ,

- $R$  Single Dynamic Cyber Resilience.
- $\sigma$  Performance Factor.
- $\rho$  Recovery Factor.
- $\delta$  Absorption Factor.
- $\zeta$  Volatility Factor.
- $\tau$  Recovery Time Factor.

$$R_{total} = \sum_{i=1}^N w_i R_i$$

Where  $0 \leq R_{total} \leq \infty$ ,

- $R_{total}$  Total Dynamic Cyber Resilience.
- $w_i$  Normalization Coefficient.
- $R_i$  Single Cyber Resilience for each Cyber Failure.
- $N$  Total number of Cyber Failures.

Similar to other cyber resilience metrics in the literature, the  $R$  and  $R_{total}$  are the metrics calculated based on the integration of five factors that modeled mathematically to evaluate the dynamic cyber resilience for interdependent CII networks under single or multiple cyber failures caused by the cyberattacks using analytical modeling platform (Patrman et al., 2019).

Integration-based cyber resilience is modified by incorporating a suite of dynamic cyber resilience factors to account for various capabilities of dynamic cyber resilience explicitly. In other words, the capabilities of dynamic cyber resilience for interdependent CII networks are evaluated by the factors of dynamic cyber resilience, which are demonstrated in the above mathematical models (Rehak et al., 2018).

The withstanding capability is evaluated by the absorption factor,  $\delta$ , which accounts for the ability of the CII to absorb robustly the effects of cyberattacks to avoid reaching the threshold state (Yin et al., 2018). Likewise, the mitigation capability is evaluated by the volatility factor  $\zeta$ , which accounts for the ability of the CII to transit smoothly after failure from the bottom state to another (Burla et al., 2016). The recovery capability is evaluated by the recovery factor,  $\rho$ , which accounts for the ability of the CII to return to the equilibrium state (Liu et al., 2016).

Finally, the normalization capability is evaluated by performance factor,  $\sigma$ , and recovery time factor,  $\tau$ . The performance factor accounts for the total performance level maintained by CII throughout the cyber failure period and after reaching the equilibrium state (Han et al., 2016). The normalized recovery time factor accounts for the CII response's temporal aspects by calculating the time required to reach an equilibrium state following a cyber failure (Brown et al., 2010).

The influence of the recovery time factor decreases as the recovered performance factor decreases. Therefore, the conditional statement in the above equation of  $R$  ensures that CII are



only rewarded for quickly reaching equilibrium state if they recover performance level is better than their minimum performance (Patrman et al., 2019).

So as to evaluate the capabilities of dynamic cyber resilience, it should measure its related factors of dynamic cyber resilience using the Tran (2015) mathematical model. The dynamic cyber resilience factors were measured throughout the computing simulations and emulation experiments (Nistor et al., 2019).

Table 4.1: Matching among Capabilities and Factors of Dynamic Cyber Resilience that Measured by Standard Simulation and Emulation Networking Metrics

<i>Dynamic Cyber Resilience Capabilities</i>	<i>Dynamic Cyber Resilience Factors</i>	<i>Standard Simulation Networking Metrics</i>	<i>Standard Emulation Networking Metrics</i>
Withstanding	Absorption	Network Traffic Dropped	Network Traffic Lost
Mitigation	Volatility	Average Delay Variation	Average End-to-End Delay
Recovery	Recovery	Average Response Time	Average Reachable Time
Normalization	Performance	Throughput	Throughput
	Recovery Time	Average Convergence Duration	Average Convergence Duration

Upon that, there are many standard networking metrics available in the literature that can be measured based on the capacity of the simulation and emulation software packages (Uday, 2015).

Table 4.1 shows the matching among dynamic cyber resilience capabilities and factors measured effectively by the standard simulation and emulation networking metrics (Pedroni et al., 2016).

In the computing simulation, assessing the standard networking metrics to measure the cyber resilience factors are as the follows: (1) Network traffic dropped: the number of data units lost over the coupling network throughout the failure; this metric measures the absorption factor (Ottenburger et al., 2020). (2) Average delay variation: the average time gap when data sent from the selected hub node to another received the replying data through failure and recovery period; this metric measures the volatility factor (Parshani et al., 2010). (3) Average response time: the

average time between the end of the cyber request and the response starts during a failure within the coupling network; this metric measures the recovery factor (Scala et al., 2016). As well, (4) Throughput: the amount of data units successfully transmitted from the hub node to another over the coupling network in the failure period; this metric measures the performance factor (Teodorescu & Pickl, 2016). (5) Average convergence duration: the average time the coupling network needs to detect and recover from a cyber-attack; this metric measures the recovery time factor (Tian et al., 2015).

On the other hand, assessing of the standard networking metrics in emulation experiments include the following: (1) Network traffic lost: the number of data units traveling across a coupling network that fails to reach the hub node destination; this metric measures the absorption factor (Wu et al., 2018). (2) Average end-to-end delay: the average time taken for a unit of data to be transmitted across a coupling network via the only path in one direction from the hub node source to the destination; this metric measures the volatility factor (Vespignani, 2010).

Additionally, (3) Average reachable time: the average time after a hub node assumes that a neighbor node is unreachable after the hub node had received the initial reachability confirmation; this metric measures the recovery factor (Yuan et al., 2016). (4) Throughput: the amount of data units successfully transmitted from the hub node to another over the coupling network in the failure period; this metric measures the performance factor (Abdel-Razeq et al., 2018). (5) Average convergence duration: the average time the coupling network needs to detect and recover from a cyber-attack; this metric measures the recovery time factor (Zhu & Chen, 2020).

### 4.1.3 Scenarios Operationalization

The scenario operationalization focused on the adaptable and importable scenario-based design of specific research procedures that produce the empirical observations and represent the experimental results (Bhuyan et al., 2015). There are essential components to operationalize scenarios.

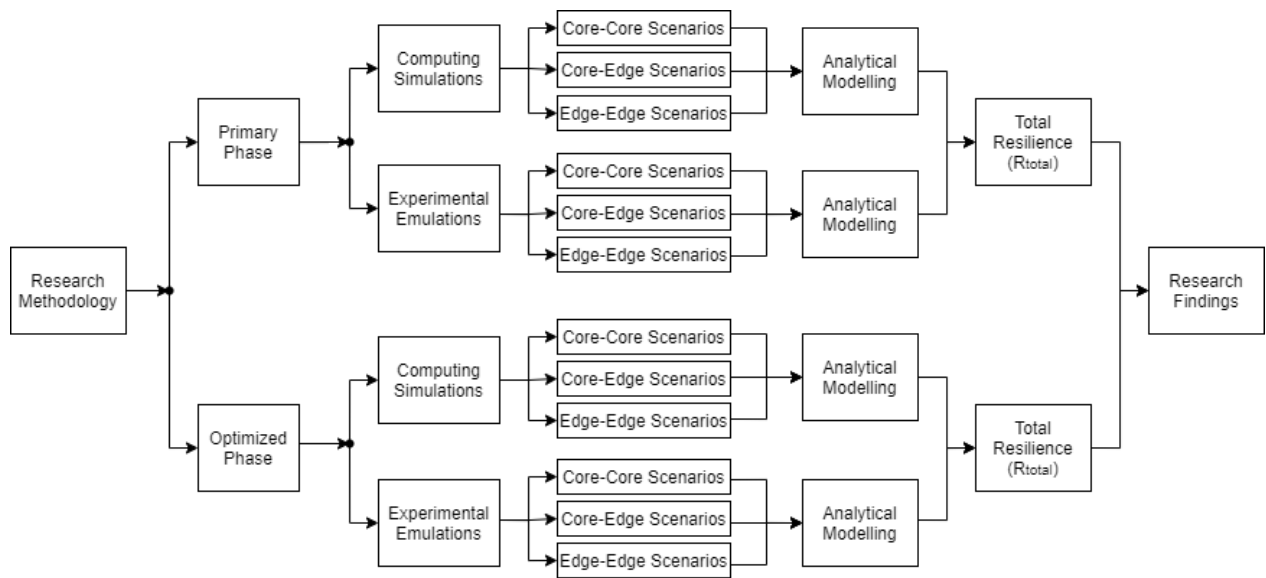


Figure 4.9: Diagram of General Scheme of Research Scenarios Operationalization

It considers seven components consisting of the following: (1) Define the showcase of interdependent CII networks through their vulnerabilities and interdependency reactions (Danziger et al., 2016). (2) Identify the cyber threat actors by their probability and frequency (Conti et al., 2018). (3) Specify the technology solution's features of dynamic cyber resilience (Brtis et al., 2013). (4) Describe the quantitative methods for collecting data during the testing scenarios (Marais & Uday, 2015). (5) Stipulate the sources of data generation for simulations and emulations (Sharif & Sadeghi-Niaraki, 2017). (6) Operate the testing scenarios to evaluate the cyber resiliency capabilities of the coupled CII networks (Wicks et al., 2018). (7) Analyze the

consequences of cyber failure on the cyber environment (Golnari & Zhang, 2015) as shown in Figure 4.9.

Firstly, the showcase of interdependent CII networks snapshotted in this research from the imaginary cyber-infrastructure map of Dubai city in the United Arab Emirates built on the governmental portals' open data and registers (dubaipulse.gov.ae) and (bayanat.ae) for the public (Sarwat et al., 2018). Figure 4.10 shows the four rectangle slices of the selected critical information infrastructure networks. Each rectangle slice in the graphical diagram demonstrates one critical information infrastructure network (Tatar, 2020).

There are four critical information infrastructure networks, two core networks, and two edge networks; the two core networks are the telecom and power infrastructures; however, the two edge networks are the finance and energy infrastructures (Zeadally & Alcaraz, 2015).

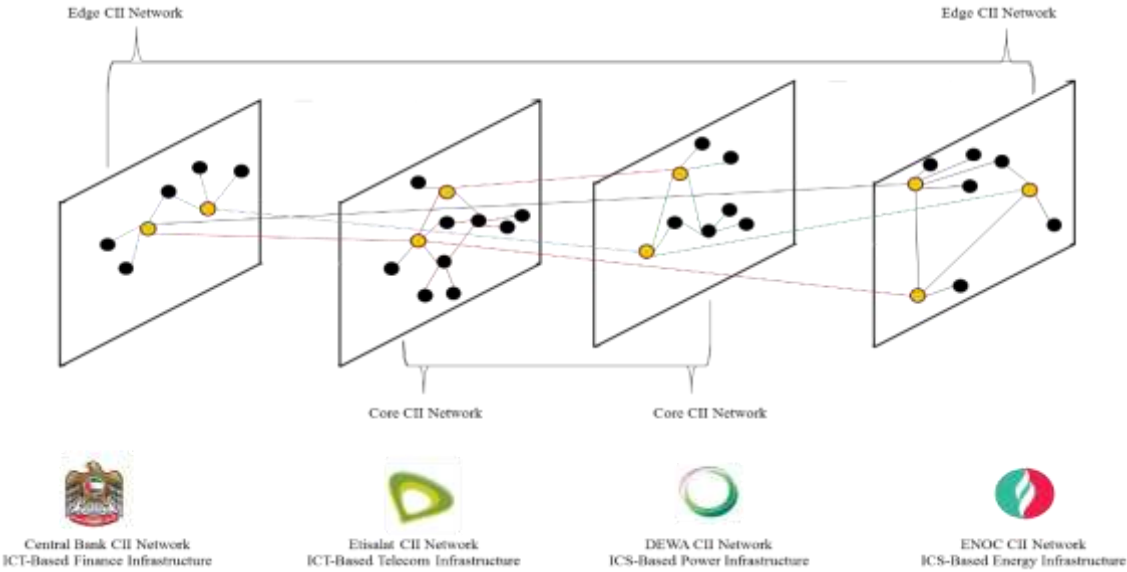


Figure 4.10: Diagram of Core CII Networks and Edge CII Networks

Typically, the fundamental difference between the core network and edge network in the interdependent cyber networks is the high level of reliability and scalability of the core network,

granting the edge networks inter-peering exchanges and redundant links with other interdependent critical information infrastructure networks (Kalala, 2017).

The Emirates Telecommunications Corporation (Etisalat) is the ICT-based telecom infrastructure, Dubai Electricity and Water Authority (DEWA) is the ICS-based power infrastructure, The Central Bank branch in Dubai is the ICT-based finance infrastructure, and Emirates National Oil Company (ENOC) is the ICS-based energy infrastructure. The differences between ICS-based and ICT-based networks are covered totally in section 2.3.1 of Chapter 2.

These interdependent CII networks tested locally in this research are considered a well-representative sample of globally interdependent CII networks. As a smart city, Dubai has advanced interdependent critical information infrastructures and adopts acceptable practices to provide smart services in this area (Sarwat et al., 2018).

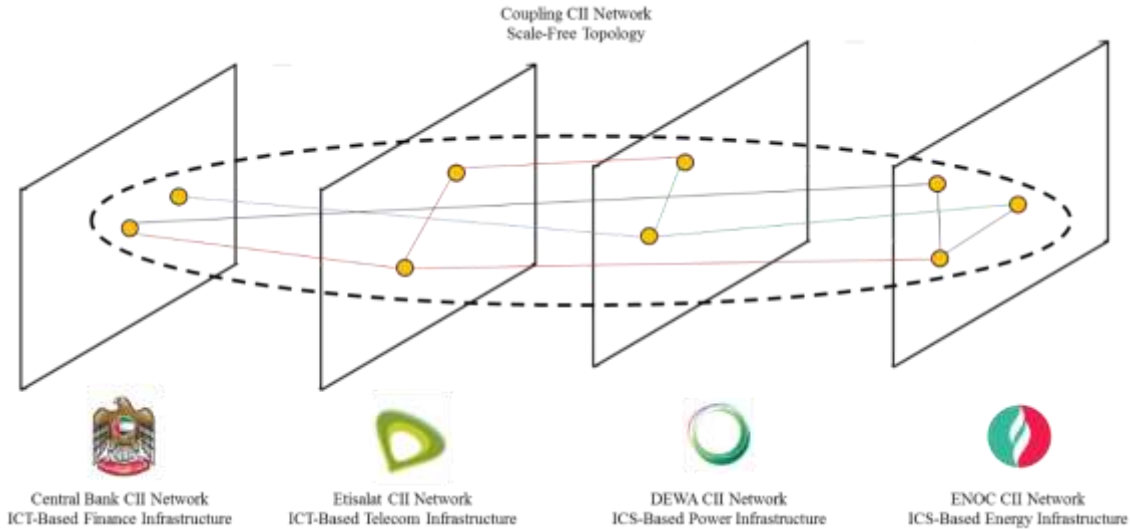


Figure 4.11: Diagram of Coupling CII Network Scale-Free Topology

Furthermore, the total nodes in the four CII networks are 35 nodes as depicted in Figure 4.10; nine goldy nodes of them considered as the hub nodes that formed coupling network and connected the entire CII networks with each other and have the highest-degree inter-links in all

these CII networks (Golnari & Zhang, 2015).

The coupling network's scale-free topology is formed by interdependent connections of the four critical information infrastructure networks that consist of two core CII networks and two edge CII networks (Buldyrev et al., 2012). The real-world hub nodes are critical connection points in cyber networks such as routers, switches, firewalls, and server farms that provide critical functions to the information infrastructure networks (O'Kelly, 2015), as illustrated in the graphical Figure 4.11.

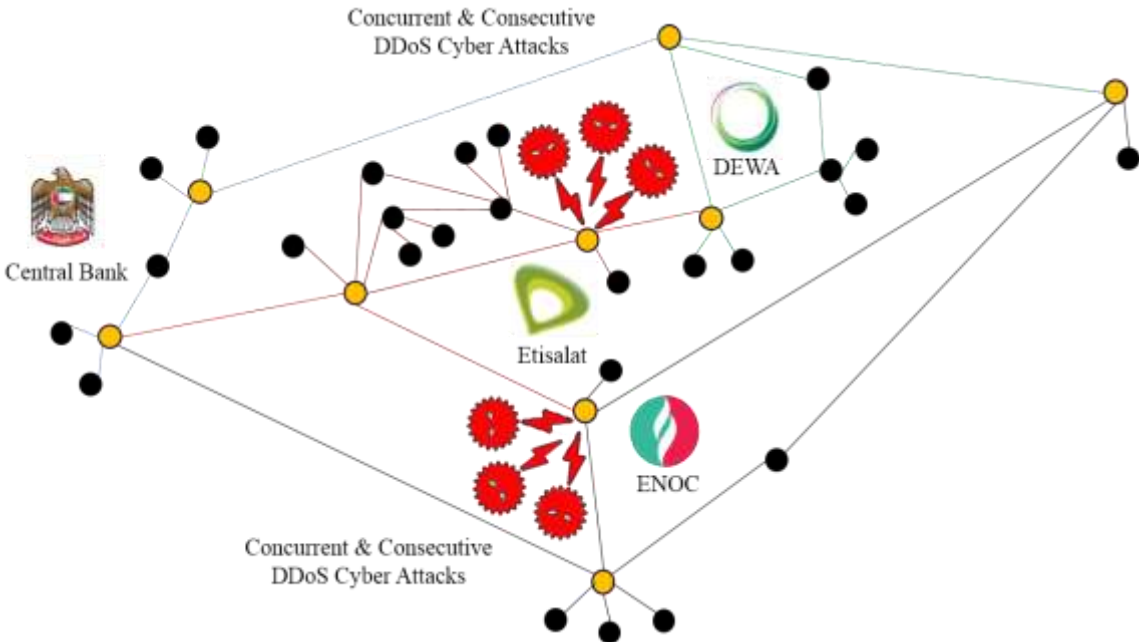


Figure 4.12: Diagram of Concurrent and Consecutive DDoS Cyberattacks against CII

Secondly, three concurrent and consecutive cyberattacks have been implemented using Petri-Nets cyber threat modeling during the testing scenarios (McCollum et al., 2018). These cyberattacks have been launched by the Distributed Denial-of-Service (DDoS) based on the STRIDE model described in detail in section 2.3.3 of Chapter 2.

DDoS cyber-attacks are achieved effectively by utilizing multiple agents like botnets as sources

of cyberattack traffic towards targeted hub nodes in CII networks (Mosharraf et al., 2015). The term the botnet combines two words, robot and network. DDoS botnets are designed to accomplish malicious tasks, including sending spam, stealing data, or ransomware (Wang, 2019). The botnets generate multiple packets towards the targeted hub nodes by overwhelming them with a flood of requests, thereby overloading the resources and surrounding CIIs, disrupting the regular traffic of their services (Georgiev & Nikolova, 2017).

There are several reasons to use DDoS in this research, including the nature of the decentralized architecture of interdependency hub nodes, easy to apply on the small and large scale of the CII networks, target the function and data in the scope of infrastructures and services with a common cause and escalating failures. Besides, it is the most well-studied type of cyberattack (Behal & Kumar, 2016).

In Figure 4.12, a DDoS malicious agent floods two goldy hub nodes, specifically of the CII networks, at a time in the scenario through protocol exploitation, resulting in bandwidth saturation that renders the service unavailable (Bhuyan et al., 2015). Two goldy hub nodes have been selected in each testing scenario in the computing simulations and emulated experiments.

The network traffic is exploited through DDoS cyber-attacks in targeted CII networks, logically connected to other heterogeneous CII networks as a one-coupled network (Wright et al., 2016). Therefore, these cyberattack scenarios are simulated and emulated, considering the coupled CII network of the Dubai map.

Thirdly, in addition to the proposed solution, prototyped and optimized in-depth in Chapter 3, the designated suites of the protocols and mechanisms of three standard solutions of dynamic cyber resilience specified in this research involve the distance-vector solution, the link-state solution, and the path-rule solution that fully described in the section 2.4.2 of Chapter 2.

The suite of the distance-vector solution used in the simulations and emulations during the testing scenarios has protocols and mechanisms comprise Message-Digest Algorithm Type 5 (MD5), Gateway Load Balancing Protocol (GLBP), Resilient Ethernet Protocol (REP), and Enhanced Interior Gateway Routing Protocol (EIGRP) (Brtis et al., 2013).

Likewise, the suite of the link-state solution contains a distribute-list filter, Virtual Router Redundancy Protocol (VRRP), Resilient Packet Ring (RPR) protocol, and Intermediate System to Intermediate System (IS-IS) protocol (Nazir et al., 2017). In addition, the suite of the path-rule solution encompasses the TTL Security Check mechanism, Control Plane Policing (CoPP), Path Computation for Resilient Networks (PCRN), and internal Border Gateway Protocol (iBGP) (Laderman et al., 2015).

Fourthly, since real DDoS cyberattacks have become more expensive and complex to conduct, modern research uses simulations or emulations to mimic this type of actual cyberattack (Mosharraf et al., 2015). Further, these quantitative research methods are acceptable practices for determining the effectiveness and efficacy of the CII capabilities measure against concurrent and consecutive DDoS cyberattacks (Wang, Z. (2019).

The OPNET simulator and GNS3 emulator are necessary technical instruments used in this research to generate configurable and adjustable network traffic during different DDoS testing scenarios and collect the primary and optimized data (Mohammad et al., 2017). These data are useful to evaluate the diverse technology solutions of dynamic cyber resilience based on computing simulation and emulated experimental methods explained in section 4.2.1 and section 4.3.2 within this Chapter.

Fifthly, the sources of the modern and free datasets are limited for use in DDoS emulations and simulations. The available ones exist publicly via some universities and specialized institutes



(Ullah et al., 2018). In this research, the dump data are real and simulated datasets to emulate and simulate the DDoS cyber-attacks correspondingly against coupled CII networks throughout testing scenarios (Dsouza et al., 2013). The standard eigenvector techniques filtered and eliminated inappropriate features from the aggregated datasets. As a final point, the technology solutions are applied to the selected real and simulated datasets (Moyer et al., 2016).

Regarding the OPNET computing simulation, the network traffic source derives from the real SSDP dataset of Colorado State University, named FRGP\_SSDP\_Reflection\_DDoS Attack\_Traffic 20140930 with DOI 10.23721/109/1377046, ID DS-0777, size 26 GB and dated September 30, (2014).

The network traffic source in GNS3 emulated experiments comes from the simulated TCP SYN dataset of Information Sciences Institute - the University of Southern California, named Mirai-B-scanning-20160601 with DOI 10.23721/109/1354225, ID DS-0740, size 1.1 GB, and dated March 30, (2017).

The source traffic datasets contain process tables of cyberattack packets that need pre-processing to extract relevant information include the saved packet inter-arrival times as a list of double-type values, the time duration between the first and last packets of the traffic source, and the list of the different IP addresses in the traffic source. Then set up the emulation and simulation instruments (Herrera & Maennel, 2019).

Sixthly, the testing scenarios are operating under-designed simulations and emulations to evaluate the cyber resiliency capabilities of the coupled CII networks. The TCP/IP interdependencies among the hub nodes are significant because the CII networks have scale-free topology at a cyber-level, are vulnerable to targeted DDoS cyberattacks (Singh et al., 2016).

The substantial property of the scale-free topology of the interdependent CII networks correlates

with the high cyber resilience to network failure when the hub nodes are affected by a cyber-attack, whether disconnecting the one or more links of the hub node partially or removing the hub node itself completely (Du et al., 2015).

The physical interdependencies of the CII networks are often planarly drawn without crossing links where possible, but the logical scale-free interdependencies of the CII networks are typically not planar in cyberspace (Seppänen et al., 2018).

Therefore, this research defined three types of testing scenarios in different conditions to fully understand the proposed solution’s effect with standard solutions on dynamic cyber resilience capabilities for CII networks (Wicks et al., 2018). Each scenario happens within one day, and there was one day off in-between every two emulations or two simulations to ensure the cache of the previous ones has been totally emptied (Yamin et al., 2020).

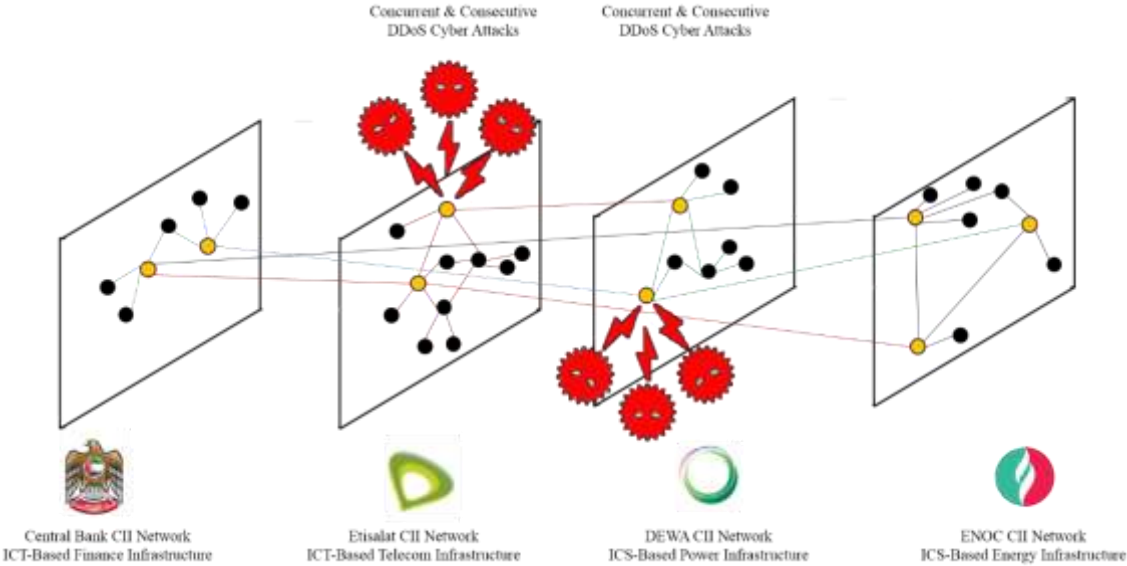


Figure 4.13: Diagram of the Core-Core Scenario

Every DDoS cyberattack stayed active for a specific duration after the beginning time during the scenario. The first is the core-core scenario demonstrating three concurrent and consecutive

DDoS cyberattacks against two interdependent hub nodes in two different core CII networks simultaneously (Burla et al., 2016). The three concurrent and consecutive DDoS cyberattacks are indicated by the two red groups of three ugly faces with arrows shown in Figure 4.13.

For triggering the cyber failures to simulate and emulate the cascading effects of the CII networks, three events of DDoS cyber-attacks are occurred to affect the targeted hub nodes in the CII networks at discrete points of time, not necessarily at the beginning of the running scenarios (Fan et al., 2014). The period of every scenario during simulation or emulation is 24 hours interspersed with seven regular events with taken screenshots intermediately after them for results recording (Hayel & Zhu, 2015).

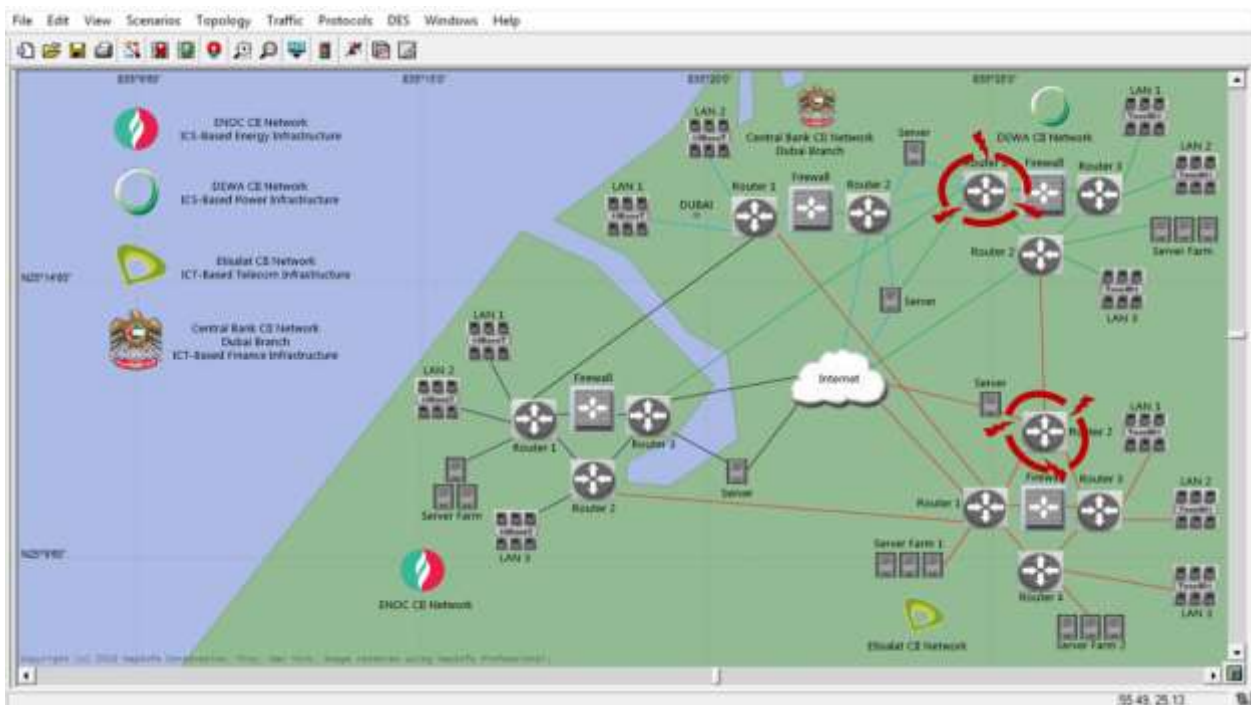


Figure 4.14: OPNET Simulation for the Core-Core Scenario

The starting point of the first event has occurred with no failure at the time  $t_0$  for hub nodes that would be tested in the interdependent CII network because they have not faced any cyber-attack yet (Başar & Zhu, 2012). The second event at the time  $t_1$  is the first failure that occurred after the

first concurrent and consecutive cyber-attacks on the two hub nodes in two different CII networks simultaneously within the coupling network. At the time  $t_2$ , the third event is the first recovery for attacked hub nodes below (Wu et al., 2018).

The fourth event at the time  $t_3$  is the second failure after the second concurrent and consecutive cyber-attacks on the same two hub nodes that attacked previously, followed by the second recovery at the time  $t_4$  as the fifth event (Buldyrev et al., 2010).

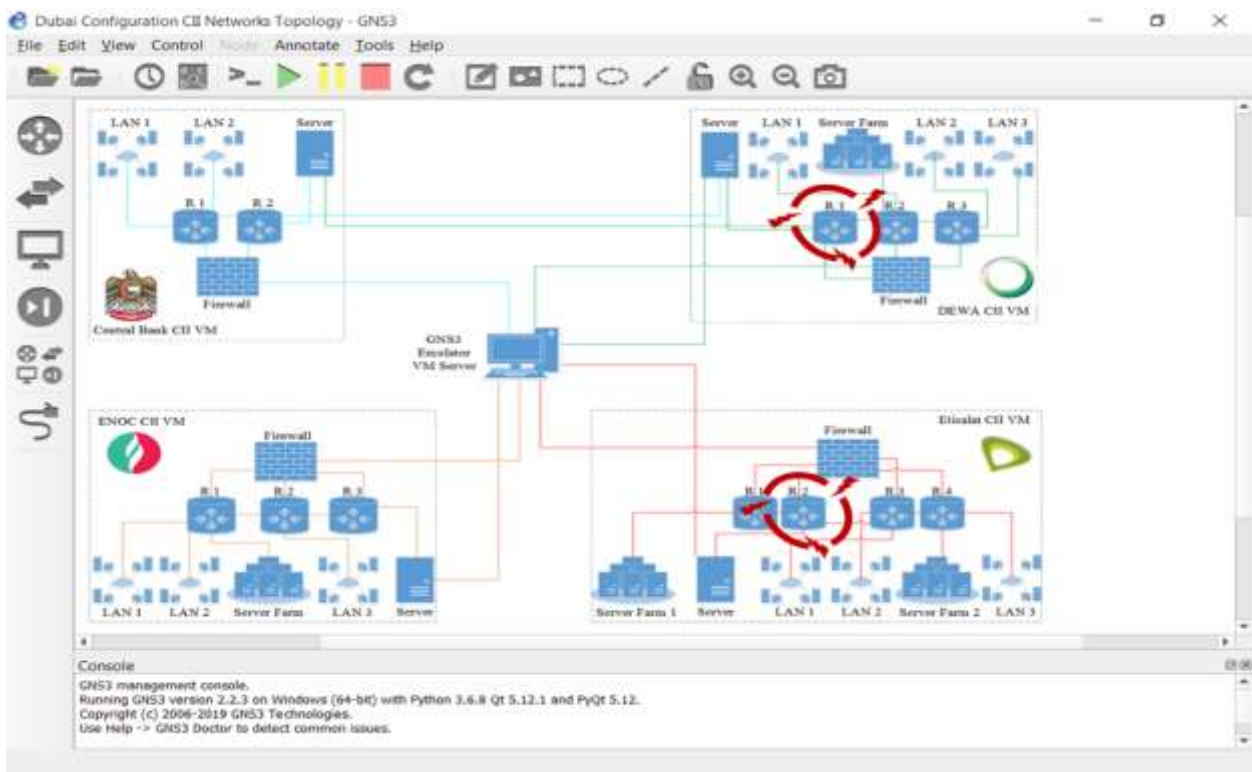


Figure 4.15: GNS3 Emulation for the Core-Core Scenario

The third failure in the sixth event at the time  $t_5$  occurred after the last concurrent and consecutive cyber-attacks on the same two hub nodes that attacked at the time  $t_1$  and the time  $t_3$  earlier. So then, the failure hub nodes have recovered at the time  $t_6$  as the seventh and final event in each scenario (Tian et al., 2015).

The Graphical diagrams of the first scenario implemented using OPNET computing simulations,

as shown in Figure 4.14, and the GNS3, emulated experiments, as shown in Figure 4.15 in both primary and optimized phases of the research.

Both router 1 ( $R_1$ ) in the Etisalat core network and router 2 ( $R_2$ ) in the DEWA core network have been attacked together by three DDoS cyberattacks at  $t_1$ ,  $t_3$ , and  $t_5$ . These cyberattacks have been indicated in the figures by the two red circles with three arrows for each. OPNET simulation and GNS3 emulation measure the five networking metrics for determining the levels of cyber resilience factors (Fernando et al., 2017).

The second scenario is the core-edge scenario that performs three concurrent and consecutive DDoS cyberattacks against two connected hub nodes simultaneously, one of them in the core CII network and the other in the one edge CII network (Rahnamay-Naeini & and 2016), as illustrated in Figure 4.16.

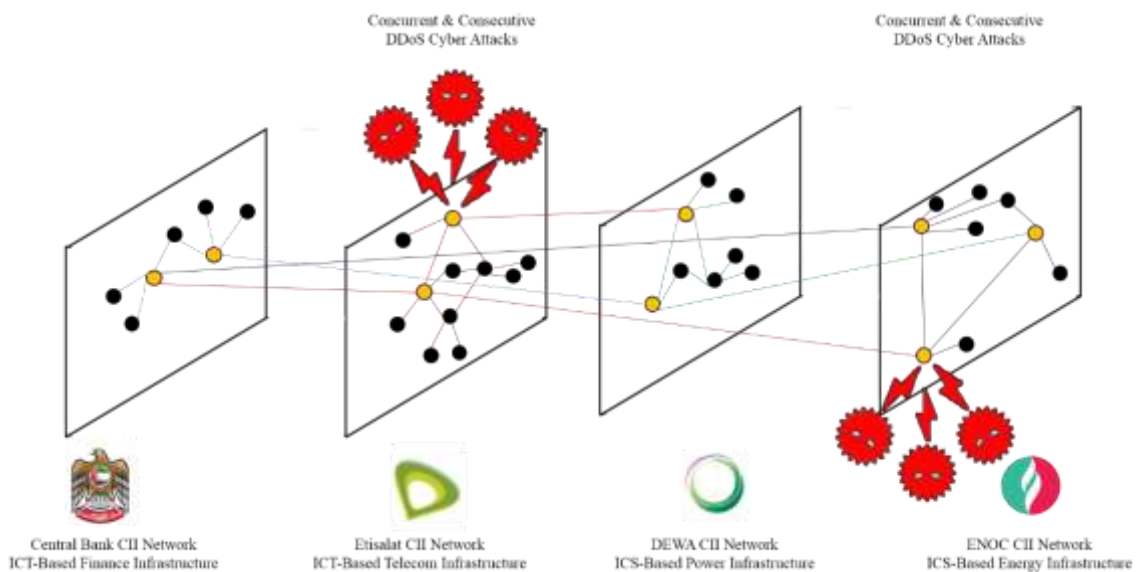


Figure 4.16: Diagram of the Core-Edge Scenario

The Riverbed OPNET modular contain a specialized module called Application Characterization Environment (ACE) that imports traces of the network traffic into computing simulation,

supports packet formats of various traffic sources, including the dataset files, provides the flexibility of selecting parts of the network traffic, and slices large dataset files into more manageable fragments preceding to computing simulation (Rozorinov et al., 2017).

In addition, there are technical features in the GNS3 to inject the traffic packets typically into the CII networks or as bursts. GNS3 parses the dataset file, extracts the packet payload headers, denotes the flag information at specific points, and identifies the interval periods of the emulation events (Emiliano & Antunes, 2015).

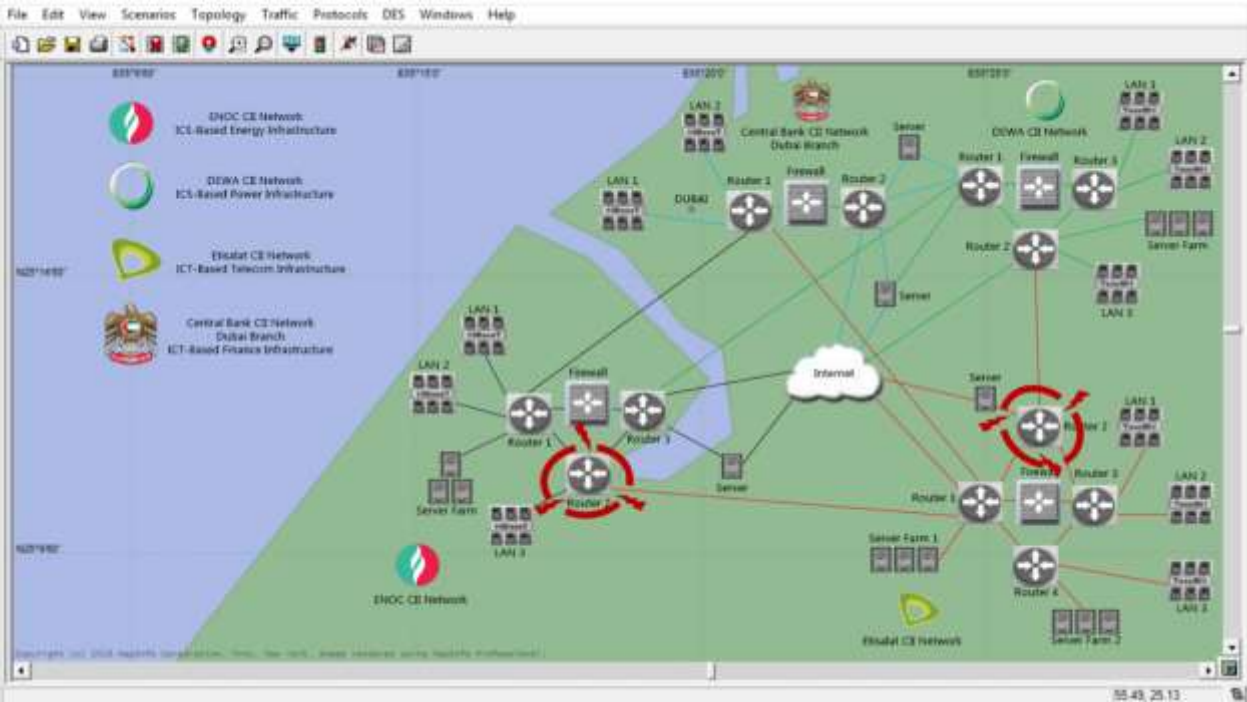


Figure 4.17: OPNET Simulation for the Core-Edge Scenario

In order to generate the data in the simulations and emulations, the DDoS cyberattack sends out-of-band data to three ports 78, 126, 139 of the operating system for the targeted hub nodes causing to crash (Mosharraf et al., 2015). The DDoS cyberattack was detected by penetrating the manipulated data for handshake traffic that followed thru flagged packets. These packets correspond to the IP header format, including IP addresses, flags, port numbers, and a few other



fields (Wright et al., 2016).

The DDoS process table's pre-processed traffic data consists of interval periods of observed three cyberattack events over 24 hours (1440 minutes) in both computing simulations and emulated experiments (Behal & Kumar, 2016). The filling up of the process table underlying the operating systems of targeted hub nodes, rendering the operating systems lifeless until the author has terminated the DDoS cyberattacks (Georgiev & Nikolova, 2017). The DDoS process table was detected by recording many connections to the targeted hub nodes' particular ports during the specified interval periods (Wang, 2019).

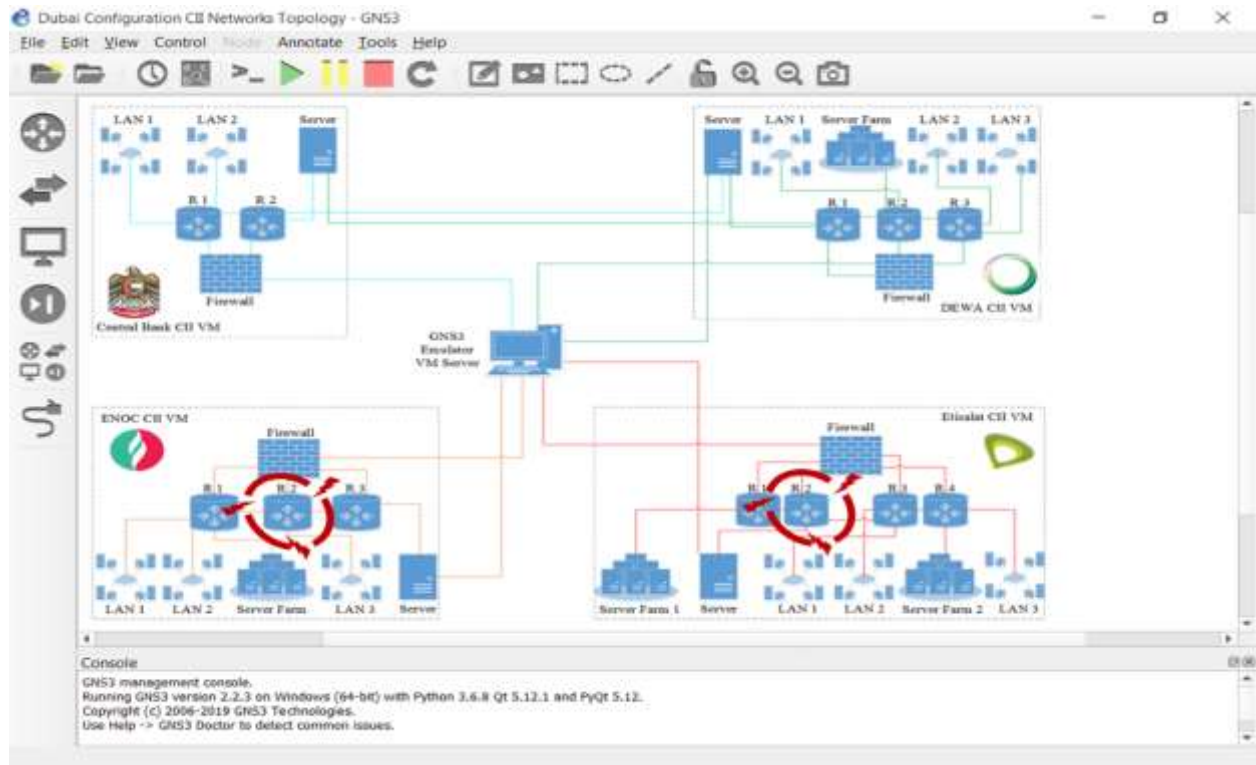


Figure 4.18: GNS3 Emulation for the Core-Edge Scenario

The first event's overall period is 74 minutes of data containing 41657 extracted packets between the interval time  $t_1$  (422<sup>nd</sup> min) to time  $t_2$  (476<sup>th</sup> min). Likewise, the overall period of the second event is 89 minutes of data containing 65644 extracted packets between the interval time  $t_3$  (936<sup>th</sup>

min) to time  $t_4$  (1025<sup>th</sup> min) (Yamin et al., 2017).

The third event's overall period is 113 minutes of data containing 89921 extracted packets between the interval time  $t_5$  (1285<sup>th</sup> min) to time  $t_6$  (1398<sup>th</sup> min). The interval between the first event at the time  $t_2$  and the second event at the time  $t_3$  are 15 minutes; the interval between the second event at the time  $t_4$  and the third event at the time  $t_5$  is 24 minutes (Sethi & Hnatyshin, 2012).

The firewalls captured 122143 packets, 103901 packets were sent from the DDoS botnets to the targeted hub nodes, and 18242 packets were sent back from the targeted hub nodes to the DDoS botnets (Lu & Yang, 2012).

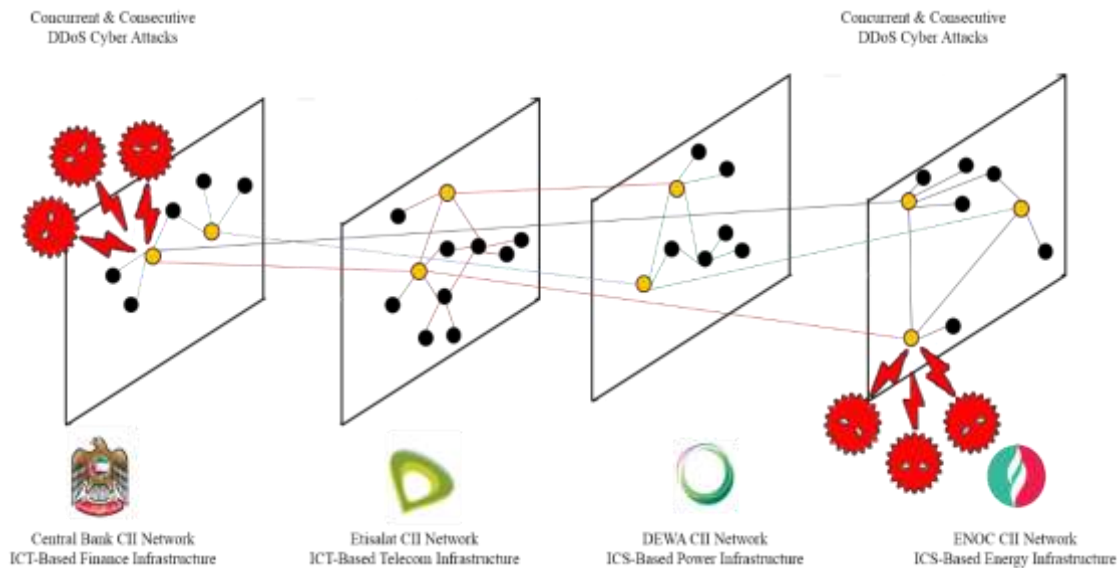


Figure 4.19: Diagram of the Edge-Edge Scenario

Several setup measures in OPNET and GNS3 study the IP address distributions of the data packets during the entire simulations and emulations, respectively, where the IP addresses correspond to the targeted routers (R1) of the DEWA and Central Bank CII networks, and the targeted routers (R2) of the Etisalat and ENOC CII networks (Sterbenz et al., 2013).



The Graphical diagrams of the second scenario implemented by using OPNET computing simulations, as shown in Figure 4.17, as well as GNS3, emulated experiments, as shown in Figure 4.18 in both primary and optimized phases of the research (Welsh, 2013).

As per OPNET simulation and GNS3 emulation in these figures, router 2 ( $R_2$ ) in the Etisalat CII as a core network and router 2 ( $R_2$ ) in the ENOC CII as an edge network have been attacked together by three DDoS cyberattacks at the time  $t_1$ ,  $t_3$ , and  $t_5$  to measure the five networking metrics for determining the levels of cyber resilience factors (Patrman et al., 2019).



Figure 4.20: OPNET Simulation for the Edge-Edge Scenario

The third is the edge-edge scenario representing the two different CII networks and the edges connecting them, indicating the interdependencies under three concurrent and consecutive DDoS cyberattacks against two hub nodes simultaneously, as displayed in Figure 4.19 (Behal & Kumar, 2016).

Each CII network of the four CII has different network architecture based on its internal operations and services (Moraitis et al., 2020). The DEWA CII network architecture has three routers, one firewall, three local area networks (LANs), one server farm, two shared servers, one direct internet connection, and three interdependent connections with other CII networks (Marchese et al., 2020).

The Etisalat CII network architecture has four routers, one firewall, three LANs, two server farms, one standalone server, one direct internet connection, and three interdependent connections with other CII networks (Rozorinov et al., 2017).

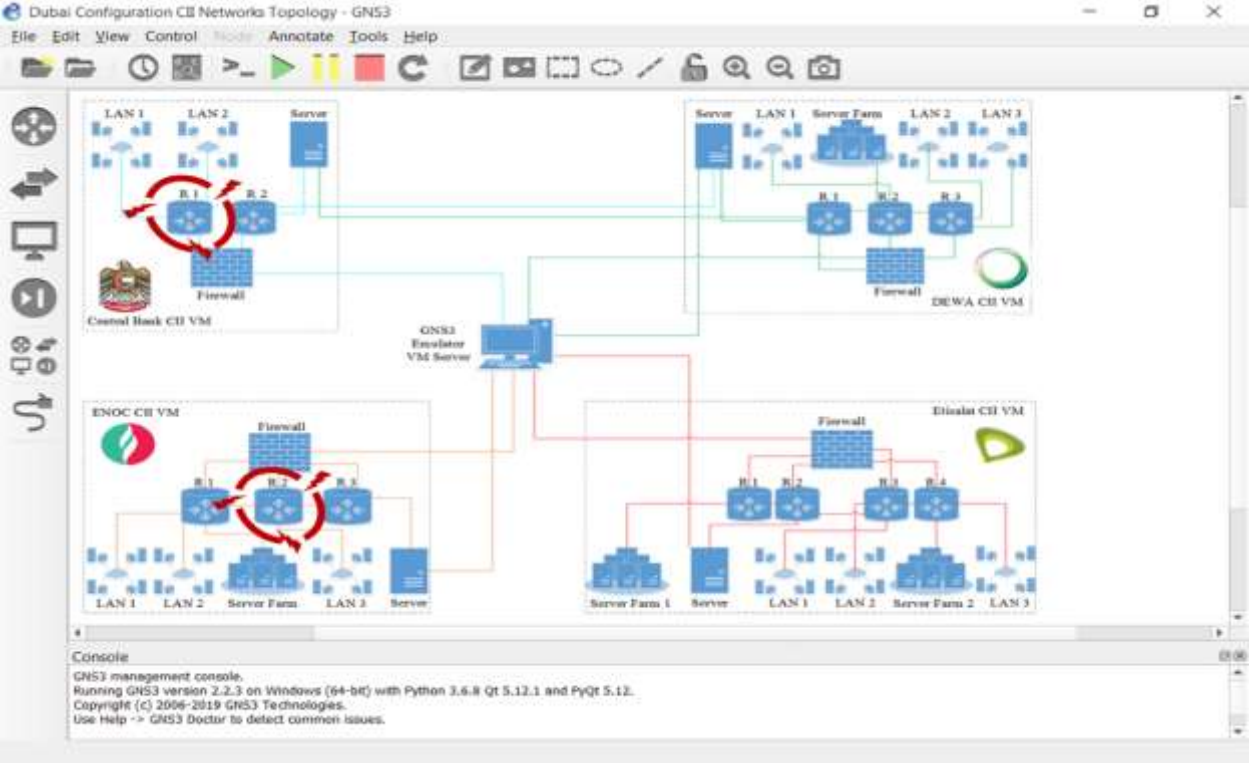


Figure 4.21: GNS3 Emulation for the Edge-Edge Scenario

Besides, the ENOC CII network architecture has three routers, one firewall, three LANs, one server farm, one standalone server, one direct internet connection, and three interdependent connections with other CII networks (Thompson et al., 2019).

Lastly, the Central Bank CII network architecture has two routers, one firewall, two LANs, two shared servers, one direct internet connection, and three interdependent connections with other CII networks (Njemaze et al., 2019).

In every emulated experiment, the four architectures of the CII networks are virtual, and each of them runs over a physical server separately. Besides, one physical server is dedicated to the GNS3 emulator's virtual machine, and two virtual machines are used as DDoS botnets (Dupont, 2019).

On the other hand, the four architectures of the CII networks in every computing simulation are OPNET and DDoS software-based, and each of the architectures runs over a physical server separately at the same time (Anne et al., 2018). Moreover, these architectures in computing simulations and emulated experiments were continuously used without any change during core-core, core-edge, and edge-edge testing scenarios (Sokolov et al., 2019).

The Graphical diagrams of the second scenario implemented using OPNET computing simulations, as shown in Figure 4.20, and GNS3, emulated experiments, as shown in Figure 4.21 in both primary and optimized phases of the research (Ostfeld et al., 2014).

As per OPNET simulation and GNS3 emulation in these figures, router 1 ( $R_1$ ) in the Central Bank CII as an edge network and router 2 ( $R_2$ ) in the ENOC CII as an edge network have been attacked together by three DDoS cyberattacks at the time  $t_1$ ,  $t_3$ , and  $t_5$  to measure the five networking metrics for determining the levels of cyber resilience factors (Hadjsaid et al., 2010).

The collected data from computing simulations and emulated experiments was observed and recorded. Data collected from the emulated experiments were deemed more trustworthy than those collected from computing simulations (Zafar et al., 2017).

This is because the emulated experiments combine two cyber and physical parts that consider

more reality to the actual world; also, the computing simulations have a minor invisible flaw, causing a significant difference in the final outputs (Castillo et al., 2019). Despite these two primary reasons, the collected data during simulations and emulations in this research were found so far to match (Sharif & Sadeghi-Niaraki, 2017).

Finally, the consequences of the cyber failure influences among the interdependent CII networks were analyzed more precisely; for example, the core-core scenario simulates or emulates a power and telecom CII network failure after three concurrent and consecutive DDoS cyberattacks (Anne et al., 2018).

The hub nodes of the power generation, transmission, and distribution sources connected in the DEWA CII network were influenced significantly (Moraitis et al., 2020). Power plants took varying amounts of time to resume the production of electricity. Backup generators and fuel supplies were not enough to maintain essential electricity services (Pedroni et al., 2015).

The lack of electricity also directly compromised the ENOC CII network's ability to manufacture or transport its products by traditional pipelines (Abdel-Razeq et al., 2018). The interdependent CII network of the Central Bank has a significant disruption by reducing the electricity supply (Njemaze et al., 2019).

The disruption in the DEWA by the beginning of the simulation or emulation common caused its CII network to stop working entirely after the first DDoS cyberattack (Fotouhi et al., 2017). Similarly, the DDoS cyber-attack caused a large negative effect on the running operations of the Etisalat telecom CII that dropped (Theron & Bologna, 2013).

The negative effect of both core CII networks' failures was escalated to other edge CII networks running functions and reached partially dropped in financial services and energy operations (Mbanaso et al., 2019). In terms of adequate service level provided, there was a total drop in the

telecommunication operations of Etisalat CII, whether for landline telephone or cellular networks (Maglaras et al., 2018).

The critical situation increased the telecommunication service demand, and most of its services were overloaded during the electricity power outage of the DEWA CII network. The recovery priority is accessing the servers of telephone landlines to emergency responders (Beyza et al., 2019). In addition to the cyber failure of the DEWA CII that mitigated by employing the backup generators to power its production processes and deliver electricity to other interdependent CII within the coupled networks (Gasser et al., 2019).

As the Central Bank's financial services rely on telecommunications operations, it experienced a rapid degradation of banking services following the electrical power collapse (Dupont, 2019). However, secure network servers and backup generators allowed Central Bank to provide at least the critical services to most banks and financial institutions (Njemaze et al., 2019).

The electricity power failure in the DEWA CII network had a maximal impact on the Central Bank CII network's activities because it interrupts the services and loses sensitive financial data with economic consequences (Joshi, 2020). Furthermore, besides the comprehensive analysis of interdependencies among CII networks, other impacts were reported directly related to cyber failures (Thompson et al., 2019).

The records collected from the status-changing events are taken from the testing scenarios outputs at the end of the simulations and emulations (Hofreiter & Zvaková, 2017). The data is analyzed crossover the proposed and standard solutions of dynamic cyber resilience with charts like in Chapter 5.

## **4.2 Research Methodology**

Many researchers describe research methodology in different ways. It is a means of doing something (Cai et al., 2018). Also, refer to following the steps, procedures, and strategies for gathering and analyzing the research investigation data. Another researcher considers the methodology inclusive of the design, setting, sample, methodological limitations, and data collection and analysis techniques in a study (Ferreira, 2019).

Besides, the methodology's description is a coherent group of methods that complement one another and can fit to deliver data and findings that will reflect the research question and suit the researcher's purpose (Graubart & Bodeau, 2016). Likewise, methodology means a framework of theories and principles on which methods and procedures are based (Pipyros, 2019).

In detail, the methodology states the scientific techniques of obtaining, organizing, and analyzing data and conducting the study (Igor & Aleksandr, 2018). The correct methodology decisions depend on the nature of the research question employed to obtain useful knowledge (Behal & Kumar, 2016).

The methodology denotes how this research is done in this study and its logical sequence. The thesis focuses on developing, implementing, evaluating, and optimizing the novel proposed solution; therefore, this research methodology was quantitative.

### **4.2.1 Data Collection**

This research's primary data has been significantly collected using two primary sources; computing simulations and emulated experiments (Sharif & Sadeghi-Niaraki, 2017). In addition, the collection procedure's scope contributes to obtaining high-quality data in terms of dynamic cyber resilience capabilities for the proposed solution compared with standard solutions (Brennan

et al., 2019).

The strengths of quantitative research methods used associate principally in understanding the developed proposed solution's crucial characteristics conducted a series of experiments and simulated scenarios that implemented, and capabilities evaluated (Nan & Sansavini, 2017).

The foremost objective of computing simulations and emulated experiments is capturing the necessary data that lead to a set of results that need an interpretation when evaluating the capabilities of the proposed solution have compared with the standard solutions of dynamic cyber resilience to answer the research questions that cannot be answered by other research methods like testbeds (Yamin et al., 2020).

The imitation of the conditions and processes of the real world is known as simulation. Simulation is a pure software-based method (Leslie et al., 2018). The CII's behavior is characterized by simulation, analysis, what-if questions raised, and CII's closely similar to real conditions designed (Wang et al., 2019). Furthermore, important information regarding the feasibility, productivity, and efficiency of CII's was assessed by simulation before the real deployment of the actual implementation (Dan-Suteu & Gânsac, 2020).

Typically, a proposed solution needs to be developed to perform a simulation. Such a solution demonstrates dynamic cyber resilience capabilities that treat the desired CII's (Ouyang, 2014).

The proposed solution represents CII itself, while the operation of the CII's is in the time shown by simulation. However, it is not trivial to derive a reliable conclusion from a simulation result. Diverse steps exist during a simulation and may vary to the purpose of the simulation (Ormrod & Turnbull, 2019).

These steps are not necessarily sequential and are applied in a non-serial manner. Nevertheless, evaluating the proposed solution's capabilities requires cyclic revision and a thorough evaluation

of the simulation functionality (Setola et al., 2017). There are three types of simulation that have been mentioned in computer science literature; Monte Carlo simulation, Trace-driven simulation, and Discrete-event simulation (Johnson et al., 2018).

Monte Carlo simulation is a static simulation or one without a time axis. Therefore, it is used for probabilistic modeling events whose characteristics vary over time (Chowdhury et al., 2020). Besides, the Monte Carlo simulation is utilized to appraise non-probabilistic expressions using probabilistic approaches (Sterbenz et al., 2013).

Trace-driven simulation uses a trace as an input in the process of simulation. A continuous-event trace is defined as a time-ordered history of the proposed solution in real CII (Singh et al., 2016). Trace-driven simulation generally analyzes or tunes resource management algorithms (Grafenauer et al., 2018).

In contrast, discrete-event uses a discrete-state proposed solution of the CII for simulation due to the variable CII state described by the number of states at various events (Dinitz & Itzhak, 2017). Furthermore, time in discrete-event simulation can be discrete or continuous. The last two simulation types are widely used due to their high performance and scalability (Abdin et al., 2019).

This research used discrete-event simulation to collect quantitative data for evaluating dynamic-based and time-dependent technology solutions. On the other hand, the emulation typically is a combination of a software-hardware-based method to perform the simulation (Castillo et al., 2019). In the emulations, actual hardware besides simulated components provides realistic dynamic cyber resilience capabilities for the proposed solution. The emulation usually has high scalability for simultaneously emulating several CII (Hehenberger et al., 2016).



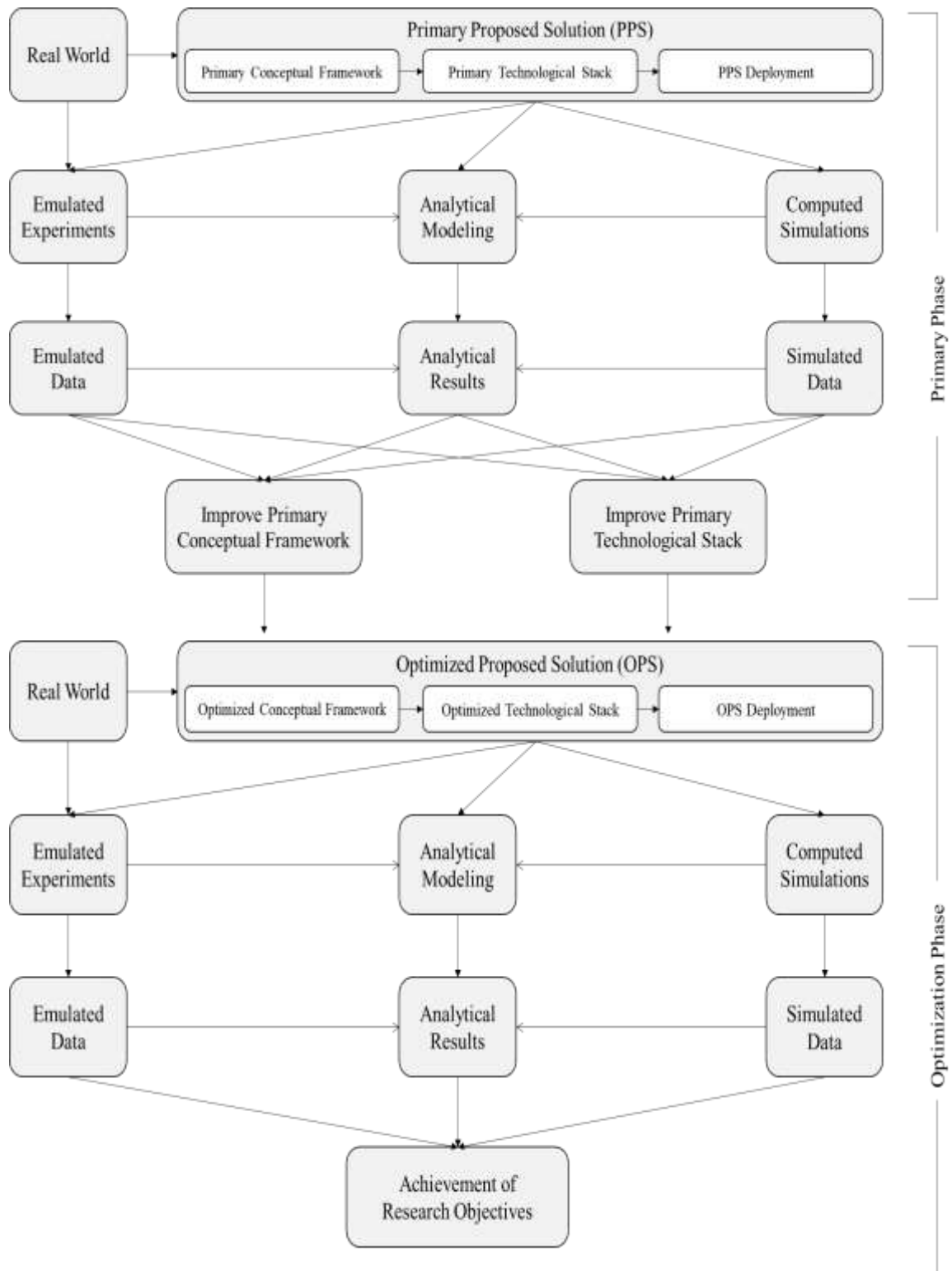


Figure 4.4: The Research Methodology

Compared to simulation, emulation is implemented in real CII, runs real proposed solution codes, and improves their capabilities precision (Rozorinov et al., 2017). Emulation is categorized into a cyber-layer and a physical layer appropriate for timing interactions among coupled CII networks and fine-tuning the proposed solution (Eldosouky, 2019).

The emulated experimental method was used broadly to evaluate new technology solutions to solve the research gaps. Experimental evaluation is often divided into two phases (Sterbenz et al., 2013). In the primary phase, the measurements are taken to identify the data concerning the proposed solution under primary evaluation. Then an optimization phase attempts to answer the research questions (Uday, 2015).

The well-designed emulation starts with a list of the research questions that the experiments are expected to answer (Banescu et al., 2015). Therefore, excellent record-keeping is essential in experimental work because experiments run on the transient coupled CII networks (Luijff et al., 2018).

In addition, the emulation design is a crucial issue to be carefully characterized by the technical specifications of hardware and software used in the experiments, controlled factors, measures taken to account, and numerical results reported during the phases. The analytical modeling provides insight into these experimental results (Pipyros, 2019).

As depicted in Figure 4.4, this research has been performed in two phases, primary and optimized. The process steps of the research in each phase have been outlined concisely. The proposed solution focuses on defining a conceptual framework as an abstract of the real world regarding data collection. This proposed solution is much less complicated than the real-world model (Ani et al., 2019).

Therefore, allowing to understand the coupled CII networks better and use the proposed solution

to perform simulations that could not perform in the real world itself because of high cost and poor accessibility (Fotouhi et al., 2017). The simulation method is often combined with emulated experiments to collect the research's primary data (Das et al., 2020). The multi-methods quantitative is deployed to verify the proposed solution's functionality and check the correctness of the collected data (Potii & Tsyplinsky, 2020).

Algorithms and models are the purposeful abstraction of a proposed solution and are driven by the study to reduce it to a limited but representative set of components and interactions that allow the quantitative description of its properties (Kochedykov et al., 2020). They have been expressed in diverse ways and described by designed diagrams or embedded coding in a computer program to specify quantitative aspects of how a proposed solution has been constructed from a data collection of interacting components and simulated and emulated its behavior (Nan & Sansavini, 2017).

Thus, the simulation and emulation specifications should be well structured and tolerate the iterative four-objective cycle, including developing, implementing, evaluating, and optimizing the proposed solution through the primary phase (Hehenberger et al., 2016). Many simulation models run out to generate much data to analyze by high-quality facilities and smooth analytical modeling (Dsouza et al., 2013).

After writing and testing a unique computer program, the collected data was analyzed to evaluate the proposed solution's capabilities (Sansavini & Fang, 2016). The primary results that lead to necessary improvements are applied to the algorithms and models to be optimized. The refinements are also utilized for better coding, easy debugging, and rapid testing of the proposed solution (Tonhauser & Ristvej, 2019).

In the next phase, the same process steps replicate in the optimization phase to collect the data again through the simulation and emulation methods under the same scenarios to evaluate the quality of the improvements implemented in the cyber zero-trust algorithms and protocols of the optimized proposed solution compared with the results of the standard solutions to achieve research goal and objectives (Eldosouky, 2019).

#### **4.2.2 Data Analysis**

Data analysis is the most crucial part of successfully running for research purposes (Bloomfield et al., 2017). In general, it is a process of organizing, transforming, summarizing, and modeling collected data to explore, extract, and categorize useful information by analytical deductive or logical inductive reasoning (Fernando et al., 2017). It leads to better understanding and interpretation of patterns, relationships, themes, or trends for added insight and value to answer the questions and solve the research problems (Zhu & Chen, 2020).

According to LeCompte and Schensul (1999), data analysis definition is a process used by researchers to reduce data to a story and interpret it to derive insights (Moyer et al., 2016). The data analysis process reduces a large chunk of data into smaller fragments, making sense (Dsouza et al., 2013). on the other hand, Marshall and Rossman (2011) describe data analysis as a messy, ambiguous, and time-consuming but creative and fascinating process through which a mass of collected data is brought to order, structure, and meaning (Vasilyev et al., 2019).

Four types of data analysis are used across all research disciplines; descriptive, diagnostic, predictive, and prescriptive analyses (Divakaran et al., 2017). They link together and build upon each other from the simplest type of analytics to more complex based on the degree of difficulty and resources required and doing them in both top-down or bottom-up fashion (Ullah et al., 2018).

The first type of data analysis is descriptive analysis. It is the simplest and most common use at the foundation of all data insight. It answers the question by summarizing past data, usually in diagrams (Dibaji & Ishii, 2015). The next type is to dive deeper to ask why it happened where the diagnostic analysis comes in. To end with, it takes descriptive insights to create detailed information, find the causes of those outcomes, and identify behavior patterns (Greenhalgh et al., 2019).

The third type of predictive analysis attempts to answer what is likely to happen. This type is another step up from the previous analytics that utilizes the collected data to make logical predictions about future outcomes by relying on quality data modeling and added technology to forecasting (Thorisson et al., 2020).

The last type is the most sought-after and frontier of data analysis; the prescriptive analysis combines the meaningful insight from all previous analyses to determine the course of action to solve the current research problem. It utilizes state-of-the-art technology and quantitative data practices (Turskis et al., 2019).

This quantitative research adopted the first three types of the above data analyses. First, the descriptive type uses to describe the basic features of the primary and optimized results. Second, the inferential diagnostic type helps compare and interpret the findings, tests the formulated research hypotheses, and discusses meaningful patterns.

The third type of predictive analysis goes beyond the conclusions to create predictions and presents the questions' answers to achieve the research goal. Applying the adopted types of data analysis in this study, the analytical modeling was used as a quantitative research method besides the simulations and emulations (Barker et al., 2017).

Analytical modeling is arranged primarily for mathematical equations or quantitative

computational processing (Villate, 2014). However, the precise equations defined sufficiently representation of the different aspects of the CII environment to meet the research purpose (Karjanto & Husain, 2017).

It specifies the parametric relationships and their associated parameter values as a function of time to explain the effects and build predictions about the components of data, behavior, and the real world for complex mechanisms (Mitchell & Chen, 2016). The analysis results are expressed in parameter values that are often functions of other parameters and time through charts, tables, and other visualizations (Filippini & Silva, 2012).

Various analytical modeling kinds are further classified as static or dynamic (Fernando et al., 2017). A static model represents the properties of coupled CII networks that are independent at any time. The analyzed properties may have deterministic values or may include probability distributions on their values (Abdin et al., 2019).

A dynamic model represents the time-varying state of the coupled CII networks, like position as a function of time. The selection of a dynamic model in the thesis depends on the type of answered research questions (Canzani, 2016).

In practical terms, it analyzes the measured capabilities of different solutions for dynamic cyber resilience over a finite time within the coupled CII networks (Goldbeck et al., 2019). In most instances, the analytical model characterizes the grouped units of work and calculates the collected data generated during a series of time intervals (Leslie et al., 2018).

Analytical modeling is constructed as a basis for change prediction to understand the various coupling behaviors of interdependent CII networks under different cyberattack scenarios and study the failure effects to consider the single and total dynamic cyber resilience metrics (Pipyros, 2019).

For the research purpose of this study, the simulated and emulated data is feeding into the analytical modeling that is executed using the computerized mathematical platform (MAXIMA) based on a set of quantification equations of dynamic cyber resilience introduced by Tran (2015) that described in the section 4.3.1 in this Chapter.

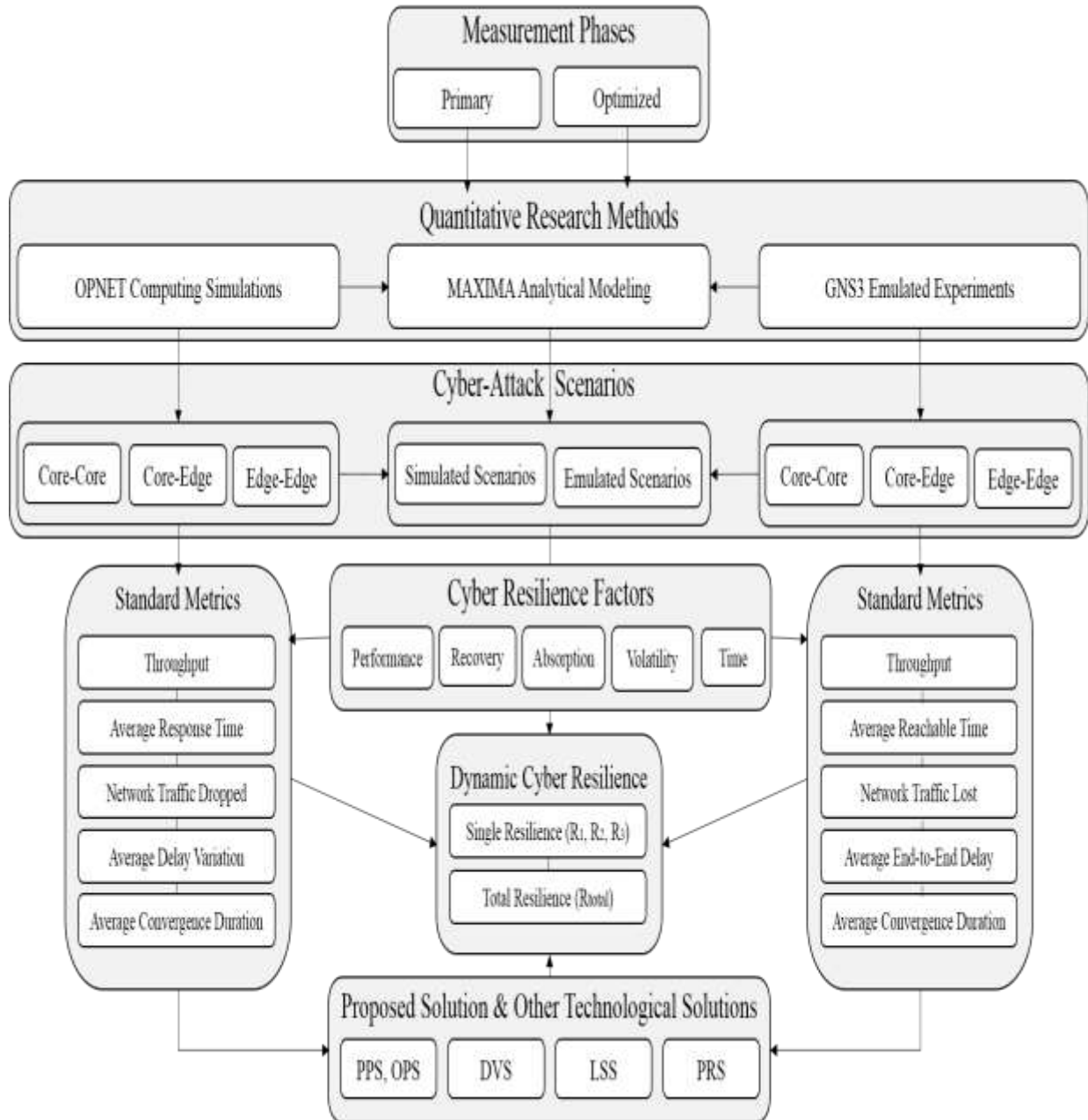


Figure 4.5: The Levels of Data Analysis in this Research

This research has five data analysis levels, as shown in Figure 4.5. The first analysis level contains two measurement phases, primary and optimized. The primary measurement phase demonstrates the initial results of the proposed solution prototype and compares them with the standard solutions of dynamic cyber resilience (Liu, 2016).

In contrast, the optimized measurement phase demonstrates the proposed solution's final results after optimization and comparisons with other results of technology solutions (Mo et al., 2017). The primary and optimized proposed solution is designated clearly in Chapter 3.

Both primary and optimized measurement phases using the same quantitative research methods at the second analysis level consist of computing simulations by using Optimized Network Engineering Tools (OPNET), emulated experiments by using Graphical Network Simulator-3 (GNS3), and analytical modeling by using the computerized mathematical platform (MAXIMA) (Teodorescu & Pickl, 2016). These technical instrumentations are well-described in section 4.3.2 of this Chapter.

The third analysis level has three concurrent cyber-attacks scenarios: core-core CII networks scenario, core-edge CII networks scenario, and edge-edge CII networks scenario for the selected critical information infrastructures such as ICS-based energy infrastructure networks ICT-based finance infrastructure network (Yamin et al., 2020).

Fourthly, the analysis in this level focused on the five cyber resilience factors described in section 2.4.3 of Chapter 2, involving the performance factor, recovery factor, absorption factor, volatility factor, and recovery time factor (Rasouli et al., 2014).

The standard networking metrics evaluated these factors: throughput, average response time, network traffic dropped, average delay variation, and average convergence duration, respectively, in the method of OPNET computing simulation (Sethi et al., 2012). In addition, the standard



networking metrics are throughput, average reachable time, network traffic lost, average end-to-end delay, and average convergence duration, respectively, in the method of GNS3 emulated experiments (Emiliano & Antunes, 2015).

The single and total resilience results are analyzed for the proposed solution and each standard solution after multiple concurrent and consecutive cyber-attacks in different scenarios (Haque et al., 2018). Finally, at the fifth analysis level, the set of comparisons are performed between the results of the Primary Proposed Solution (PPS) and Optimized Proposed Solution (OSP) and the standard solutions of dynamic cyber resilience, are Distance-Vector Solution (DVS), Link-State solution (LSS), and Path-Rule Solution (PRS) (Alcaraz, 2018).

The deductive method of quantitative data analysis in this research has a non-linear and iterative process aimed at testing the proposed solution depending on the continuous cycle of intertwined data collection and analysis activities to develop coherent interpretation adequately, answers the research questions (Das et al., 2020).

The forms of quantitative data analysis through the entire course of this research are textual and numeric data in detail, such as numbers, diagrams, documents, and experimental notes (Hehenberger et al., 2016). Observing the data, developing the initial ideas, comparing the outputs, finding the relationships are the primary required steps to judge and interpret the results (Shevchenko et al., 2018).

The quantitative analysis in this research is based on analytical notes, numerical data-oriented displays, and software packages combined or separately used to enhance the identification of findings, explore the differences and similarities, and develop the relationships between them (Marais & Uday, 2015).

The analytical notes are written during the research process to facilitate the reflection insight and

convert the simulations and emulations into visible forms for further manipulation (Cai et al., 2018). Thus, writing analytical notes of numerical data is a vital and valuable analysis technique for many purposes in this research (Deng et al., 2017).

Numerical data-oriented displays such as flowcharts, diagrams, and concept maps are permanent besides the visible technique used for data reduction and presentation to allow grasp and elaborate the quantitative analysis as a whole (Moraitis et al. 2020).

Software packages are ready-made computer programs that perform the technical tasks of aggregating, storing, and retrieving the massive amounts of data produced during the simulations and emulations for testing the proposed solution compared with standard solutions. In addition, it facilitates manipulation and makes explicit connections between results (Grafenauer et al., 2018).

#### **4.2.3 Data Validation**

Data validation is the research process of providing justification and confirmation through the provision of objective evidence that the specific requirements for intended use, collection, or analysis of data have been fulfilled (Behal & Kumar, 2016). The research process of determining the degree to which computing simulation or emulated experiments and their associated data accurately represents the real world from the perspective of the proposed solution's intended purpose compared with standard solutions (Pedroni et al., 2015).

This quantitative research's data validation is highly applied to data collected and analyzed (Divakaran et al., 2017). Moreover, it represents the degree of stability and consistency of the simulated and emulated data collected genuinely within the research process against the real world, proposed solution, and standard solutions (Gatchin & Sukhostat, 2019).

In addition to simulation and emulation are the explanation and prediction methods. They

represent the specification states to examine the proposed solution's capabilities and recognize the significant effects of the relationships between the simulated and emulated data observed after tested-retested (Sharif & Sadeghi-Niaraki, 2017). The valuable analysis under different scenarios compares the results using the same data and quantitative methods (Ormrod & Turnbull, 2019).

As the equilateral triangle illustrated in Figure 4.6, the different aspects of data validation were performed explicitly in this research process (Anne et al., 2018). The data validation was executed throughout the heart of the research process to ensure the successful proposed solution initially identified the research goal and objectives (Tsochev et al., 2019). It involves three main components: The real world to be modeled, the proposed solution developed, and the standard solution (Behal & Kumar, 2016).

For this research, the real world is any given CII network; the proposed solution is developed for dynamic cyber resilience and the standard solutions (Cao et al., 2017).

In the right edge of the outer triangle, the research process develops a proposed solution that represents the real world (Fraccascia et al., 2018). According to the research objectives, the conceptual model captures all the real world's relevant characteristics without oversimplifying or unnecessary complexity (Herrington & Aldrich, 2013). The proposed solution is obtained by a conceptual framework that represents the real world through computing simulation in data collection (Bosetti et al., 2016).

The proposed solution abstraction is based on the key aspects that significantly affect real-world behavior to be replicated (Gatchin & Sukhostat, 2019). This abstraction ensures that the proposed solution outputs are similar to those expected from the real world, and therefore its results enable the achievement of the research goal and objectives (Lade & Peterson, 2019).

The research process in the left edge of the outer triangle deploys the dynamic cyber resilience technology solutions extracted from the state-of-the-art related literature (Wang et al., 2019). During the development of distance-vector, link-state, and path-rule solutions, the emulated experiments were utilized as a quantitative method for valid data collection (Zafar et al., 2017). The emulations replicated the real world, estimated the capabilities required for dynamic cyber resilience from each cyberattack scenario, and utilized the generated information for managing cyber failure in real-world of the coupled CII networks considered (Castillo et al., 2019).

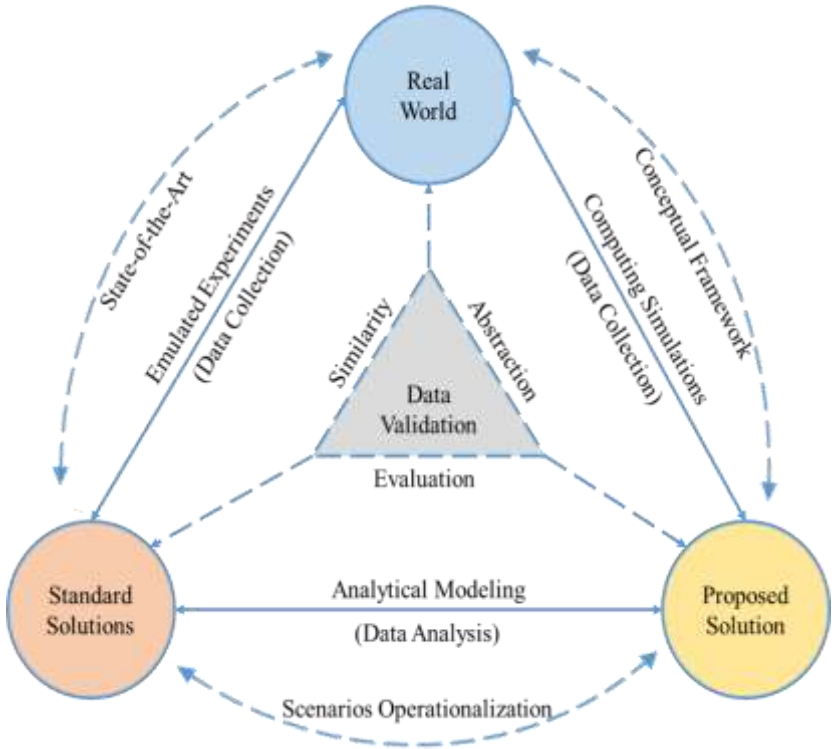


Figure 4.6: The Research Process

Finally, the outer triangle’s bottom edge ensures that data analysis is correct concerning the proposed solution and standard solutions (Fernando et al., 2017). In other words, analytical modeling is the quantitative method to ensure that the proposed solution is developed and

implemented smoothly (Ouyang, 2014).

Analytical modeling evaluates the proposed solutions by comparing obtained results from the scenarios operationalization with observations from the standard solutions (Alderson et al., 2015). The validation of the proposed solution is intended to ensure that data analysis is within an acceptable accuracy range (Pedroni et al., 2015).

The inner triangle of the data validation integrates the abstraction for running the simulated and emulated data over a particular time, gathering data, generating outcomes, and checking the similarity of the collected data by the developed proposed solution with those produced by standard solutions (Rozorinov et al., 2017).

All components throughout the research process support the valid data to be clean, correct, and proper and emphasize the need for explaining the correlation between the results of the evaluation metrics that measured the capabilities of coupled CII networks over time (Sterbenz et al., 2013). The data validation enables successful simulations and emulations to produce accurate enough and valuable results for achieving the research purpose (Ip & Wang, 2011).

Furthermore, the data validation aims to balance the simplicity of abstraction, scaling of similarity, and the evaluation's accuracy as the vital requirements for proposed solution development (Viswanathan et al., 2017). If the need for balancing increased, the complexity would increase because the extra data required led to more data validation requirements, which means satisfactory conclusions might be challenging to draw from the research (Orojloo & Azgomi, 2017).

Additionally, many practices have been implemented to make sure the requirements of the data validation in this research as the following: (1) Replication: three replications for each scenario,

where a scenario includes simulation and emulation depending on the data collection method and data analysis level (Wicks et al., 2018). Also, (2) Multimethod: two quantitative research multimethods contain computing simulation and emulated experiments to validate the collected data from two sources and two analysis levels (Yusta et al., 2011).

Moreover, (3) Research Phasing: two research phases have been performed to incorporate primary and optimized phases, confirming the same data collected and analyzed over different research phases (Lade & Peterson, 2019). As well, (4) Various Scenarios: three various cyberattack scenarios have been conducted in this study involve core-core, core-edge, edge-edge scenarios that collect and analyze diverse primary data by the same technology solutions of dynamic cyber resilience (Johnson et al., 2018).

(5) Control Solutions: the standard solutions consider as a control solutions group in the testing scenarios because no change occurred on their data collected and analyzed through the research phases in contrast to the changing of the proposed solution by the technical improvements in the optimized phase, influence on its data collected and analyzed (Laderman et al., 2015).

Further, (6) Secondary data: the primary data of standard solutions collected and analyzed during this empirical research compared objectively with the secondary data of the previous studies done by the other researchers on the same technology solutions (Caverzan & Solomos, 2014).

Finally, (7) Measurement Metrics: two different sets of standard networking metrics used for the duration of the measurement phases to collect and analyze the primary data for the proposed solution and standard solutions of dynamic cyber resilience that offered by the technical research instrumentations (Bhuyan et al., 2015).

The research process had designed, built, and performed the validation of the data to evaluate the

proposed solution to compare with what was developed to do before and upon the expectations because the numerous data inputs generated randomly in every simulation and emulation run are easy to make errors, especially with coding (Sharif & Sadeghi-Niaraki, 2017).

The data validation ascertains that standard solutions' data outputs compare rationality with the data collected from the proposed solution (Bergström et al., 2015). The research process's validation outcomes are likely to be link-dependent based on the precise values and certain initial factors for empirical research to analyze the variance for evaluating quantitative changes (Luijff et al., 2018).

## **CHAPTER 5. RESULTS AND DISCUSSION**

The thesis results are presented in this chapter and described in detail through graphical diagrams, snapshot charts, and numerical tables. Primary and optimized results are gathered and analyzed using computing simulations, emulated experiments, and analytical modeling.

The proposed solution results in both primary and optimization phases were evaluated, organized, and compared to the standard solutions under several testing scenarios with concurrent and consecutive cyberattack events based on the networking metrics set. The primary and optimized results were discussed, and the final research findings were interpreted according to the thesis purpose, study goal and objectives, and relevant literature. *See Appendix F: Primary Results Analysis and Discussion.*

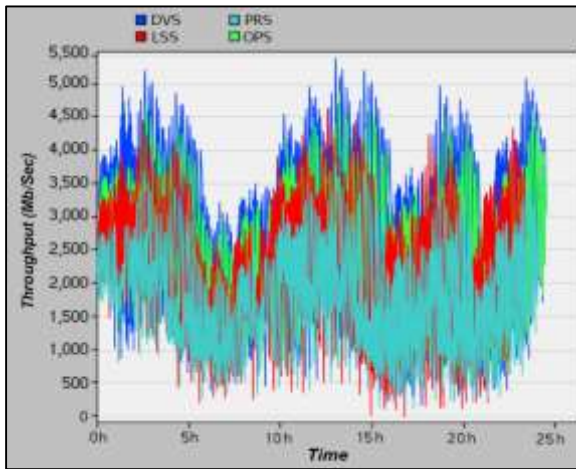
### **5.1 Optimized Results Analysis of Computing Simulations**

After the primary research phase was conducted, many improvements based on the primary evaluation and results analysis have been made on the primary proposed solution (PPS) as described in section 3.3.1, and section 3.3.2 of Chapter 3 to foster its strengths and handle the weaknesses competed with other standard solutions (PRS), (LSS) and (DVS).

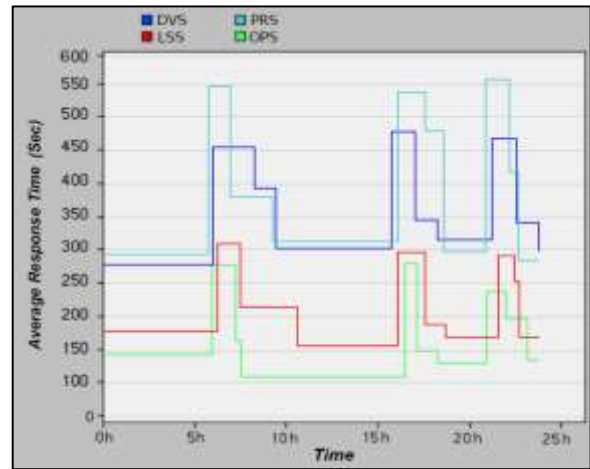
The computing simulations were conducted precisely throughout three repeated scenarios in the optimized phase. These scenarios include core-core scenario, core-edge scenario, and edge-edge scenario. Besides, five networking metrics consist of throughput, average response time, network traffic dropped, average delay variation, and average convergence duration.

These metrics are used to measure the associated factors of dynamic cyber resilience capabilities of the optimized proposed solution (OPS), and standard solutions include distance-vector solution (DVS), link-state solution (LSS), and path-rule solution (PRS). Additional analysis supplemented with results concerning causes and effects of failure and recovery events across the time frames.

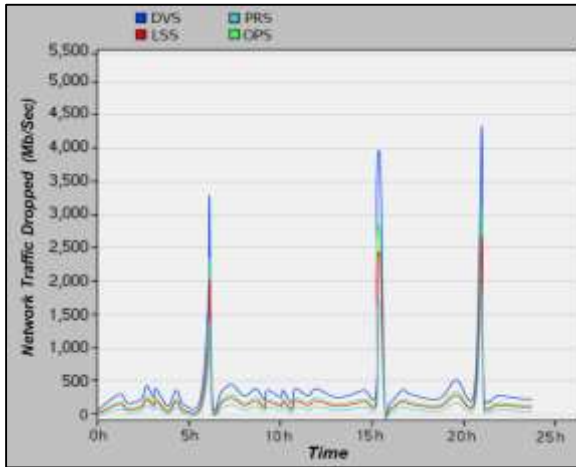




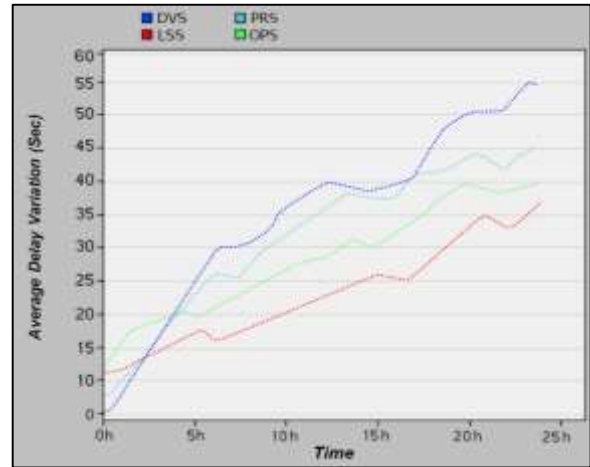
(a)



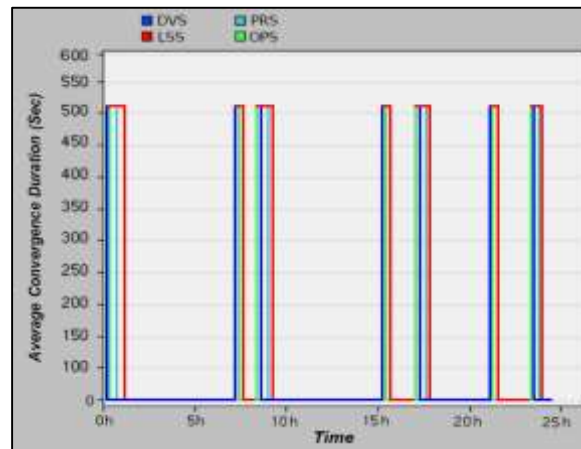
(b)



(c)



(d)



(e)

Figure 5.13: Optimized Results of OPNET Simulation for the Core-Core Scenario  
 (a) Throughput (b) Average Response Time (c) Network Traffic Dropped  
 (d) Average Delay Variation (e) Average Convergence Duration

Table 5.17: Optimized Results of OPNET Simulation for the Core-Core Scenario

Networking Metrics	OPNET Simulation			Dynamic Cyber Resilience Solutions			
	Event	Time (min)		OPS	PRS	LSS	DVS
Throughput (Mb/Sec)				No Cyber Attack			
	No Failure	$t_0$	0420	3374	2312	2914	3763
				First Cyber Attack			
	First Failure	$t_1$	0421	2340	1270	1738	2554
	First Recovery	$t_2$	0493	3511	2283	2962	3816
				Second Cyber Attack			
	Second Failure	$t_3$	0939	2733	1184	2423	2924
	Second Recovery	$t_4$	1022	3214	2155	2894	3992
				Third Cyber Attack			
	Third Failure	$t_5$	1287	2424	1207	2444	2475
	Third Recovery	$t_6$	1395	3469	2315	2927	3886
	Average Response Time (Sec)				No Cyber Attack		
No Failure		$t_0$	0423	0145	0293	0183	0277
			First Cyber Attack				
First Failure		$t_1$	0424	0284	0550	0312	0456
First Recovery		$t_2$	0501	0167	0376	0218	0391
			Second Cyber Attack				
Second Failure		$t_3$	0938	0289	0542	0292	0489
Second Recovery		$t_4$	1023	0150	0472	0188	0348
			Third Cyber Attack				
Third Failure		$t_5$	1280	0243	0563	0286	0466
Third Recovery		$t_6$	1394	0200	0425	0252	0341
Network Traffic Dropped (Mb/Sec)					No Cyber Attack		
	No Failure	$t_0$	0425	0219	0113	0156	0252
				First Cyber Attack			
	First Failure	$t_1$	0426	2374	1431	2006	3268
	First Recovery	$t_2$	0492	0233	0127	0162	0301
				Second Cyber Attack			
	Second Failure	$t_3$	0937	2818	1667	2413	4000
	Second Recovery	$t_4$	1031	0248	0131	0168	0313
				Third Cyber Attack			
	Third Failure	$t_5$	1284	3121	1834	2606	4448
	Third Recovery	$t_6$	1401	0206	0088	0129	0244
	Average Delay Variation (Sec)				No Cyber Attack		
No Failure		$t_0$	0426	0013	0006	0011	0002
			First Cyber Attack				
First Failure		$t_1$	0427	0021	0026	0017	0032
First Recovery		$t_2$	0494	0020	0025	0016	0030
			Second Cyber Attack				
Second Failure		$t_3$	0937	0031	0037	0026	0040
Second Recovery		$t_4$	1025	0030	0036	0025	0038
			Third Cyber Attack				
Third Failure		$t_5$	1283	0040	0044	0035	0051
Third Recovery		$t_6$	1404	0038	0043	0033	0050
Average Convergence Duration (Sec)					No Cyber Attack		
	No Failure	$t_0$	0428	0332	0379	0394	0308
				First Cyber Attack			
	First Failure	$t_1$	0429	0477	0423	0494	0464
	First Recovery	$t_2$	0498	0368	0384	0422	0353
				Second Cyber Attack			
	Second Failure	$t_3$	0941	0462	0412	0498	0483
	Second Recovery	$t_4$	1026	0371	0378	0408	0376
				Third Cyber Attack			
	Third Failure	$t_5$	1283	0444	0432	0499	0489
	Third Recovery	$t_6$	1394	0346	0373	0495	0326

In general, Table 5.17 introduced proof that the improvements leveraged the overall results of the proposed solution through the core-core simulated scenarios. The OPS solution has the optimal results in both standard networking metrics of average response time and convergence duration compared to other standard solutions. It also has outstanding throughput, and average delay variation metrics with modest network traffic dropped metric results.

The irregular light-green hexagons in Figure 5.13 (b) presented that the average response time of the OPS solution at time  $t_0$  423 min with no failure event was 145 sec increased to 167 sec at  $t_2$  501 min in the first recovery event then closed to 150 sec after the second recovery at  $t_4$  1023 min but jumped to 200 sec at  $t_6$  1394 min within the last recovery event.

Furthermore, the OPS solution was accomplished the standard metric results of the average convergence duration over three recovery events at time  $t_2$  498 min,  $t_4$  1026 min, and  $t_6$  1394 min with one-to-one 368 sec grown tiny to the 371 sec but then again subsided to the 346 sec, as per light-green lines illustrated in Figure 5.13 (e).

On the other hand, the DVS solution has the optimal results in the throughput metric by 2554 Mb/sec at time  $t_1$  421 min in the first failure event; however, in the second failure event, the throughput rate was 2924 Mb/sec at  $t_3$  939 min, then it was lessened to 2475 Mb/sec at  $t_5$  1287 min. DVS results in this metric were shadowed with OPS solution results as disclosed via zigzag curves in Figure 5.13 (a) by 2340 Mb/sec pushed to 2733 Mb/sec before reduced 2424 Mb/sec.

Comparably, the red plotted curve of the LSS solution in Figure 5.13 (d) displayed its average delay variation results as the best one across other solutions followed by the OPS solution. At the time  $t_1$  427 min in the first failure event, the LSS delay was 17 sec while the OPS solution was 21 sec. Also, in the second failure event, the delay variation of the LSS escalated to 26 sec as well as the average delay of the OPS solution reached 31 sec at  $t_3$  937 min. Likewise, the average delay

variations of the LSS and OPS solutions were become more intense in the third failure event, too, at  $t_5$  1283 min by 35 sec and 40 sec, separately.

Correspondingly, Table 5.17 was indicated that the network traffic dropped results of the PRS solution were 1431 Mb/sec at time  $t_1$  426 min in the first failure event, 1667 Mb/sec at time  $t_3$  937 min in the second failure event, and 1834 Mb/sec at time  $t_5$  1284 min in last failure event.

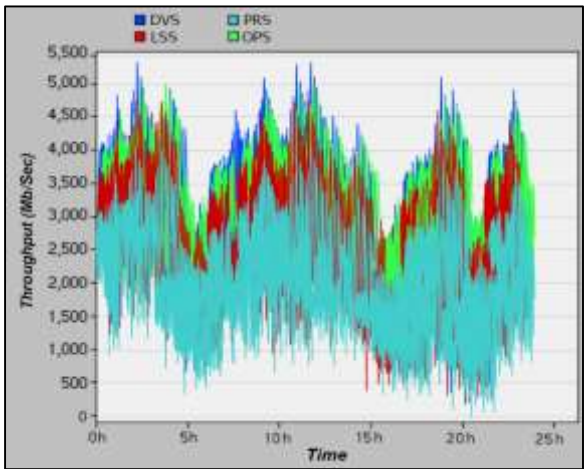
In place of the light-green peak illustrated in Figure 5.13 (c), the OPS solution was dropped network traffic by the rate of 2374 Mb/sec, 2818 Mb/sec, and 3121 Mb/sec over three failure events above within the same time frames. However, its network traffic dropped rate at time  $t_0$  425 min without failure event was 219 Mb/sec.

Table 5.18: Solutions Ranking of Optimized Simulation Results for the Core-Core Scenario

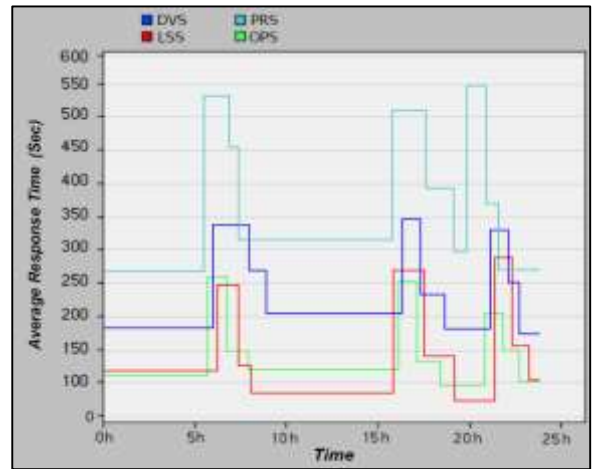
<i>Standard Simulation Networking Metrics</i>	<i>Dynamic Cyber Resilience Factors</i>	<i>Ranking of Dynamic Cyber Resilience Solutions</i>			
		<i>OPS</i>	<i>PRS</i>	<i>LSS</i>	<i>DVS</i>
<i>Throughput</i>	<i>Performance</i>	2	4	3	1
<i>Average Response Time</i>	<i>Recovery</i>	1	4	2	3
<i>Network Traffic Dropped</i>	<i>Absorption</i>	3	1	2	4
<i>Average Delay Variation</i>	<i>Volatility</i>	2	3	1	4
<i>Average Convergence Duration</i>	<i>Recovery Time</i>	1	3	4	2

The optimized simulation results for the core-core scenario have represented the ranking of the dynamic cyber resilience solutions regarding the dynamic cyber resilience factors based on the measured outputs of the standard simulation networking metrics clarified in Table 5.18.

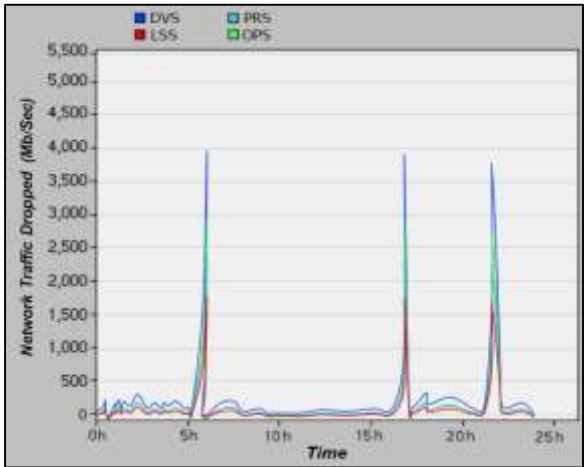
In conclusion, the OPS solution was achieved the first title in both the recovery and recovery time factors. It also has the second class in two factors: performance and volatility, while it was categorized third in the absorption factor compared to other standard solutions. In contrast, the PRS solution was classed first in the absorption factor as well as the LSS solution has the first-rate in the volatility factor, while the first position of the performance factor goes to the DVS solution.



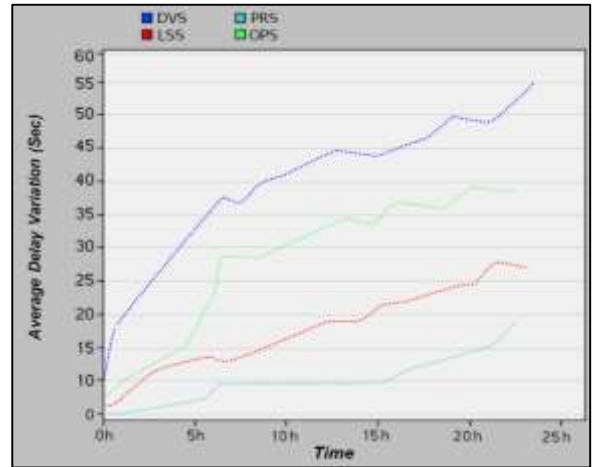
(a)



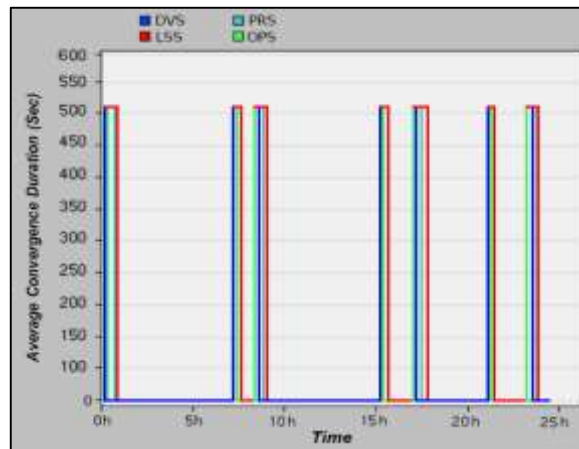
(b)



(c)



(d)



(e)

Figure 5.14: Optimized Results of OPNET Simulation for the Core-Edge Scenario  
 (a) Throughput (b) Average Response Time (c) Network Traffic Dropped  
 (d) Average Delay Variation (e) Average Convergence Duration

Table 5.19: Optimized Results of OPNET Simulation for the Core-Edge Scenario

Networking Metrics	OPNET Simulation			Dynamic Cyber Resilience Solutions			
	Event	Time (min)		OPS	PRS	LSS	DVS
Throughput (Mb/Sec)				No Cyber Attack			
	No Failure	$t_0$	0424	3984	2737	3500	4229
				First Cyber Attack			
	First Failure	$t_1$	0425	2783	1343	2404	2818
	First Recovery	$t_2$	0492	3666	2451	3228	4203
				Second Cyber Attack			
	Second Failure	$t_3$	0940	2348	1407	1993	2719
	Second Recovery	$t_4$	1026	3489	2382	2828	4004
				Third Cyber Attack			
	Third Failure	$t_5$	1289	2695	1129	1878	2643
	Third Recovery	$t_6$	1391	3638	2456	3334	4111
	Average Response Time (Sec)				No Cyber Attack		
No Failure		$t_0$	0422	0119	0278	0128	0182
			First Cyber Attack				
First Failure		$t_1$	0423	0258	0542	0246	0345
First Recovery		$t_2$	0493	0150	0459	0132	0277
			Second Cyber Attack				
Second Failure		$t_3$	0944	0252	0518	0275	0350
Second Recovery		$t_4$	1021	0140	0388	0145	0233
			Third Cyber Attack				
Third Failure		$t_5$	1285	0206	0550	0282	0336
Third Recovery		$t_6$	1392	0153	0374	0161	0250
Network Traffic Dropped (Mb/Sec)					No Cyber Attack		
	No Failure	$t_0$	0421	0133	0108	0092	0166
				First Cyber Attack			
	First Failure	$t_1$	0422	2983	2400	1750	3994
	First Recovery	$t_2$	0487	0106	0073	0051	0124
				Second Cyber Attack			
	Second Failure	$t_3$	0940	2981	2400	1750	3939
	Second Recovery	$t_4$	1021	0112	0099	0086	0163
				Third Cyber Attack			
	Third Failure	$t_5$	1288	2887	2289	1734	2768
	Third Recovery	$t_6$	1401	0101	0081	0063	0136
	Average Delay Variation (Sec)				No Cyber Attack		
No Failure		$t_0$	0426	0006	0001	0003	0010
			First Cyber Attack				
First Failure		$t_1$	0427	0028	0009	0013	0037
First Recovery		$t_2$	0495	0027	0005	0012	0036
			Second Cyber Attack				
Second Failure		$t_3$	0932	0034	0012	0021	0045
Second Recovery		$t_4$	1028	0033	0010	018	0044
			Third Cyber Attack				
Third Failure		$t_5$	1287	0038	0016	0028	0050
Third Recovery		$t_6$	1397	0032	0014	0024	0048
Average Convergence Duration (Sec)					No Cyber Attack		
	No Failure	$t_0$	0421	0310	0369	0422	0305
				First Cyber Attack			
	First Failure	$t_1$	0422	0445	0419	0478	0443
	First Recovery	$t_2$	0491	0338	0383	0430	0346
				Second Cyber Attack			
	Second Failure	$t_3$	0940	0468	0412	0482	0463
	Second Recovery	$t_4$	1024	0342	0367	0426	0354
				Third Cyber Attack			
	Third Failure	$t_5$	1282	0465	0416	0466	0461
	Third Recovery	$t_6$	1396	0303	0363	0427	0316

The OPS solution in the core-edge scenario also has the optimal results in both standard metrics of the average response time and average convergence duration compared with other standard solutions. For example, at the time of  $t_1$  423 min, the response time of the OPS solution was 258 sec after the first failure event and 252 sec in the second failure event at  $t_3$  944 min; however, its response time was 206 sec at  $t_5$  1285 min in the third failure event. At the same time, LSS has an average response time over the previous three failure events of 246 sec, 275 sec, and 282 sec, singly, as irregular hexagon curves illustrated in red and light-green colors within Figure 5.14 (b). In Table 5.19, the average convergence duration outputs of the OPS solution were ranged between 310 sec at time  $t_0$  421 min in the starting point with no failure event to reach 303 sec at  $t_6$  1396 min in the third recovery event passing by 338 sec at  $t_2$  491 min and 342 sec at  $t_4$  1024 min in the first and second recovery events. These results compared the average convergence duration of the DVS solution, completed 346 sec, 354 sec, and 316 sec across the first, second and last recovery events as per blue lines shown in Figure 5.14 (e).

Moreover, the blue zigzag curve of the DVS solution throughput in Figure 5.14 (a) demonstrated that it has the optimal results achieved in this standard simulation networking metric followed by the OPS solution results with the light-green zigzag curve. The DVS throughput rate was the highest by 2818 Mb/sec at the time  $t_1$  425 min afterward the first failure event, but the throughput rate of the OPS solution at the same time was 2783 Mb/sec. Likewise, the DVS throughput was 2719 Mb/sec in the second failure event at  $t_3$  940 min with the rate of 2348 Mb/sec for the OPS solution. Finally, in the last failure event at  $t_5$  1289 min, the throughput rates of both DVS and the OPS solutions were closed to 2643 Mb/sec and 2695 Mb/sec, separately.

The latter two standard metrics results of the network traffic dropped, and average delay variation was modest for the OPS solution contrasted to the LSS red peak curve presented in Figure 5.14

(c), and the PRS dark-green curve plotted in Figure 5.14 (d). Both standard solutions succeeded to attain the optimal results in these metrics as follows: 1750 Mb/sec the dropped rate of the network traffic for the LSS solution during the first and second failure events at  $t_1$  422 min and  $t_3$  940 min, individually, even so, in the remaining failure event at  $t_5$  1288 min the LSS traffic dropped decreased by 1734 Mb/sec.

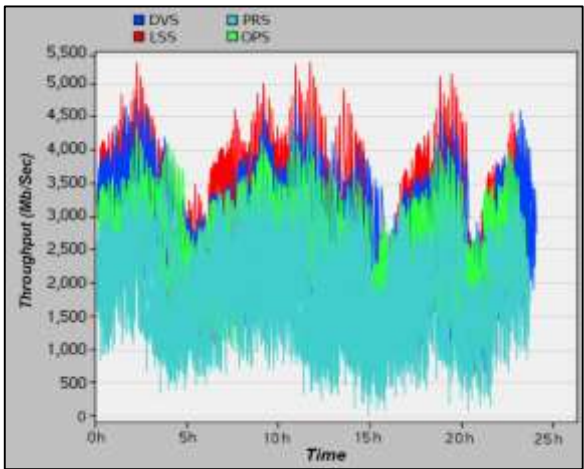
On the other hand, the average delay variation outputs of the PRS solution were 1 sec with no failure event at the initial time  $t_0$  426 min increased to the 9 sec in the first failure time at  $t_1$  427 min then increased again to stretch to 12 sec at  $t_3$  932 min in the second failure time and finally extended to 16 sec in the latest failure event at  $t_5$  1287 min. Indeed, results of the OPS solution in these two standard metrics were 2983 Mb/sec, 2981 Mb/sec, and 2887 Mb/sec for its network traffic dropped rate for a period of three failure events, as made known in Table 5.17, in parallel with its average delay variation over the failure events to access alone 28 sec, 34 sec, and 38 sec.

Table 5.20: Solutions Ranking of Optimized Simulation Results for the Core-Edge Scenario

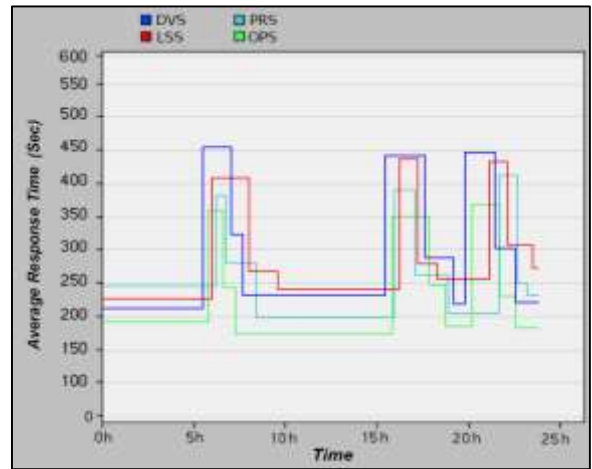
<i>Standard Simulation Networking Metrics</i>	<i>Dynamic Cyber Resilience Factors</i>	<i>Ranking of Dynamic Cyber Resilience Solutions</i>			
		<i>OPS</i>	<i>PRS</i>	<i>LSS</i>	<i>DVS</i>
<i>Throughput</i>	<i>Performance</i>	2	4	3	1
<i>Average Response Time</i>	<i>Recovery</i>	1	4	2	3
<i>Network Traffic Dropped</i>	<i>Absorption</i>	3	2	1	4
<i>Average Delay Variation</i>	<i>Volatility</i>	3	1	2	4
<i>Average Convergence Duration</i>	<i>Recovery Time</i>	1	3	4	2

In Table 5.20, the concluding ranking of the dynamic cyber resilience solutions in the dynamic cyber resilience factors through the core-edge scenario is based on the standard simulation networking metrics. The OPS solution has first grades in two factors, recovery and recovery time factors than other standard solutions. It was categorized second in the performance factor and third in the rest factors of the absorption and volatility factors. The LSS, PRS, and DVS solutions individually have the first levels in absorption, volatility, and performance factors.

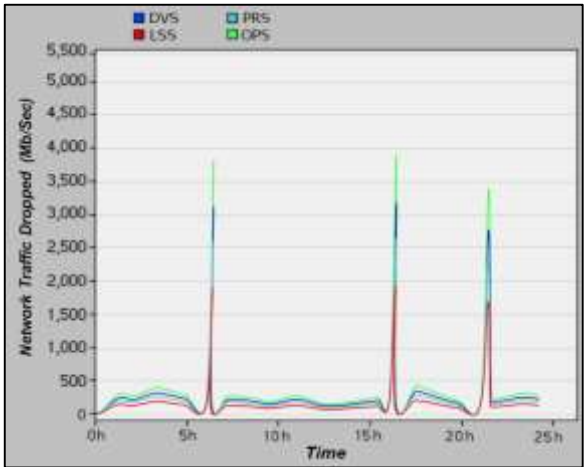




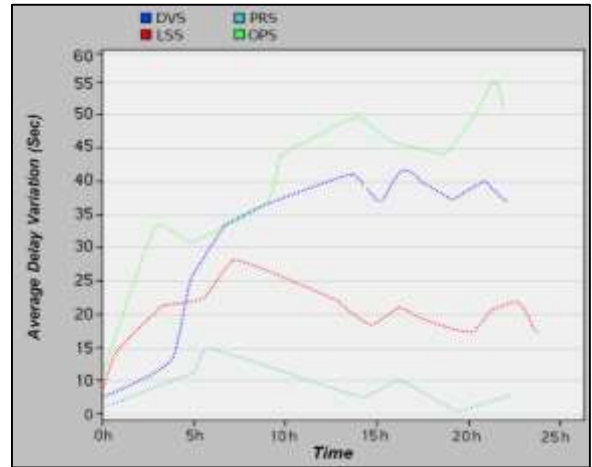
(a)



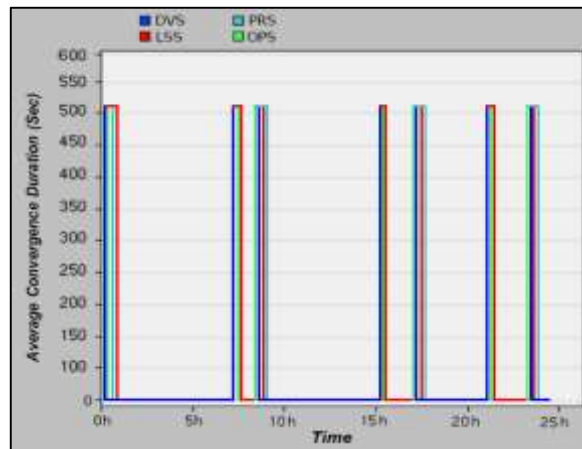
(b)



(c)



(d)



(e)

Figure 5.15: Optimized Results of OPNET Simulation for the Edge-Edge Scenario

(a) Throughput (b) Average Response Time (c) Network Traffic Dropped

(d) Average Delay Variation (e) Average Convergence Duration

Table 5.21: Optimized Results of OPNET Simulation for the Edge-Edge Scenario

Networking Metrics	OPNET Simulation			Dynamic Cyber Resilience Solutions			
	Event	Time (min)		OPS	PRS	LSS	DVS
Throughput (Mb/Sec)				No Cyber Attack			
	No Failure	$t_0$	0420	3107	2453	4199	3659
				First Cyber Attack			
	First Failure	$t_1$	0421	2388	1263	3000	2534
	First Recovery	$t_2$	0492	3126	2421	4120	3803
				Second Cyber Attack			
	Second Failure	$t_3$	0939	2471	1012	2525	2635
	Second Recovery	$t_4$	1023	3062	2204	4005	3582
				Third Cyber Attack			
	Third Failure	$t_5$	1294	2456	1237	2507	2468
Third Recovery	$t_6$	1389	3155	2424	3824	3619	
Average Response Time (Sec)				No Cyber Attack			
	No Failure	$t_0$	0425	0192	0246	0237	0218
				First Cyber Attack			
	First Failure	$t_1$	0426	0355	0372	0415	0456
	First Recovery	$t_2$	0488	0242	0275	0265	0324
				Second Cyber Attack			
	Second Failure	$t_3$	0947	0350	0380	0440	0441
	Second Recovery	$t_4$	1014	0250	0263	0286	0393
				Third Cyber Attack			
	Third Failure	$t_5$	1293	0373	0422	0432	0450
Third Recovery	$t_6$	1387	0233	0250	0312	0300	
Network Traffic Dropped (Mb/Sec)				No Cyber Attack			
	No Failure	$t_0$	0426	0317	0215	0168	0272
				First Cyber Attack			
	First Failure	$t_1$	0427	3840	2603	1925	3114
	First Recovery	$t_2$	0483	0326	0224	0176	0288
				Second Cyber Attack			
	Second Failure	$t_3$	0946	3856	2616	1953	3154
	Second Recovery	$t_4$	1019	0333	0247	0181	0292
				Third Cyber Attack			
	Third Failure	$t_5$	1285	3465	2314	1678	2734
Third Recovery	$t_6$	1395	0341	0253	0188	0297	
Average Delay Variation (Sec)				No Cyber Attack			
	No Failure	$t_0$	0426	0012	0002	0008	0006
				First Cyber Attack			
	First Failure	$t_1$	0427	0034	0015	0027	0033
	First Recovery	$t_2$	0491	0031	0011	0023	0025
				Second Cyber Attack			
	Second Failure	$t_3$	0936	0050	0010	0021	0041
	Second Recovery	$t_4$	1024	0044	0006	0017	0037
				Third Cyber Attack			
	Third Failure	$t_5$	1286	0055	0005	0020	0043
Third Recovery	$t_6$	1397	0051	0001	0016	0048	
Average Convergence Duration (Sec)				No Cyber Attack			
	No Failure	$t_0$	0429	0289	0334	0300	0281
				First Cyber Attack			
	First Failure	$t_1$	0430	0325	0390	0360	0308
	First Recovery	$t_2$	0494	0290	0369	0318	0301
				Second Cyber Attack			
	Second Failure	$t_3$	0941	0334	0391	0361	0320
	Second Recovery	$t_4$	1026	0305	0346	0315	0312
				Third Cyber Attack			
	Third Failure	$t_5$	1284	0343	0376	0347	0335
Third Recovery	$t_6$	1395	0321	0348	0320	0324	

Table 5.19 above presented the results of the OPNET simulations for the dynamic cyber resilience solutions in the edge-edge scenario during the optimization research phase. Like the previous core-core and the core-edge scenarios, the OPS solution optimal results in the average response time and convergence duration metrics measured up to other standard solutions.

It was realized that a response time of 355 sec at the simulation time  $t_1$  426 min in the course of the first failure event lessened to 350 sec upon the second failure event at  $t_3$  947 min then turned up again 373 sec at  $t_5$  1293 min. Thus, the average response time outputs of the PRS solution followed the OPS solution ones by the 372 sec, 380 sec, and 422 sec crosswise the failures caused by the wave of the concurrent and consecutive cyberattacks, as per light and dark green irregular curves appeared in Figure 5.15 (b).

Besides, the results of the average convergence duration in Figure 5.15 (e) revealed that the OPS solution was succeeded to attain its convergence duration ranged between 290 sec to 321 sec, passing by 305 sec over three recovery events at time  $t_2$  494 min,  $t_4$  1026 min, and  $t_6$  1395 min contested with the second-optimal results done by the DVS solution in the same standard metric and time frames that closed to 301 sec in the first recovery event, 312 sec thru the second one. Last of all ended with 324 sec.

The red zigzag curve in Figure 5.15 (a) and the red peak curve in Figure 5.15 (c) indicated that LSS was completed the optimal results of the throughput metric and network traffic dropped metric than other solutions while OPS solution has inconsiderable results in these two metrics.

The LSS solution has initiated the throughput by 4199 Mb/sec at  $t_0$  420 min with no failure event. However, its throughput results have fluctuated relatively near initial one by 4120 Mb/sec in the first recovery event at  $t_2$  492 min, reduced to 4005 Mb/sec at  $t_4$  1023 min in the second recovery event, then again was cut at  $t_6$  1389 min by 3824 Mb/sec in the prior recovery event.

On the contrary, the throughput results of the OPS solution were 3126 Mb/sec, 3062 Mb/sec, and 3155 Mb/sec across the preceding recovery events. Moreover, the LSS solution was dropped the amount of network traffic by the rate of 1925 Mb/sec in the earliest failure event at  $t_1$  427 min, slightly increased by 1953 Mb/sec at  $t_3$  946 min in the next failure event, then dramatically decreased by 1678 Mb/sec in the third failure event at  $t_5$  1285 min. Along the same lines, the OPS solution was dropped traffic off by 3840 Mb/sec, 3856 Mb/sec, and 3465 Mb/sec.

On the other hand, the PRS solution outputs plotted in Figure 5.15 (d) denoted that its average delay variation was the lowest than other solutions, especially the OPS solution. After the first cyberattack, the PRS solution delay was 15 sec at  $t_1$  427 min, shrunken to 10 sec at  $t_3$  936 min in the next cyberattack down to 5 sec in the final cyberattack  $t_5$  1286 min. The average OPS solution delay variations were 34 sec, 50 sec, and in the end, 55 sec.

Table 5.22: Solutions Ranking of Optimized Simulation Results for the Edge-Edge Scenario

<i>Standard Simulation Networking Metrics</i>	<i>Dynamic Cyber Resilience Factors</i>	<i>Ranking of Dynamic Cyber Resilience Solutions</i>			
		<i>OPS</i>	<i>PRS</i>	<i>LSS</i>	<i>DVS</i>
<i>Throughput</i>	<i>Performance</i>	3	4	1	2
<i>Average Response Time</i>	<i>Recovery</i>	1	2	3	4
<i>Network Traffic Dropped</i>	<i>Absorption</i>	4	2	1	3
<i>Average Delay Variation</i>	<i>Volatility</i>	4	1	2	3
<i>Average Convergence Duration</i>	<i>Recovery Time</i>	1	4	3	2

In Table 5.22, the optimized simulation results surfaced. The OPS solution ranks first in the recovery factor and recovery time factor related to standard solutions through the edge-edge scenario like the core-core and the core-edge scenarios. The rankings of the OPS solution in the rest factors were the third status in performance factor and the last classes in two factors of the absorption and volatility rather than other solutions. In opposite, LSS was placed first in both performance and absorption factors, even as the first place of the volatility factor goes to PRS; nevertheless, DVS has no first rank in any dynamic cyber resilience factors.

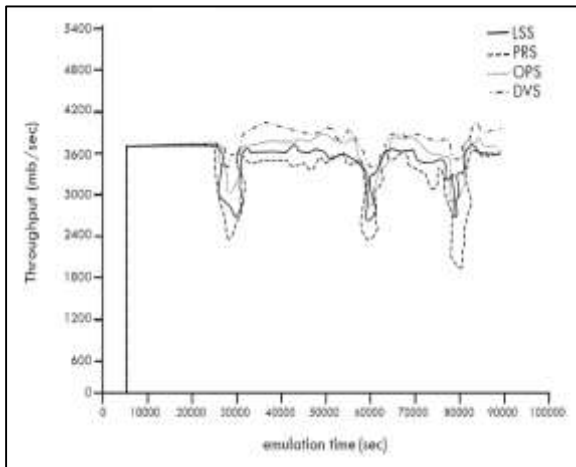
## 5.2 Optimized Results Analysis of Emulated Experiments

The experimental emulations were similarly implemented with frequent testing scenarios to validate the data accumulated and investigated by the computing simulations. These investigating emulations consist of core-core, core-edge, and edge-edge scenarios.

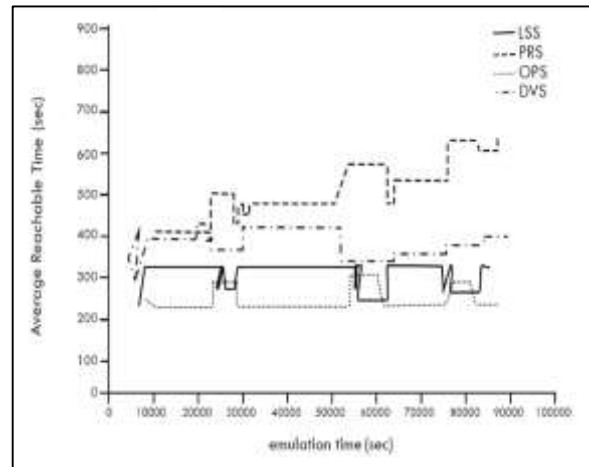
Above and beyond, an established set of standard emulation metrics was used to measure and gather the experimental optimized results include the networking ones deliberated in Chapter 4 as follows: throughput, average reachable time, network traffic lost, average end-to-end delay, and average convergence duration were conforming with the standard simulation metrics.

Characteristically, each standard networking metric treated in the emulation scenarios was reporting the given quantities to assess dynamic cyber resilience factors that evaluate correlated capabilities of the optimized proposed solution (OPS), and other standard solutions incorporate path-rule solution (PRS), link-state solution (LSS), and distance-vector solution (DVS) through three waves of the concurrent and consecutive cyberattacks within particular timelines.

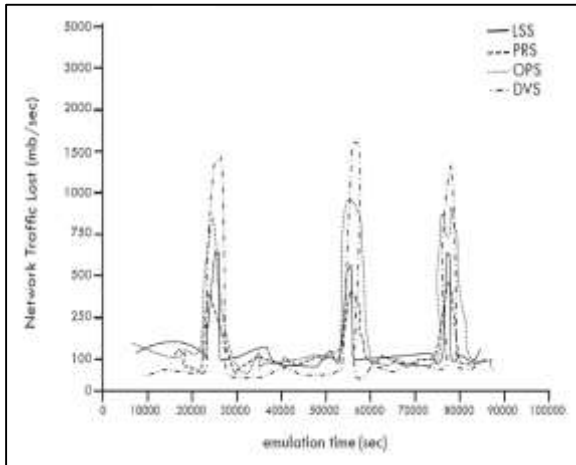
Below, the optimized results of the GNS3 emulations for the core-core scenario represented in Table 5.23 ensured that the OPS solution results were the best in the average reachable time metric and the average convergence duration metric competed with the standard solutions. The dotted lines of the OPS solution in Figure 5.16 (b) illuminated that its reachable time in the first failure event was 294 sec at  $t_1$  426 min contrasted with the 222 sec in the case of no failure at  $t_0$  425 min. Also, the average reachable time for the OPS solution improved to 303 sec in the next failure event at  $t_3$  942 min before it was declined to get in touch with 277 sec at  $t_5$  1286 min after the latter cyberattack event occurred. In differing, the reachable time outputs of the LSS were confined by 327 sec, 328 sec, and 322 sec in that order upon the identical failure events.



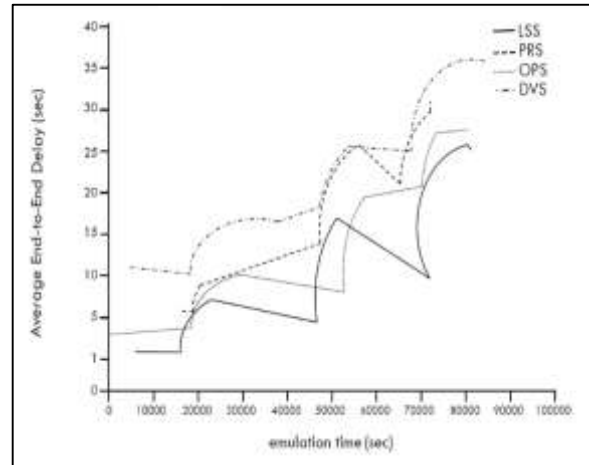
(a)



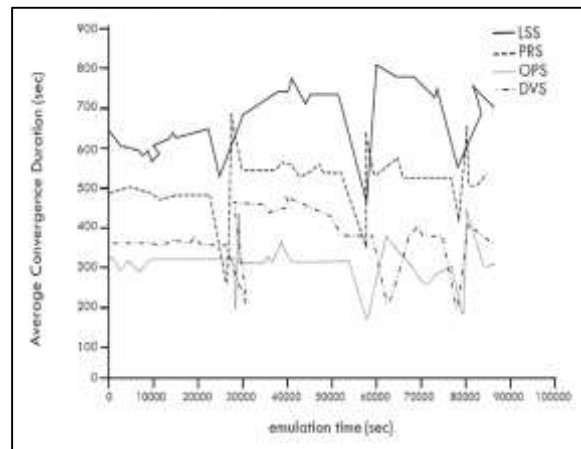
(b)



(c)



(d)



(e)

Figure 5.16: Optimized Results of GNS3 Emulation for the Core-Core Scenario  
 (a) Throughput (b) Average Reachable Time (c) Network Traffic Lost  
 (d) Average End-to-End Delay (e) Average Convergence Duration

Table 5.23: Optimized Results of GNS3 Emulation for the Core-Core Scenario

Networking Metrics	GNS3 Emulation			Dynamic Cyber Resilience Solutions			
	Event	Time (min)		OPS	PRS	LSS	DVS
Throughput (Mb/sec)				No Cyber Attack			
	No Failure	$t_0$	0424	3657	3609	3634	3683
				First Cyber Attack			
	First Failure	$t_1$	0425	3021	2392	2641	3459
	First Recovery	$t_2$	0489	3772	3561	3606	4083
				Second Cyber Attack			
	Second Failure	$t_3$	0928	2882	2398	2605	3521
	Second Recovery	$t_4$	1020	3718	3314	3627	3957
				Third Cyber Attack			
	Third Failure	$t_5$	1284	2934	1985	2636	3585
	Third Recovery	$t_6$	1392	3613	3604	3608	4129
	Average Reachable Time (sec)				No Cyber Attack		
No Failure		$t_0$	0425	0222	0408	0323	0400
			First Cyber Attack				
First Failure		$t_1$	0426	0294	0500	0327	0421
First Recovery		$t_2$	0491	0224	0488	0284	0375
			Second Cyber Attack				
Second Failure		$t_3$	0942	0303	0587	0328	0362
Second Recovery		$t_4$	1020	0223	0524	0258	0343
			Third Cyber Attack				
Third Failure		$t_5$	1286	0277	0618	0322	0396
Third Recovery		$t_6$	1394	0225	0603	0273	0387
Network Traffic Lost (Mb/sec)					No Cyber Attack		
	No Failure	$t_0$	0421	0146	0088	0156	0058
				First Cyber Attack			
	First Failure	$t_1$	0422	0832	0352	0651	1490
	First Recovery	$t_2$	0481	0122	0108	0134	0062
				Second Cyber Attack			
	Second Failure	$t_3$	0934	0989	0436	0538	1608
	Second Recovery	$t_4$	1022	0134	0117	0129	0091
				Third Cyber Attack			
	Third Failure	$t_5$	1285	0814	0474	0668	1411
	Third Recovery	$t_6$	1397	0126	0093	0127	0083
	Average End-to-End Delay (sec)				No Cyber Attack		
No Failure		$t_0$	0425	0003	0006	0002	0011
			First Cyber Attack				
First Failure		$t_1$	0426	0010	0009	0007	0016
First Recovery		$t_2$	0496	0004	0005	0002	0010
			Second Cyber Attack				
Second Failure		$t_3$	0933	0020	0026	0017	0025
Second Recovery		$t_4$	1023	0008	0014	0005	0019
			Third Cyber Attack				
Third Failure		$t_5$	1285	0037	0029	0025	0035
Third Recovery		$t_6$	1397	0021	0021	0009	0025
Average Convergence Duration (sec)					No Cyber Attack		
	No Failure	$t_0$	0424	0328	0495	0634	0372
				First Cyber Attack			
	First Failure	$t_1$	0425	0200	0266	0522	0208
	First Recovery	$t_2$	0491	0437	0696	0731	0474
				Second Cyber Attack			
	Second Failure	$t_3$	0942	0184	0370	0472	0223
	Second Recovery	$t_4$	1028	0362	0643	0818	0391
				Third Cyber Attack			
	Third Failure	$t_5$	1282	0178	0426	0563	0211
	Third Recovery	$t_6$	1403	0404	0666	0778	0442

The dotted zigzag curve in Figure 5.16 (e) was put on view the optimal results of the average convergence duration metric for the OPS solution were started on  $t_0$  424 min with 328 sec earlier any failure event happened, at the same time as the DVS solution was ongoing with 327 sec. In the foremost recovery event at  $t_2$  491 min, the convergence duration was 437 sec for the OPS solution and 474 sec for the DVS solution, later subsided at  $t_4$  1028 min for both solutions to become 362 sec and 391 sec of the average convergence for the OPS and DVS solutions correspondingly in the subsequent recovery event. However, the convergence output of the OPS solution was extended to 404 sec in the third recovery event at  $t_6$  1403 min; likewise, for the DVS solution, its final output was jumped up from 391 sec towards 442 sec.

In this core-core scenario, the optimized results of the OPS solution were successful in turning out the second-best ones in two standard emulation metrics of the throughput and average end-to-end delay among the tested solutions of the dynamic cyber resilience; these optimized results achieved comparable the primary results that obtained previously.

In the first recovery event at emulation time  $t_2$  489 min, the OPS throughput was 3772 Mb/sec per the drooping dotted curve demonstrated in Figure 5.16 (a), likened to the best throughput results of the DVS solution with 4083 Mb/sec. At  $t_4$  1020 min in the second recovery event, the throughput outputs of the OPS and DVS solutions were in that order by 3718 Mb/sec and 3957 Mb/sec; these outputs were different between both solutions through the third recovery event at  $t_6$  1392 min whereas dropping off by 3613 Mb/sec for OPS solution and per contra rated by 4129 Mb/sec for the DVS solution.

Regarding the metric results of the average end-to-end delay for the OPS solution and the LSS solution based on the solid and dotted stairs curved in Figure 5.16 (d) that showed the delay of the OPS solution at time  $t_1$  426 min was 10 sec while it was 7 sec for the LSS solution in the first



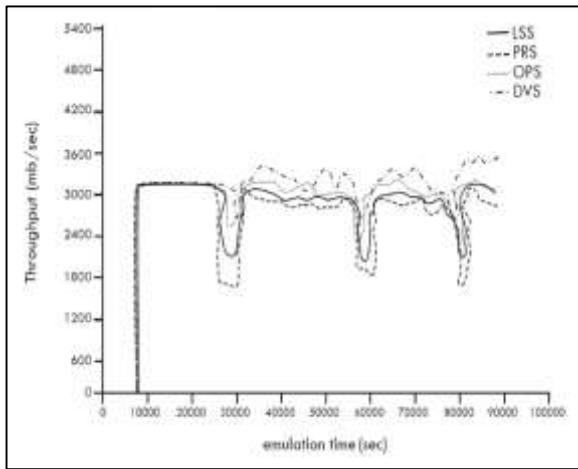
failure event. In parallel, the average delays in the next failure event were 20 sec and 17 sec at  $t_3$  933 min for the OPS and LSS solutions, respectively. Finally, at  $t_5$  1285 min, the end-to-end delay of the OPS solution was 37 sec in the remaining failure event, and it was 35 sec for LSS. On the other hand, the OPS solution was lost network traffic at the rate of 832 Mb/sec at  $t_1$  422 min and 352 Mb/sec by the PRS solution after the first cyberattack. The dotted and dashed peaks in Figure 5.16 (c) revealed that the amount of the packets lost during the second failure event was increased for both OPS and PRS solutions by 989 Mb/sec at  $t_3$  934 min and in turn 538 Mb/sec. To end, the rate of the network traffic loss of the OPS solution in the third failure event at  $t_5$  1285 min was 814 Mb/sec, even though the traffic loss rate of the PRS solution was 474 Mb/sec.

Table 5.24: Solutions Ranking of Optimized Emulation Results for the Core-Core Scenario

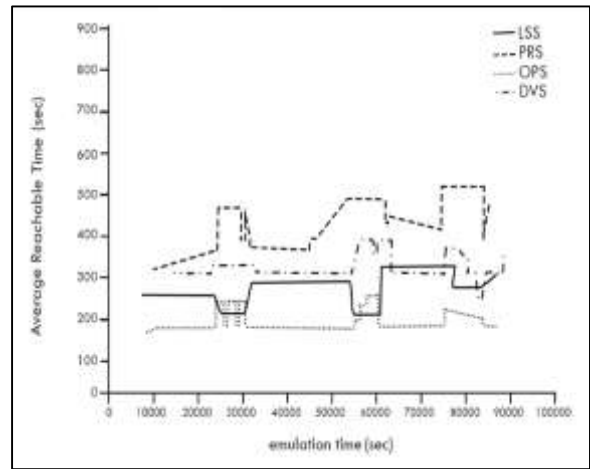
<i>Standard Emulation Networking Metrics</i>	<i>Dynamic Cyber Resilience Factors</i>	<i>Ranking of Dynamic Cyber Resilience Solutions</i>			
		<i>OPS</i>	<i>PRS</i>	<i>LSS</i>	<i>DVS</i>
<i>Throughput</i>	<i>Performance</i>	2	4	3	1
<i>Average Reachable Time</i>	<i>Recovery</i>	1	4	2	3
<i>Network Traffic Lost</i>	<i>Absorption</i>	3	1	2	4
<i>Average End-to-End Delay</i>	<i>Volatility</i>	2	3	1	4
<i>Average Convergence Duration</i>	<i>Recovery Time</i>	1	3	4	2

Table 5.24 concluded the ranking of the OPS solution on the basis of the optimized emulation results over the core-core scenario according to other standard solutions. In the recovery factor and recovery time factor, the OPS solution was rated the first in both of them, while it was positioned second in the performance and volatility factors; nevertheless, the OPS position in the absorption factor was the third one.

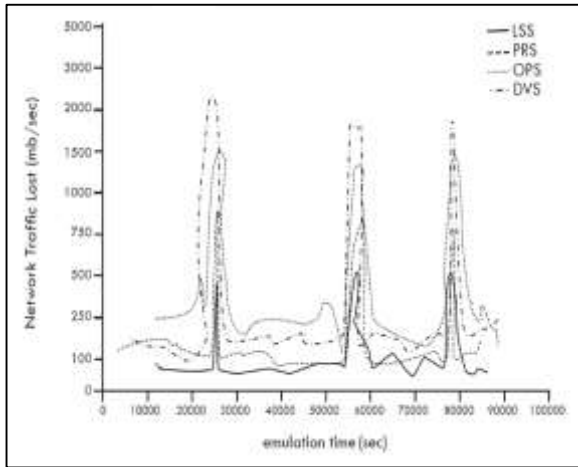
Generally, the PRS, LSS, and DVS standard solutions were classed first in the absorption factor, volatility factor, and performance factor separately. Besides, LSS solution was arranged second in recovery factor and absorption factor. The DVS also was graded second in the recovery time factor. Still, the PRS solution was not rated first or second in any dynamic cyber resilience factor.



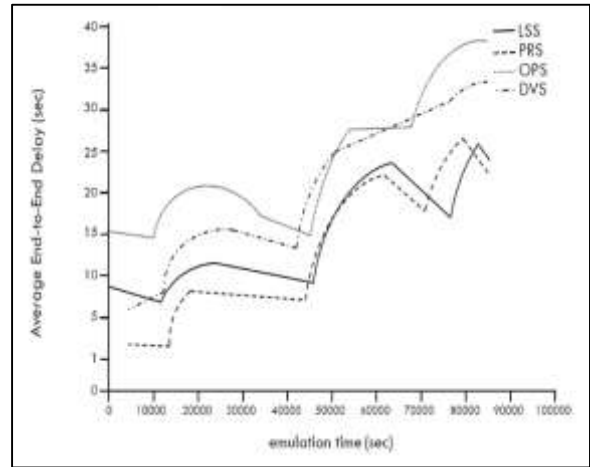
(a)



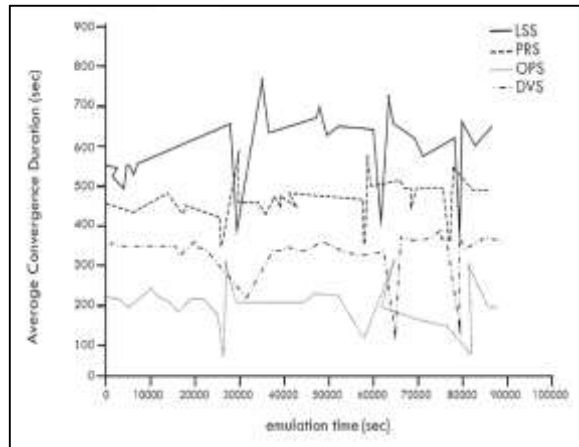
(b)



(c)



(d)



(e)

Figure 5.17: Optimized Results of GNS3 Emulation for the Core-Edge Scenario

(a) Throughput (b) Average Reachable Time (c) Network Traffic Lost

(d) Average End-to-End Delay (e) Average Convergence Duration

Table 5.25: Optimized Results of GNS3 Emulation for the Core-Edge Scenario

Networking Metrics	<u>GNS3 Emulation</u>			<u>Dynamic Cyber Resilience Solutions</u>			
	Event	Time (min)		OPS	PRS	LSS	DVS
Throughput (Mb/sec)	No Cyber Attack						
	No Failure	$t_0$	0421	3212	3158	3188	3264
	First Cyber Attack						
	First Failure	$t_1$	0422	2542	1775	2166	2617
	First Recovery	$t_2$	0492	3107	2954	3012	3654
	Second Cyber Attack						
	Second Failure	$t_3$	0940	2395	1835	2059	2633
	Second Recovery	$t_4$	1023	3076	2888	3027	3714
	Third Cyber Attack						
	Third Failure	$t_5$	1288	2315	1788	2116	2633
Third Recovery	$t_6$	1394	3050	2919	3110	3527	
Average Reachable Time (sec)	No Cyber Attack						
	No Failure	$t_0$	0423	0183	0313	0273	0316
	First Cyber Attack						
	First Failure	$t_1$	0424	0235	0327	0281	0484
	First Recovery	$t_2$	0490	0182	0310	0212	0378
	Second Cyber Attack						
	Second Failure	$t_3$	0940	0256	0385	0301	0500
	Second Recovery	$t_4$	1013	0185	0302	0205	0422
	Third Cyber Attack						
	Third Failure	$t_5$	1282	0237	0384	0296	0519
Third Recovery	$t_6$	1382	0188	0307	0308	0406	
Network Traffic Lost (Mb/sec)	No Cyber Attack						
	No Failure	$t_0$	0428	0250	0173	0083	0193
	First Cyber Attack						
	First Failure	$t_1$	0429	1500	0866	0457	2313
	First Recovery	$t_2$	0488	0242	0162	0093	0201
	Second Cyber Attack						
	Second Failure	$t_3$	0942	1373	0829	0500	1885
	Second Recovery	$t_4$	1021	0237	0157	0106	0196
	Third Cyber Attack						
	Third Failure	$t_5$	1284	1460	0724	0492	1916
Third Recovery	$t_6$	1399	0282	0138	0081	0211	
Average End-to-End Delay (sec)	No Cyber Attack						
	No Failure	$t_0$	0427	0005	0002	0004	0011
	First Cyber Attack						
	First Failure	$t_1$	0428	0014	0007	0008	0017
	First Recovery	$t_2$	0496	0012	0003	0003	0012
	Second Cyber Attack						
	Second Failure	$t_3$	0930	0020	0020	0021	0027
	Second Recovery	$t_4$	1024	0012	0006	0010	0023
	Third Cyber Attack						
	Third Failure	$t_5$	1286	0035	0027	0030	0038
Third Recovery	$t_6$	1396	0025	0020	0025	0028	
Average Convergence Duration (sec)	No Cyber Attack						
	No Failure	$t_0$	0428	0334	0463	0588	0357
	First Cyber Attack						
	First Failure	$t_1$	0429	0082	0356	0385	0234
	First Recovery	$t_2$	0493	0303	0596	0777	0326
	Second Cyber Attack						
	Second Failure	$t_3$	0936	0108	0352	0400	0125
	Second Recovery	$t_4$	1016	0308	0584	0716	0300
	Third Cyber Attack						
	Third Failure	$t_5$	1284	0078	0355	0376	0087
Third Recovery	$t_6$	1391	0291	0557	0669	0289	

Based on the optimized results were available via the standard metrics of the average reachable time and the average convergence duration in Table 5.25 confirmed by the irregular dotted line in Figure 5.17 (b) and dotted zigzag curve in Figure 5.17 (e) lightened that the OPS solution also has the best outputs in these two metrics than other standard solutions throughout the core-edge scenario like the core-core scenario in the optimization phase.

At emulation time  $t_1$  424 min, the reachable time of the OPS solution over the first failure event was 235 sec enlarged to 256 sec at  $t_3$  940 min in next failure event then returned back again to 237 sec in the finishing failure event at  $t_5$  1282 min. As well, the convergence duration of the OPS solution across three recovery events at timeframes of  $t_2$  493 min,  $t_4$  1016 min, and  $t_6$  1391 min were begun with 303 sec in the number one of these events pushed to 308 sec in the second one and formerly retreated to 291 sec during the final recovery event.

Back to the OPS solution results in the remaining networking metrics as appeared in Figure 5.17 (a) concerning the throughput, and Figure 5.17 (c) and Figure 5.17 (d) regarding the network traffic lost and average end-to-end delay correspondingly, it was pulled off throughput by 3107 Mb/sec at  $t_2$  492 min in the first recovery event, decreased by 3076 Mb/sec in following an event of the recovery at  $t_4$  1023 min, moved to the end recovery event at  $t_6$  1394 min by 3050 Mb/sec.

Moreover, the OPS solution was lost network traffic by 1500 Mb/sec at  $t_1$  429 min in the first failure event, before dropped off by 1373 Mb/sec at  $t_3$  942 min in the second failure event, knowing that was lost the network traffic by the rate of 1284 Mb/sec in the third failure event. Furthermore, it has an average end-to-end delay with 14 sec, 20 sec, and 35 sec over three failure events in that order at  $t_1$  428 min,  $t_3$  930 min, and  $t_5$  1286 min.

Otherwise, the optimal results of the rest standard metrics were the share of other standard solutions distributed evenly among them, whereas the PRS solution has the lowest average end-

to-end delay through 7 sec, 20 sec, and 27 sec in addition to the LSS solution, was lost the lowest network traffic across the previous failure events by 457 Mb/sec, 500 Mb/sec, and 492 Mb/sec. In the end, the highest throughput that went to the DVS solution was 2617 Mb/sec, 2633 Mb/sec, and again 2633 Mb/sec thru the first, second, and third failures.

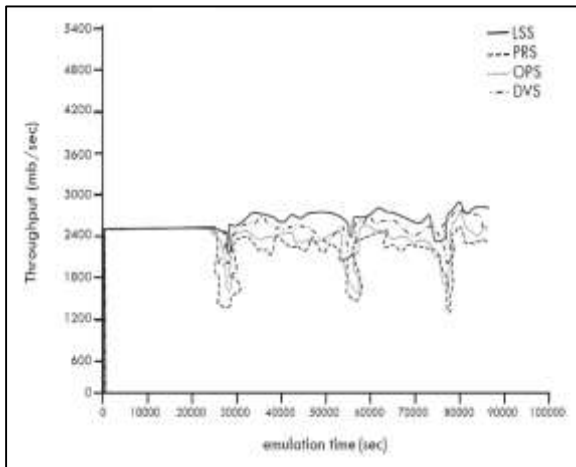
Table 5.26: Solutions Ranking of Optimized Emulation Results for the Core-Edge Scenario

<i>Standard Emulation Networking Metrics</i>	<i>Dynamic Cyber Resilience Factors</i>	<i>Ranking of Dynamic Cyber Resilience Solutions</i>			
		<i>OPS</i>	<i>PRS</i>	<i>LSS</i>	<i>DVS</i>
<i>Throughput</i>	<i>Performance</i>	2	4	3	1
<i>Average Reachable Time</i>	<i>Recovery</i>	1	4	2	3
<i>Network Traffic Lost</i>	<i>Absorption</i>	3	2	1	4
<i>Average End-to-End Delay</i>	<i>Volatility</i>	3	1	2	4
<i>Average Convergence Duration</i>	<i>Recovery Time</i>	1	3	4	2

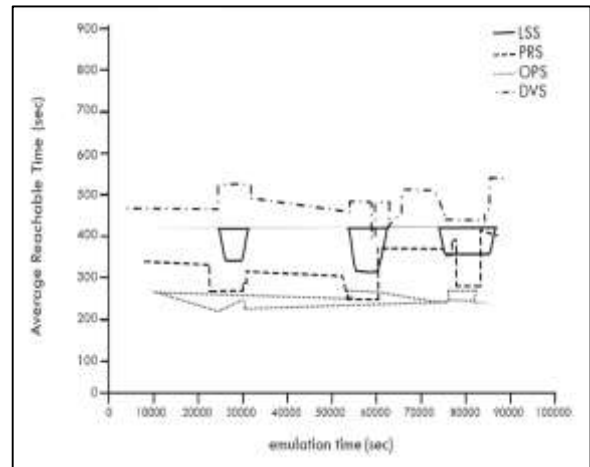
The ranking of the dynamic cyber resilience solutions was different considering the dynamic cyber resilience factors resulting from the standard emulation networking metrics throughout the core-edge scenario, as represented in Table 5.26 above. Therefore, the optimized results have supported the categorizing of the OPS solution contrasted to the other standard solutions.

Therefore, the OPS solution was tiered first in the recovery factor and recovery time factor; note that it was also classified the first in these two factors in the previous core-core scenario. Additionally, the OPS solution was ordered second via this scenario in the performance factor and third in absorption and volatility factors.

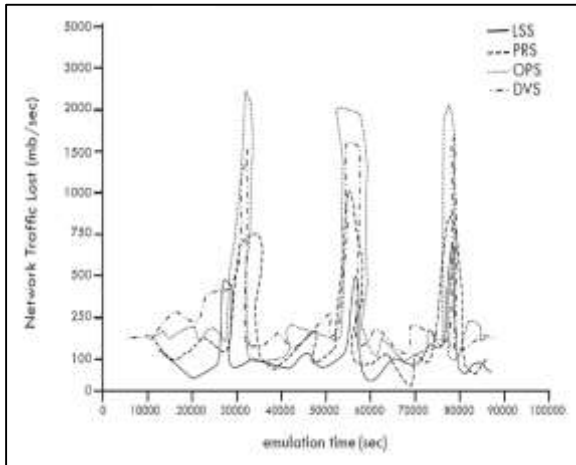
On the other hand, the standard solutions have first been categorized in three dynamic cyber resilience factors, whereas the DVS solution has the first class in the performance factor in this scenario and the aforementioned core-core scenario. In comparison, the LSS solution was placed first in the absorption factor using the core-edge scenario, while it was classified first in the volatility factor within the core-core scenario. After all, individually, PRS has the first volatility factor and absorption factor in core-edge and core-core scenarios.



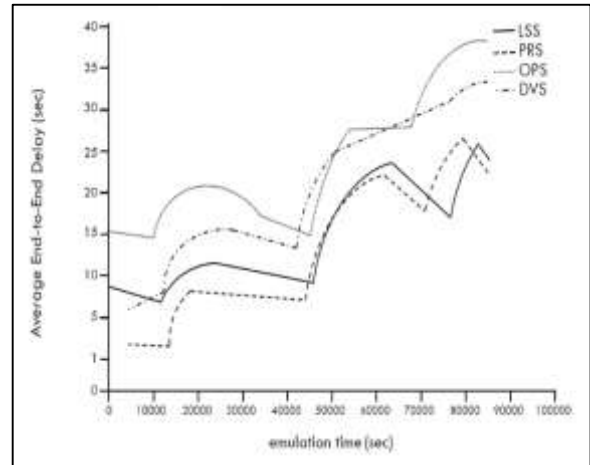
(a)



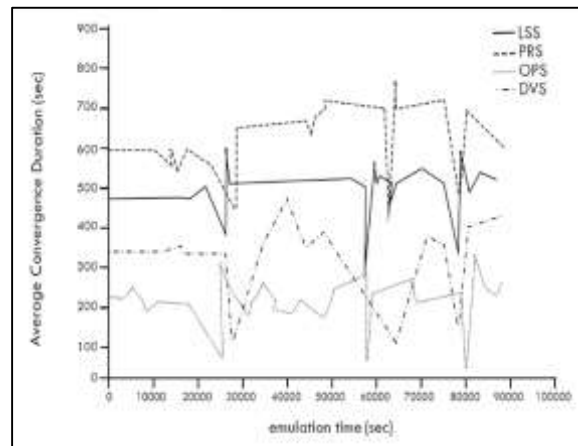
(b)



(c)



(d)



(e)

Figure 5.18: Optimized Results of GNS3 Emulation for the Edge-Edge Scenario  
 (a) Throughput (b) Average Reachable Time (c) Network Traffic Lost  
 (d) Average End-to-End Delay (e) Average Convergence Duration

Table 5.27: Optimized Results of GNS3 Emulation for the Edge-Edge Scenario

Networking Metrics	<u>GNS3 Emulation</u>			<u>Dynamic Cyber Resilience Solutions</u>			
	Event	Time (min)		OPS	PRS	LSS	DVS
Throughput (Mb/sec)	No Cyber Attack						
	No Failure	$t_0$	0425	2423	2416	2440	2437
	First Cyber Attack						
	First Failure	$t_1$	0426	1669	1358	2214	1955
	First Recovery	$t_2$	0493	2394	2307	2550	2417
	Second Cyber Attack						
	Second Failure	$t_3$	0933	1616	1445	2342	1946
	Second Recovery	$t_4$	1022	2311	2282	2673	2421
	Third Cyber Attack						
	Third Failure	$t_5$	1281	1724	1272	2304	1998
Third Recovery	$t_6$	1396	2406	2183	2698	2460	
Average Reachable Time (sec)	No Cyber Attack						
	No Failure	$t_0$	0423	0265	0236	0320	0482
	First Cyber Attack						
	First Failure	$t_1$	0424	0284	0327	0417	0517
	First Recovery	$t_2$	0492	0224	0271	0346	0454
	Second Cyber Attack						
	Second Failure	$t_3$	0941	0285	0387	0423	0487
	Second Recovery	$t_4$	1026	0231	0246	0315	0417
	Third Cyber Attack						
	Third Failure	$t_5$	1286	0377	0413	0438	0505
Third Recovery	$t_6$	1398	0235	0282	0361	0445	
Network Traffic Lost (Mb/sec)	No Cyber Attack						
	No Failure	$t_0$	0428	0224	0165	0068	0374
	First Cyber Attack						
	First Failure	$t_1$	0429	2414	0750	0490	1500
	First Recovery	$t_2$	0481	0213	0178	0089	0242
	Second Cyber Attack						
	Second Failure	$t_3$	0932	1991	1011	0493	1512
	Second Recovery	$t_4$	1029	0134	0075	0104	0183
	Third Cyber Attack						
	Third Failure	$t_5$	1281	2000	0778	0667	1527
Third Recovery	$t_6$	1396	0217	0105	0062	0155	
Average End-to-End Delay (sec)	No Cyber Attack						
	No Failure	$t_0$	0427	0015	0002	0009	0006
	First Cyber Attack						
	First Failure	$t_1$	0428	0017	0008	0011	0015
	First Recovery	$t_2$	0499	0015	0002	0007	0008
	Second Cyber Attack						
	Second Failure	$t_3$	0933	0027	0021	0023	0025
	Second Recovery	$t_4$	1026	0015	0006	0009	0013
	Third Cyber Attack						
	Third Failure	$t_5$	1282	0037	0025	0025	0034
Third Recovery	$t_6$	1408	0028	0016	0016	0030	
Average Convergence Duration (sec)	No Cyber Attack						
	No Failure	$t_0$	0423	0227	0594	0480	0347
	First Cyber Attack						
	First Failure	$t_1$	0424	0064	0464	0377	0124
	First Recovery	$t_2$	0490	0309	0722	0600	0480
	Second Cyber Attack						
	Second Failure	$t_3$	0935	0078	0413	0275	0111
	Second Recovery	$t_4$	1017	0285	0776	0552	0495
	Third Cyber Attack						
	Third Failure	$t_5$	1282	0036	0500	0341	0177
Third Recovery	$t_6$	1399	0312	0700	0589	0400	

The OPS solution was continued to achieve the optimal results of other standard solutions in the average reachable time metric and average convergence duration metric throughout the edge-edge scenario. The optimized outputs of the OPS solution presented in Table 5.27 that its reachable time in the first failure event was 284 sec at  $t_1$  424 min also closed to 285 sec at  $t_3$  941 min during the next failure event, but it was hopped up to 377 sec around the last failure event at  $t_5$  1286 min. Besides, the RPS has the second-optimal results in this metric for the periods of testing emulations with one-to-one events 327 sec, 387 sec, and 413 sec, as in Figure 5.18 (b).

Moreover, the three average convergence durations of the OPS solution were 309 sec at  $t_2$  490 min in the first recovery event, decreased to 285 sec at  $t_4$  1017 min in the second recovery event, then returned to 312 sec once more at  $t_6$  1399 min in the third recovery event. Note that it was initiated with 227 sec at  $t_0$  423 min with no failure event before cyberattacks were started as per the dotted zigzag curve displayed in Figure 5.18 (e). The DVS solution's convergence durations were 480 sec, 495 sec, and 400 sec, singly.

In overlooking, the LSS solution also has the optimal results in two standard metrics of the throughput and network traffic lost, whereas the OPS solution has intermediate results observing these metrics. As the solid drooping curve was denoted in Figure 5.18 (a), the throughput metric yields of the LSS solution were 2214 Mb/sec at  $t_1$  426 min in the opening failure event and was raised to a rate of 2342 Mb/sec in the subsequent failure event at  $t_3$  933 min nonetheless was declined slightly to touch 2304 Mb/sec at  $t_5$  1281 min in the final failure event. In turn, the OPS throughput rates were 1669 Mb/sec, 1616 Mb/sec, and 1724 Mb/sec across exact time frames.

Likewise, the tested CII networks were lost traffic when using the LSS solution by 490 Mb/sec in the failure event firstly at  $t_1$  429 min, although it was 68 Mb/sec at  $t_0$  428 min without failure event. Secondly, the LSS solution dropped the amount of network traffic by 493 Mb/sec at  $t_3$  932



min and ended thirdly by 667 Mb/sec at  $t_5$  1281 min. Finally, however, the OPS solution was lost many packets by the rate of 2414 Mb/sec diminished to 1991 Mb/sec and then pushed a little bit to get hold of 2000 Mb/sec in excess of the forgoing failure events, as solid and dotted peaks were represented in Figure 5.18 (c).

The optimal results of the fifth standard metric for the average end-to-end delay went to the PRS solution, where it was 8 sec even as the average delay of the OPS solution was 17 sec at  $t_1$  428 min in the first failure time. An update to the second failure event was that the PRS delay was 21 sec, and the OPS delay was 27 sec at  $t_3$  933 min. After all, the end-to-end delay of the PRS solution in the third failure event was 25 sec and 37 sec for the OPS solution at  $t_5$  1282 min. Even though the initial measurements of the average end-to-end delay at  $t_0$  427 min without failure event were 2 sec and 15 sec one by one for the PRS and OPS solutions, as dashed and dotted curved stairs were offered in Figure 5.18 (d).

Table 5.28: Solutions Ranking of Optimized Emulation Results for the Edge-Edge Scenario

<i>Standard Emulation Networking Metrics</i>	<i>Dynamic Cyber Resilience Factors</i>	<i>Ranking of Dynamic Cyber Resilience Solutions</i>			
		<i>OPS</i>	<i>PRS</i>	<i>LSS</i>	<i>DVS</i>
<i>Throughput</i>	<i>Performance</i>	3	4	1	2
<i>Average Reachable Time</i>	<i>Recovery</i>	1	2	3	4
<i>Network Traffic Lost</i>	<i>Absorption</i>	4	2	1	3
<i>Average End-to-End Delay</i>	<i>Volatility</i>	4	1	2	3
<i>Average Convergence Duration</i>	<i>Recovery Time</i>	1	4	3	2

In Table 5.28, the optimized emulation results support that the OPS solution has the first level in the recovery factor and recovery time factor competed with other standard solutions. It has third place in performance and fourth-order in both absorption and volatility factors through the edge-edge scenario. The remaining first rankings of the dynamic cyber resilience factors were divided between two standard solutions: the volatility factor for PRS solution, performance, and absorption factors for the LSS solution. No first order for the DVS solution.

### 5.3 Optimized Results Analysis of Analytical Modeling

Similar to the procedures of the analysis of the results that conducted through the primary research phase after the computing simulations and experimental emulations as described in subsection 5.1.3, the analytical modeling was also used as a quantitative research method in the optimizing research phase to analyze the simulated and emulated data for the optimized proposed solution and other standard solutions and performed abroad comparisons among them.

The analysis and comparison of the optimized simulation results and emulations under concurrent and consecutive cyberattacks in different scenarios were based on metrics measuring the  $R$  the single dynamic cyber resilience and  $R_{total}$  the total dynamic cyber resilience mathematically. Besides, analyses and comparisons were between total resilience of primary proposed solution and optimized proposed solution and comparison for total resilience in all research scenarios.

In Table 5.29, the analytical results of the  $R_1$ ,  $R_2$ ,  $R_3$  as a single resilience metric and  $R_{total}$  as a total resilience metric for the OPS solution through simulated scenarios revealed the level of the advancements achieved in these metrics on the basis of the improvements implemented on the proposed solution in the optimizing phase compared to primary proposed solution PPS and other standard solutions PRS, LSS, and DVS.

In the optimized simulated core-core scenario, the value of the first single dynamic cyber resilience  $R_1$  of the OPS solution was 32 at  $t_2$  498 min enhanced to become 34 in the second single resilience  $R_2$  at  $t_4$  1026 min then the value has been added up to 35 at  $t_6$  1394 min in the third single resilience  $R_3$  as made known in Figure 5.19 (a). Also, the overall value of the total resilience  $R_{total}$  for the OPS was 108, the DVS was 91, the PRS was 67, and the LSS was 43, as in Figure 5.19 (b), consider that the OPS has the best total resilience result achieved than others.

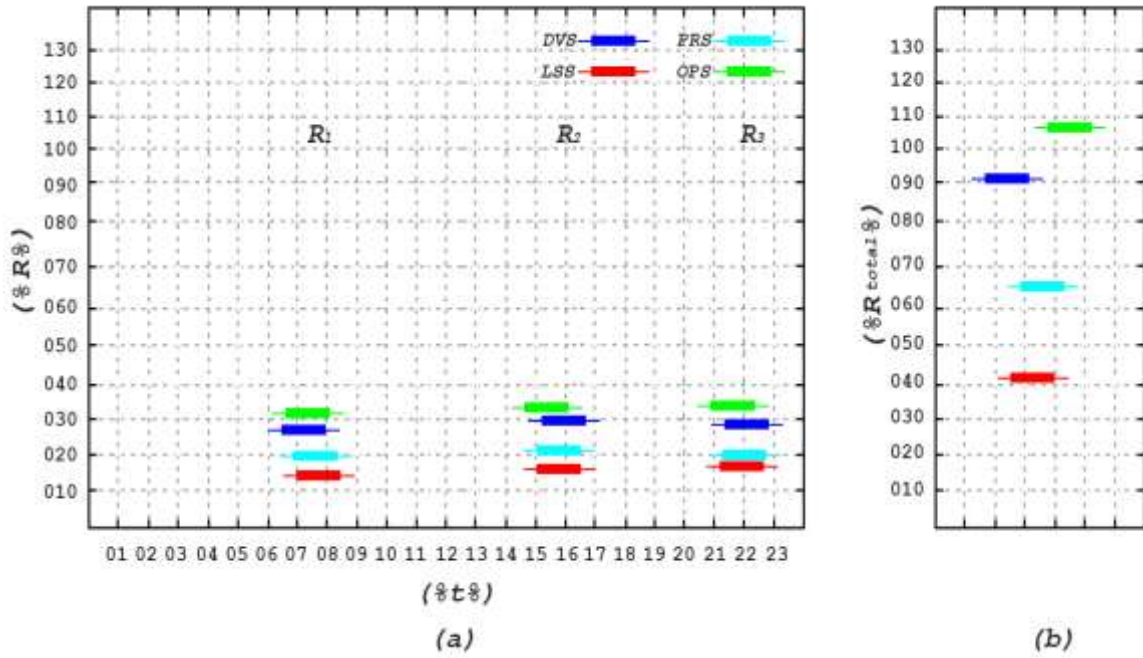


Figure 5.19: MAXIMA Analytical Modeling for Optimized Simulated Core-Core Scenario  
 (a) Single Resilience ( $R_1, R_2, R_3$ ) (b) Total Resilience ( $R_{total}$ )

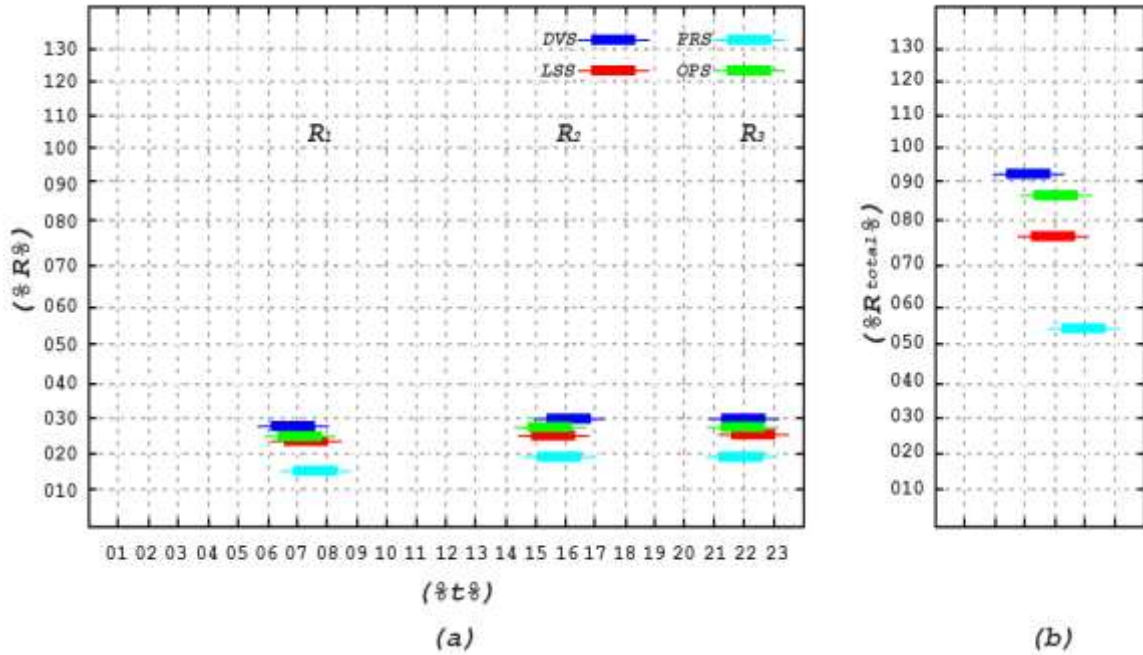


Figure 5.20: MAXIMA Analytical Modeling for Optimized Simulated Core-Edge Scenario  
 (a) Single Resilience ( $R_1, R_2, R_3$ ) (b) Total Resilience ( $R_{total}$ )

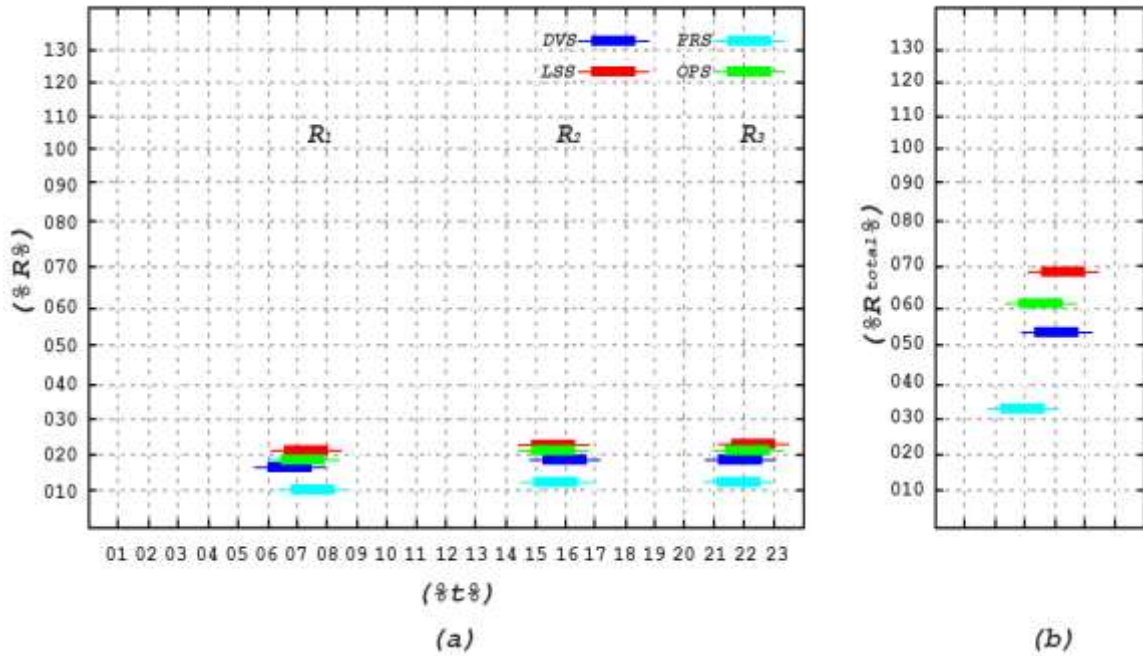


Figure 5.21: MAXIMA Analytical Modeling for Optimized Simulated Edge-Edge Scenario  
 (a) Single Resilience ( $R_1, R_2, R_3$ ) (b) Total Resilience ( $R_{total}$ )

Table 5.29: Results of MAXIMA Analytical Modeling for Optimized Simulated Scenarios

Simulated Scenarios	MAXIMA Analytical Modeling			Dynamic Cyber Resilience Solutions				
	Time (min)	Resilience	(R)	OPS	PRS	LSS	DVS	
Core-Core Scenario	<i>First Cyber Attack</i>							
	$t_2$	0498	First Resilience	$R_1$	0032	0020	0012	0027
	<i>Second Cyber Attack</i>							
	$t_4$	1026	Second Resilience	$R_2$	0034	0021	0014	0030
	<i>Third Cyber Attack</i>							
$t_6$	1394	Third Resilience	$R_3$	0035	0020	0016	0029	
<i>Total Resilience</i>								
			$R_{total}$	0108	0067	0043	0091	
Core-Edge Scenario	<i>First Cyber Attack</i>							
	$t_2$	0491	First Resilience	$R_1$	0027	0014	0022	0028
	<i>Second Cyber Attack</i>							
	$t_4$	1024	Second Resilience	$R_2$	0028	0019	0025	0030
	<i>Third Cyber Attack</i>							
$t_6$	1396	Third Resilience	$R_3$	0027	0019	0024	0030	
<i>Total Resilience</i>								
			$R_{total}$	0088	0055	0077	0092	
Edge-Edge Scenario	<i>First Cyber Attack</i>							
	$t_2$	0494	First Resilience	$R_1$	0019	0010	0021	0017
	<i>Second Cyber Attack</i>							
	$t_4$	1026	Second Resilience	$R_2$	0021	0011	0023	0018
	<i>Third Cyber Attack</i>							
$t_6$	1395	Third Resilience	$R_3$	0021	0011	0022	0017	
<i>Total Resilience</i>								
			$R_{total}$	0062	0034	0069	0054	

On top of Figure 5.20 (a), the single resilience values of the DVS solution and the OPS solution in the optimized simulated core-edge scenario were converging, whereas the first single resilience  $R_1$  for the DVS solution was 28 at  $t_2$  491 min while it was  $R_1$  by 27 for the OPS solution. Likewise, the DVS solution has a second single resilience  $R_2$  value of 30; however, the OPS solution has a second single resilience  $R_2$  value of 28 at  $t_4$  1024 min. Finally, the third single resilience  $R_3$  values of the DVS and the OPS were 30 and 27 in that order at  $t_6$  1396 min.

These values were consequentially reflected on the total resilience value  $R_{total}$  for both solutions, where the total resilience of the DVS solution was 92 and for the OPS solution was 88; in contrast, the total resilience values for the rest solutions were 77 for the LSS solution and 55 for the PRS solution as appeared in Figure 5.20 (b).

In the same way, the LSS solution value of the total resilience in the optimized simulated edge-edge scenario was the highest one than other solutions, including the OPS solution, as displayed in Figure 5.21 (b). The  $R_{total}$  of the LSS solution was 69, although the  $R_{total}$  of the OPS solution was closed to 62, the  $R_{total}$  of the DVS solution was 54, and the  $R_{total}$  of the PRS solution was 34, which is the lowest one.

These total resilience values of the competing solutions above in the optimized simulated edge-edge scenario result from the accumulative values of the single dynamic cyber resilience. The LSS solution also has the highest ones across the others, as shown in Figure 5.21 (a). At  $t_2$  494 min, the first single resilience  $R_1$  value of the LSS solution was 21, followed by the  $R_1$  value of the OPS solution with 19.

As well, the  $R_2$  value of the LSS was 23 even though the  $R_2$  value of the OPS solution was 21 in the second single resilience at  $t_4$  1026 min. The third single resilience values of the two solutions were not out of this context where  $R_3$  of the LSS and the OPS solutions were 22 and 21 singly at

$t_6$  1395 min. Indifference, the single resilience values of the remaining solutions ranged between 10 and 18 over similar time frames. The  $R_1$ ,  $R_2$ , and  $R_3$  values of the DVS solution were 17, 18, and 17. The  $R_1$  value of the PRS solution was 10, so its  $R_2$  and  $R_3$  values were 11 for each.

Table 5.30: Solutions Ranking for Total Resilience in Optimized Simulated Scenarios

	<i>Ranking of Dynamic Cyber Resilience Solutions for <math>R_{total}</math> in Optimized Simulated Scenarios</i>			
	<i>OPS</i>	<i>PRS</i>	<i>LSS</i>	<i>DVS</i>
<i>Core-Core Scenarios</i>	1	3	4	2
<i>Core-Edge Scenarios</i>	2	4	3	1
<i>Edge-Edge Scenarios</i>	2	4	1	3

Table 5.30 introduced evidence that the OPS solution allowed the tested interdependent CII networks in the core-core scenarios to become more resilient rather than using other standard solutions with the first position based on the total resilience results keeping up with the DVS solution in the second grade. In contrast, the PRS solution has the third class, and the LSS solution was rated the fourth.

Moreover, the OPS solution was succeeded in keeping the second class in the core-edge scenarios, and the edge-edge scenarios, shadowed for the DVS solution and the LSS solution, have the first level in both series of simulated scenarios. Also, the DVS solution has the second type in the core-core scenarios and the third in the edge-edge scenarios.

Furthermore, the LSS solution was positioned third in the core-edge scenario and fourth in the core-core scenarios. Note that the PRS solution has no first echelon in any series of simulated scenarios, but it was classed third in the core-core scenarios and arranged the last in both the core-edge and edge-edge scenarios.

The rankings of the OPS solution in the optimized simulated scenarios as described in Table 5.30 were highest than the rankings of the PPS solution in the primary simulated scenarios at all series of three scenarios as listed in Table 5.14 on the basis of the total resilience.

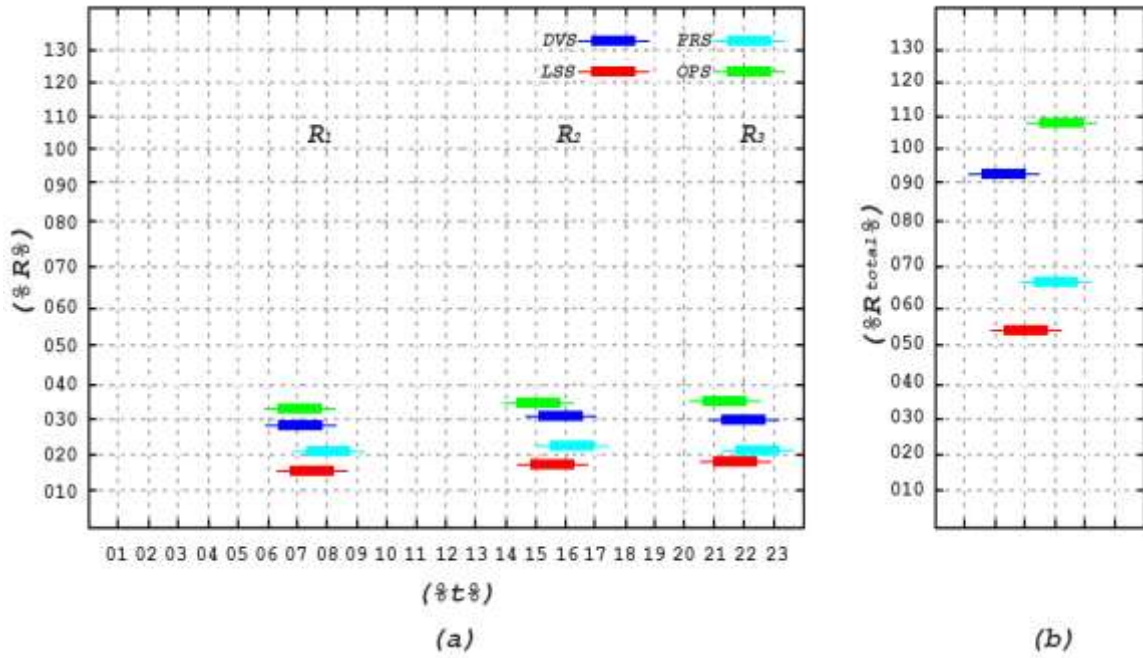


Figure 5.22: MAXIMA Analytical Modeling for Optimized Emulated Core-Core Scenario  
 (a) Single Resilience ( $R_1, R_2, R_3$ ) (b) Total Resilience ( $R_{total}$ )

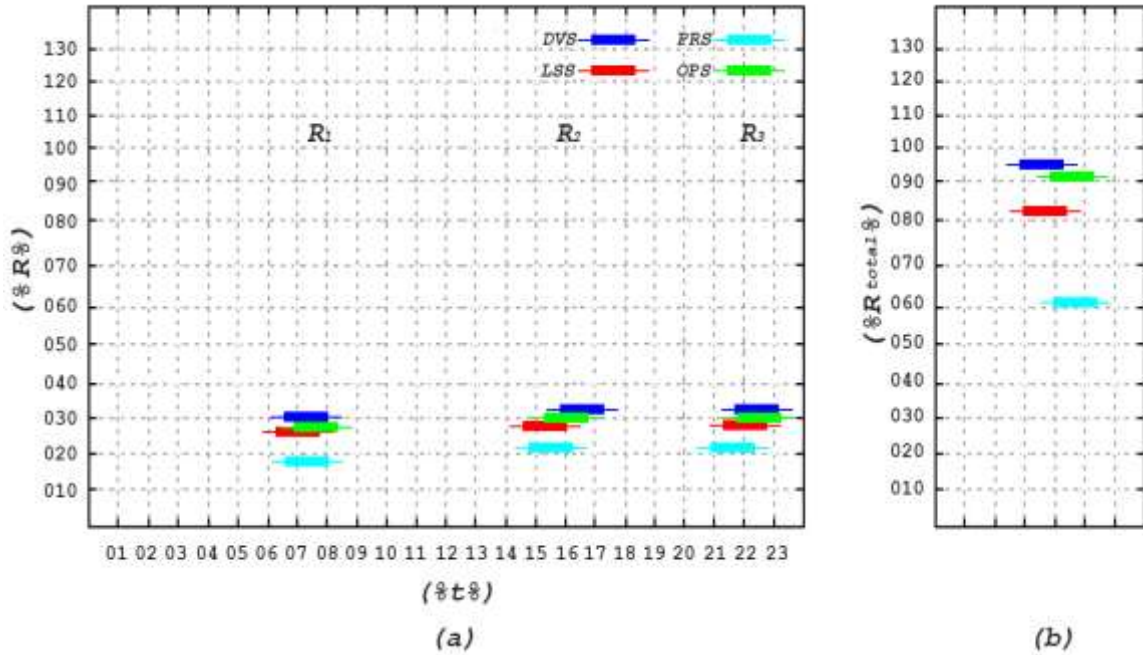


Figure 5.23: MAXIMA Analytical Modeling for Optimized Emulated Core-Edge Scenario  
 (a) Single Resilience ( $R_1, R_2, R_3$ ) (b) Total Resilience ( $R_{total}$ )



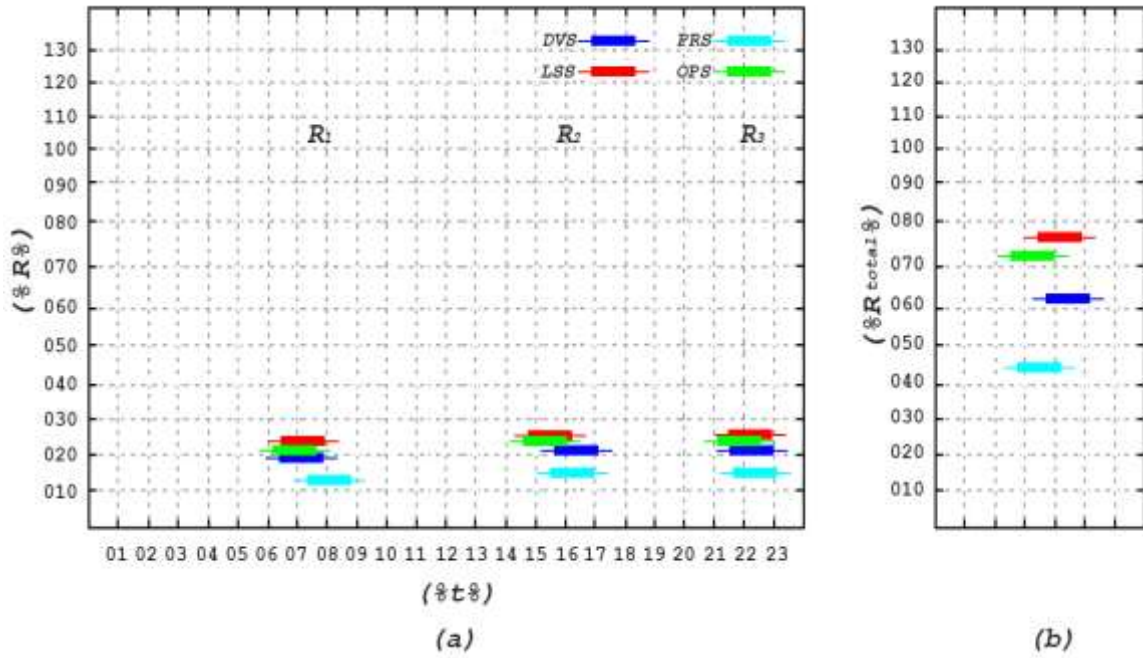


Figure 5.24: MAXIMA Analytical Modeling for Optimized Emulated Edge-Edge Scenario  
 (a) Single Resilience ( $R_1, R_2, R_3$ ) (b) Total Resilience ( $R_{total}$ )

Table 5.31: Results of MAXIMA Analytical Modeling for Optimized Emulated Scenarios

Emulated Scenarios	MAXIMA Analytical Modeling			Dynamic Cyber Resilience Solutions				
	Time (min)	Resilience	(R)	OPS	PRS	LSS	DVS	
Core-Core Scenario	<i>First Cyber Attack</i>							
	$t_2$	0491	First Resilience	$R_1$	0032	0021	0014	0028
	<i>Second Cyber Attack</i>							
	$t_4$	1028	Second Resilience	$R_2$	0035	0022	0017	0031
	<i>Third Cyber Attack</i>							
$t_6$	1403	Third Resilience	$R_3$	0036	0021	0018	0030	
<i>Total Resilience</i>								
			$R_{total}$	0109	0068	0053	0092	
Core-Edge Scenario	<i>First Cyber Attack</i>							
	$t_2$	0493	First Resilience	$R_1$	0028	0018	0024	0030
	<i>Second Cyber Attack</i>							
	$t_4$	1016	Second Resilience	$R_2$	0030	0021	0027	0032
	<i>Third Cyber Attack</i>							
$t_6$	1391	Third Resilience	$R_3$	0030	0021	0027	0031	
<i>Total Resilience</i>								
			$R_{total}$	0091	0062	0082	0095	
Edge-Edge Scenario	<i>First Cyber Attack</i>							
	$t_2$	0490	First Resilience	$R_1$	0022	0012	0025	0019
	<i>Second Cyber Attack</i>							
	$t_4$	1017	Second Resilience	$R_2$	0024	0015	0026	0021
	<i>Third Cyber Attack</i>							
$t_6$	1399	Third Resilience	$R_3$	0023	0014	0025	0021	
<i>Total Resilience</i>								
			$R_{total}$	0073	0045	0086	0063	



The results of the optimized emulated scenarios for the OPS solution emphasized the results obtained from the previous optimized simulated scenarios that support the same context in terms of single resilience and total resilience values, as designated in Table 5.31. Thus, for example, the first single resilience  $R_1$  value of the OPS solution in the core-core scenario was 32 at  $t_2$  491 min, followed by the single resilience  $R_1$  value of the DVS solution was 28, the  $R_1$  value of the PRS solution was 21, and the  $R_1$  value of the LSS solution was 14.

Likewise, the OPS solution has the  $R_2$  value of 35 at  $t_4$  1028 min, closed to the DVS solution with the  $R_2$  value of 31. In turn, the second single resilience  $R_2$  of the PRS and the LSS solutions were one-by-one 22 and 17, as demonstrated in Figure 5.22 (a). At  $t_6$  1403 min, the last single resilience in this scenario for the OPS solution was the  $R_3$  value of 36. The  $R_3$  values of the standard solutions starting from 30 for the DVS solution reached 18 for the LSS solution, passed by 21 for the PRS solution.

In the equivalent situation, the total resilience values were varied between the contesting solutions where the  $R_{total}$  value of the OPS solution was the highest one by 109. The  $R_{total}$  values gradually dropped from 92 for the DVS solution, then 68 for the PRS solution, to 53 for the LSS solution, as illustrated in Figure 5.22 (b).

In the core-edge scenario, the optimized emulated results of the OPS solution were slightly changed for the DVS standard solution favor, whereas its first single resilience  $R_1$  value was 30 at  $t_2$  493 min compared to the  $R_1$  value 28 for the OPS solution. Similarly, the  $R_2$  value 32 was the second single resilience of the DVS solution in the opposite  $R_2$  value of 30 for the OPS solution at  $t_4$  1016 min. Finally, figure 5.23 (a) has appeared that the margin of the third single resilience between the DVS solution and the OPS solution was narrow, where the DVS  $R_3$  value was 31, and the OPS  $R_3$  value was 30 at  $t_6$  1391 min.

Remaining in this scenario to counterweight the values of the total resilience for these solutions as presented in Figure 5.23 (b), the  $R_{total}$  of the DVS solution was the uppermost value with 95 even though the  $R_{total}$  of the OPS solution was by way of 91 despite the fact that the  $R_{total}$  of LSS solution was on the average alongside the value of 82. Lastly, the PRS solution  $R_{total}$  value was 62. The outstanding results of the LSS solution in the edge-edge scenario were not much different from the previous scenario, as presented in Table 5.31. The values of the single resilience and total resilience for the LSS solution were the highest-level contended to other solutions shadowed by the  $R_1$ ,  $R_2$ ,  $R_3$ , and  $R_{total}$  values of the OPS solution.

Table 5.32: Solutions Ranking for Total Resilience in Optimized Emulated Scenarios

	<i>Ranking of Dynamic Cyber Resilience Solutions for <math>R_{total}</math> in Optimized Emulated Scenarios</i>			
	<i>OPS</i>	<i>PRS</i>	<i>LSS</i>	<i>DVS</i>
<i>Core-Core Scenarios</i>	1	3	4	2
<i>Core-Edge Scenarios</i>	2	4	3	1
<i>Edge-Edge Scenarios</i>	2	4	1	3

Figure 5.24 (a) revealed that the LSS solution has the first single resilience  $R_1$  value of 25 at  $t_2$  490 min pushed at  $t_4$  1017 min a little bit in second single resilience to become  $R_2$  value of 26 then return back again at  $t_6$  1399 min within the final single resilience to be  $R_3$  value of 25, note that the total resilience  $R_{total}$  value was 86.

These values have competed with the OPS solution values in the single resilience and total resilience as the following:  $R_1$  value was 22,  $R_2$  value was 24,  $R_3$  value was 23, and  $R_{total}$  value was 73. Also, the total resilience values for the rest standard solutions of the DVS and the PRS were  $R_{total}$  of 63 and 45 in that order, as shown in Figure 5.24 (b).

The final rankings of the OPS solution in the optimized emulated scenarios in Table 5.32 above confirmed the final rankings of the OPS solution in the optimized simulated scenarios in Table 5.30 based on the overall total resilience values. The OPS was organized first in the core-core

scenarios and second in the core-edge and edge-edge scenarios contrasted with other standard dynamic cyber resilience solutions. The DVS solution has the first position in the core-edge scenarios, and the LSS solution has the first-rate in the edge-edge scenarios without any first place for PRS in any series of emulated scenarios.

Table 5.33: Solutions Ranking Comparison for Total Resilience in All Research Scenarios

	<i>Ranking of Dynamic Cyber Resilience Solutions for <math>R_{total}</math> in All Scenarios</i>							
	<i>Primary Phase</i>				<i>Optimization Phase</i>			
	<i>PPS</i>	<i>PRS</i>	<i>LSS</i>	<i>DVS</i>	<i>OPS</i>	<i>PRS</i>	<i>LSS</i>	<i>DVS</i>
<i>Core-Core Scenarios</i>	2	3	4	1	1	3	4	2
<i>Core-Edge Scenarios</i>	3	4	2	1	2	4	3	1
<i>Edge-Edge Scenarios</i>	3	4	1	2	2	4	1	3

On the other hand, a final grading comparison was performed among the opposing technology solutions used in this thesis include PPS, OPS, PRS, LSS, and DVS solutions across all research scenarios, whether over simulations or emulations testing scenarios in both the primary phase and optimization phase on the basis of the total resilience  $R_{total}$  metric as represented in Table 5.33.

## 5.4 Optimized Results Discussion

This work addresses the proposed solution that focuses on the architecture design of the conceptual framework and integration drives the technology stack in the primary phase and further revisited the proposed solution to develop an optimized one through added new modules during the second study phase in an attempt to fill the current research gaps and accomplish the thesis purpose.

On the other hand, the computing simulations emulated experiments were employed to verify the dynamic cyber resilience capabilities of the proposed solution. Also, various assessment measures and testing scenarios were utilized to evaluate the proposed solution in both research phases. The simulated and emulated results proved that the optimized proposed solution has the highest total resilience results than the several existing solutions.

This section provided a full discussion of the optimized results, followed by a detailed explanation of the optimized results collected and analyzed through the research simulations and emulations. Furthermore, a comprehensive presentation regarding the final research findings was elaborated in the context of the study rationale and thesis objectives that significantly impacted deep interpretation.

The optimized conceptual framework was developed to analyze every dynamic cyber resilience factor contributing to the optimized proposed solution, as highlighted in section 3.2 while tracing these factors of high importance powering the proposed solution implementation. The optimized proposed solution (OPS) comprises additional modules that significantly affected the overall results and rankings of the proposed solution in several metrics.

The conceptual framework revision for optimized proposed solution implementation in this work is a one-of-its-kind that contains the added constituents that led to considered more benefits to match the study objectives and examines the aspects influencing the dynamic cyber resilience capabilities of the interdependent CII networks were afterward generalized.

Therefore, the discussion of the results in this subsection focused on the optimization influences of the additional modules that enhanced the capabilities of the optimized proposed solution competed with the same dynamic cyber resilience capabilities of the standard solutions through the simulated and emulated testing scenarios.

However, the first capability improved in the optimized proposed solution was the withstanding capability depending on three integrated encryption protocols: TWINE protocol, RSA protocol, and SHA protocol to boost the configuration, controls, and operational procedures. Also, the second capability improved was the mitigation capability through using MPLS protocol to minimize escalating consequences and maintain the critical functions of interdependent CIIs

during DDoS cyberattacks within acceptable degradation parameters to resist internal drifts and cascading failures.

The recovery capability of the OPS solution was improved by FRP protocol to rebuild structural properties and critical functions within an acceptable time and composite costs (Riaz et al., 2018). These improvements reinforced the current overall protocols of the proposed solution and supported the restorative capacities that should be assessed against a defined set of requirements derived from a desirable level of controls and services (Papán et al., 2018).

In the optimization phase, all testing scenarios were repeated to evaluate the dynamic cyber resilience capabilities of the optimized proposed solution compared to the primary proposed solution and standard solutions under core-core, and core-edge, and edge-edge scenarios. Table 5.18 and Table 5.24 showed the competing solutions simulated and emulated ranking results during the core-core scenarios.

The withstanding capability of the OPS solution was improved by augmenting the current hash graph and aBFT protocols with the hybrid triple cryptography scheme that combined TWINE, RSA, and SHA protocols together to form secure end-to-end transmissions (Minematsu et al., 2011). In addition, RSA characteristically was identified authentication performed via digital signatures to decentralize TWINE bulk encryption key of data due to its fast speed for efficient computation jointly with deterministic SHA protocol collision-resistance (Hayel & Zhu, 2015).

The withstanding capability of the OPS solution was better than the withstanding capabilities of the PPS solution and the DVS solution in all core-core scenarios because the MD5 protocol used by the DVS solution was quite slower than the optimized SHA protocol controlled by the OPS solution as well as SHA was much secure than the MD5 (Gupta & Kumar, 2014). Moreover, SHA was implemented in the optimized technology stack of the OPS solution with exceeding

rates, unlike MD5 (Khan, 2021).

However, the withstanding capabilities of the PRS and LSS solutions were still better than the withstanding capability of the OPS solution for the TTL security check functioned by the PRS solution and distribute-list filter operated by the LSS solution. TTL mechanism was effective to establish, easy to deploy, maintaining the peering session, and passing the Etisalat-DEWA CII traffic only when the TTL values were equal to or greater than the configured values. Otherwise, it was silently discarded. (Jiang et al., 2021). Furthermore, the distribute-list filter was hidden networking data records to avoid routing loops in Etisalat-DEWA networks with redundant paths that permit routing updates for only specific paths (Dünner et al., 2018).

Likewise, the OPS results in the mitigation capability were also improved and became higher than the mitigation capability results of the PPS, PRS, and DVS solution altogether except the LSS solution due to the reliability of the Multiprotocol Label Switching (MPLS) protocol, which was worked mutually with IGMP and TLS protocols. Moreover, MPLS has connected all hub nodes for optimized any-to-any inter-connectivity growth from one core network to another through quality connections (Masood et al., 2018).

Thus, it was offered consistency with no traffic loss and fixed latency. Also, it was secure and did not require a higher level of functionality (Olszewski, 2012). On the contrary, the VRRP protocol managed by LSS has high adaptability where the traffic packets of the Etisalat-DEWA CIIs were encapsulated in IP packets and supported other protocols in the LSS solution suit (Neumann, 2015).

In a related, the recovery capability of the OPS solution was reached to the top results competed to all other standard solutions and, of course, the PPS solution too. Furthermore, the OPS solution adopted the Fast Reroute Protocol (FRP) to drive simultaneously with the gossip and virtual

voting protocols since the FRP protocol was lightweight and suitable for any size of the Etisalat-DEWA CII networks with multiple cyber failure protection (Jarry, 2013).

FRP computed per-prefix possibility calculations to define custom backup paths on each hub node with the least control overhead (Qiu et al., 2019). It has fast rerouting where the traffic packets were shifted immediately to the pre-computed backup paths as the next-hop routes delivered to the destination without looping back via standardized bit-string headers (Papán et al., 2018).

For example, despite the LSS solution used the RPR protocol for the recovery capability that was a simple, inherent, and straightforward multicast support using the coupled structure of the Etisalat-DEWA CII networks, but it has no bandwidth dedicated for recovery purposes; therefore, Etisalat CII network resources utilization were high in the cyber failure events (Robles et al., 2021). Furthermore, the bandwidth available was substantially reduced depending on the actual load and decentralization of the DEWA CII network traffic (An et al., 2021).

Table 5.20 and Table 5.26 presented the simulated and emulated results of the OPS solution in the overall edge-core scenarios, where the improvements caused by additional protocols also affected the OPS capabilities positively like in the core-core scenarios. The withstanding capability of the OPS solution was advantageous than the withstanding capabilities of the PPS and DVS solutions but did not exceed the withstanding capabilities of the LSS and PRS solutions.

The RSA protocol functioned by the OPS solution was fast and efficient for large amounts of data records (Couteau et al., 2016). In addition, it provided more effectiveness and unwavering quality over the Etisalat-ENOC CII networks by utilizing three rounds of encryption to reduce their vulnerability to DDoS cyberattacks (Bensalem et al., 2021).

However, this protocol has low diffusion where all embedded data were contained in a single ciphertext record. So, the susceptibility to modifications with active interceptors who break it could insert spurious records that looked original (Mahajan & Sachdeva, 2013).

Per contra, TWINE was the second encrypted protocol used by the OPS solution that has high diffusion of data from one record diffused into several ciphertext records; it also resisted corruption by inserting data records without detection (Aboshosha et al., 2020). Nevertheless, error propagation of the TWINE protocol in one data record corrupted the entire record block (Suzaki et al., 2013). Moreover, it was limited with key sharing, causing losses for the source and destination hub nodes (Minematsu et al., 2011).

On the far side, the mitigation capability results of the OPS solution in the edge-core scenarios were similar to the mitigation capability results of the PPS solution despite optimization performed by operating the MPLS protocol because it has a lack of total control over all IP routing in the Etisalat-ENOC CII networks (Kempf et al., 2011). The hub nodes did not establish direct routing adjacencies but instead peered with others (Olszewski, 2012).

The OPS results in this capability were lower than the PRS and LSS solutions. The MPLS protocol was designed alongside insufficient attention to short volatility during cyber failures with a long time to deploy, especially when the hub nodes were spread across the Etisalat core and ENOC edge networks. It required streamlining to deliver point-to-point connectivity only (Masood et al., 2020).

However, MPLS was more scalable than the GLBP protocol used by the DVS solution to ensure high-volatility communications needed by the large-scale services of the Etisalat-ENOC CII networks with easily maintaining and sharing the networking resources (Aweya, 2021).

Beyond the bounds, the recovery capability optimization of the OPS solution has boosted the



results to become superior to the PPS solution and all standard solutions due to implementing Fast Reroute Protocol (FRP) by the OPS solution. The end-to-end delay of the FRP protocol was the minimum compared to the RPR protocol used by the LSS solution because FRP has supported the explicitly defined shortest primary and alternative paths (Papán et al., 2018). Furthermore, it handled links among hub nodes as members of an equal cost path-split set for hub node destinations. The other set members were provided alternative paths when the links failed (Qiu et al., 2019).

The FRP protocol was provided fast network traffic recovery upon hub node cyber failures for mission-critical services (Jarry, 2013). Upon any single hub node, cyber failure recovered impacted network traffic flows quickly (Riaz et al., 2018). On the contrary, the RPR protocol investigated each cyber failure scenario to determine whether a given load was handled properly (Hadjioannou, 2015). The need to verify whether the Etisalat-ENOC CII networks satisfied the necessary parameters for all conceivable network traffic flow patterns (Manzoor et al., 2020). Also, concerning the use of different classes of network traffic, FRP required external measures to prevent congestion because they were not standardized (Papán et al., 2018).

Table 5.22 and Table 5.28 presented the simulated and emulated results of the OPS solution and standard solutions in these scenarios in the edge-edge scenarios. Except for the improvement shift in recovery capability results of the OPS solution, the rest results of the withstanding and mitigation capabilities of the OPS solution were similar to the results of the PPS solution as well as the other standard solutions.

In detail, the withstanding capability of the OPS solution was the lowest one regarding all standard solutions, where it closed to the withstanding capability of the DVS solution. Correspondingly, the reason was the complexity value of the MD5 protocol and SHA protocol

used by the DVS and OPS solutions. Both values were equal, but the running time of the MD5 protocol was faster than the SHA protocol (Gupta & Kumar, 2014). Also, the SHA protocol required more computing resources and affected the withstanding capability (Bensalem et al., 2021).

Although the RSA protocol conducted by the OPS solution has the speed of transformation with linear in time and constant in space (Mahajan & Sachdeva, 2013). It also has low error propagation in encrypting one record, was not affect subsequent data records by establishing a session key pair (Smart, 2016).

Nevertheless, RSA was deficient in availability, high complexity, and weak quantum session key decentralization (Vasilyev et al., 2019). This was because encryption, one bit simultaneously, was more difficult to implement correctly (Kessler, 2016). Moreover, the TWINE protocol typically requires more resources, slowing encryption where an entire records block must be accumulated before encryption or decryption can begin (Minematsu et al., 2011).

In like manner, the mitigation capability of the OPS solution was the least opposite to the mitigation capability of the standard solutions. Even though the OPS solution drove the MPLS protocol to simplify the traffic routing and avoid traffic congestion, especially when using old frame-relay ENOC-Central Bank CII networks (Masood et al., 2018).

Also, this protocol has divided the requests into various ENOC CII network paths, adds labels on data packets when leaving the ENOC-Central Bank CII networks (Kempf et al., 2011). Then, the label was checked directly to pre-determine the paths and predict the network traffic (Olszewski, 2012). This way, it utilized path bandwidth and transverses through the whole Central Bank CII network quickly (Sapundzhi & Popstoilov, 2018).

Inappropriately, MPLS protocol was natively supported IP multicast traffic transport only,

tunneled between the hub nodes by configuring generic routing encapsulation tunnels (Masood et al., 2018). Furthermore, it has similar network traffic segregation like other protocols with a lack of volatility (Liu et al., 2016). Therefore, it did not natively offer a robust connection. However, it was doable to keep the end-to-end network traffic between hub nodes (Vugrin et al., 2014).

As a quantum leap in the recovery capability, the OPS solution has the optimal results, whether the PPS solution or the standard solutions. This is because the FRP protocol employed by the OPS solution has total control packets during routing with less than partially disjointing, and the routing entries on the intermediate hub nodes were small (Jarry, 2013).

The primary and backup paths were partially disjoint, and cyber failures occurred on the primary path; the hub node detected them ahead, shifted the network traffic to an alternate hub node, and informed the source hub node to choose an alternate path and retransmission of dropped packets (Papán et al., 2018).

However, MPLS depended on the complicated precomputation with encapsulation packet overhead causing internal ENOC CII network resources internal consumption (Olszewski, 2012). It has some difficulty in the complicated architecture elements of the ENOC-Central Bank CII networks (Kempf et al., 2011).

A fast recovery was required, the time for correction was critical with limited ENOC CII network resources; therefore, the convergence was insufficient (Brown et al., 2010). So, the MPLS protocol was computing original paths and backups to satisfy the end-to-end service quality constraints under the edge-edge scenarios of cyber failures to recover them (Liu et al., 2016).

This protocol was required to compute recovery distances for each hub node that failed as hard as computing multiple-source shortest paths in the ENOC-Central Bank CII networks (Masood et al., 2018). It ran in steps; therefore, it was optimal. Nonetheless, it was faster for undirected hub

nodes with time complexity; the convergence time was no greater than three rounds (Olszewski, 2012).

The second-better recovery capability goes to the PRS solution that used the PCRN protocol to optimize path computation between source and destination hub node pairs by leveraging weighted links and considering bandwidth and link usage metrics (De Florio, 2015).

Also, it was achieved optimality without full visibility at computation time and passed the set of potential paths across each neighboring destination domain when the sequence of the multi-domain network was known; it computed the optimal paths from each entry hub node to each exit hub node rooted at the destination with high function (Djojo & Karyono, 2013).

However, the PCRN was limited to a domain responsibility of intelligent control management, bad for responsiveness and dynamic use of ENOC network resources, and not flexible to high operational overhead changes in the ENOC-Central Bank CII networks (Pescaroli & Alexander, 2016). Moreover, the lack of complete topology information exchange across multiple domains due to scalability was a trust relationship between multi-domain in the Central Bank CII network (Sapundzhi & Popstoilov, 2018).

Therefore, no single hub node has the full visibility of the ENOC-Central Bank CII networks to determine optimal end-to-end paths that should be established with feasible domain boundaries from an exit hub node to select the next one (Wang et al., 2017).

## **5.5 Final Research Findings**

The post review of the primary and secondary research data and the detailed discussions of the primary and optimized results conducted above sections in this Chapter, it is found that the most crucial dynamic cyber resilience capabilities for the success of proposed solution implementation

are those described in the new perspective of the dynamic cyber resilience.

Having reviewed the proposed solution in section 3.2, the conceptual framework was developed and optimized based on the dynamic cyber resilience factors influencing the proposed solution conceptualization and implementation to respond to research gaps for the interdependent CII networks, achieve the study goal, and answer the thesis questions with meeting the related research hypotheses.

Furthermore, the overall results of the primary and optimized proposed solution with the dynamic cyber resilience capabilities were validated and identified rankings with a detailed mapping of the dynamic cyber resilience factors, the strengths, and weaknesses of efficient implementation for the proposed solution, as well as standard solutions. The final findings of this thesis were summarized and interpreted in listed below points as the following:

- **1<sup>st</sup> Finding:** The research gaps elaborated in the literature review found the historical absence of a cohesive theoretical or technology solution dedicated to dynamic cyber resilience for the interdependent critical information infrastructures. All current technologies in this area primarily were network routing protocols. Accumulatively, other protocols have been developed and integrated with these routing protocols in an attempt to contribute to coping with cybersecurity and cyber continuity challenges of the CIIs. Therefore, the current standard solutions for dynamic cyber resilience as a collection of different protocols usually have inadequate comprehending with several limitations related to their functionalities and interoperability.
- **2<sup>nd</sup> Finding:** From the extensive literature review, all standard solutions were built based on cyber trust engineering and investigated their algorithms individually to examine the various

protocols applicable for research implementation. For that reason, these solutions could not resolve the single cyber failure dilemma fundamentally in the interdependent critical information infrastructures because their hub nodes' structure has a scale-free topology that is very vulnerable to the single cyber failure, especially under DDoS cyberattacks that targeted hub nodes. The above structural dilemma of interdependent CIIs led this research to introduce the initial ground for the conceptual framework and technology stack of the proposed solution on the basis of cyber zero-trust engineering as a new one-of-its-kind solution considerably. It then identified the development life cycles, implementation characteristics, and optimization. Thus, the proposed solution increases the robustness and reliability of the decentralized hub nodes against cyberattacks and enhances the fast response and recovery from cyber failure events, thereby returning the critical services to the expected level of performance within an acceptable timeframe.

- **3<sup>rd</sup> Finding:** The research community was not dealing with all-embracing perspectives of dynamic cyber resilience. Thus, the published studies partially identified and carried out particular concepts of cyber resilience such as robustness, response, or recovery but not all together without an integrated conceptual framework. As a result, standard solutions developed based on these studies did not tackle the all-inclusive barriers, benefits, and impacts of cyber resilience applications in the sophisticated environment of the interdependent critical information infrastructures. Accordingly, one of the significant findings in this research combined all aspects of cyber risk management components with a new perspective of dynamic cyber resilience concepts to shift the paradigm towards resilient CIIs for enhancing their cybersecurity and cyber continuity of vital services.

- **4<sup>th</sup> Finding:** The optimization approach usually benefits from the lessons learned to improve efficiency and effectiveness. In this context, the optimization phase in this research thoroughly revisited the concerning strengths and highlighted weaknesses of the primary proposed solution after the first round of testing scenarios. Vast improvements made critical changes to the conceptual framework and technology stack to develop an optimized proposed solution. These significant enhancements boosted the available strengths and addressed the current weaknesses and thus reflected, in general, the achieved outcomes after re-executing the second round of the testing scenarios under the same circumstances. Consequently, comparing those optimized results with standard solutions results found out the fruitful success of the optimization approach applied to the proposed solution during this research.
- **5<sup>th</sup> Finding:** The quantification of dynamic cyber resilience as a crucial part of this study examined critically how different evaluation metrics, technical instrumentations, and testing scenarios influence the total resilience results of the dynamic cyber resilience solutions. Thereby, it is found that each metric, instrument, or scenario plays a significant role in reflecting the ability to measure and compare properly the accurate and consistent results that can be analyzed and validated to lead the investigations of the strengths and weaknesses of those solutions at both research implementation phases. Furthermore, it is essential to note that quantifying dynamic cyber resilience formed the basis of the research discussions and hence, derived the improvements regarding the proposed solution capabilities.

## **CHAPTER 6. CONCLUSIONS AND RECOMMENDATIONS**

The revisiting of the thesis parts, involving introduction, literature review, proposed solution, methodology, concludes the final results of both research phases conducted with areas for discussion in the context of dynamic cyber resilience of interdependent critical information infrastructures. The conclusions derived from the findings in light of the thesis goal and objectives and presented the recommendations were on the basis of the conclusions and research purpose.

This chapter is the last one of the thesis that consists of two main sections; the first section is the research conclusions, answering the research questions and meeting the associated hypotheses of the study objectives developed in Chapter 1 to accomplish the research purpose. Similarly, the outcomes and implications of the thesis findings are also briefly introduced.

The second section for resultant recommendations shared the research limitations were explained and summarized. Finally, several suggestions were made while highlighting, and the directions were mentioned for possible future works.

### **6.1 Research Conclusions**

Today, most of the core services in modern communities are based on interdependent critical information infrastructures to increase efficiency and effectiveness globally. Therefore, the cyber risks lead to shortages in vital services that directly affect national security and the economy.

As a result, several standard solutions were developed and implemented to protect CIIs and enhance their dynamic cyber resilience against sophisticated cyberattacks. Nevertheless, frequent cyber disrupts in CIIs space still occurred over the last decades. For two reasons, the first one is due to the single hub node failure within the interdependent CIIs resulting from the scale-free



topology and decentralized structure. Secondly, the standard solutions that have been built depend on cyber trustfulness engineering.

The overall purpose of this research is to introduce a theoretical and empirical solution to bridge the critical research gaps resulting in an intensive review of relevant literature. This thesis presents the novel proposed solution of dynamic cyber resilience on the basis of the cyber zero-trust engineering to cope with the shortcomings of the current standard solutions and overcome the single hub node failure under concurrent and consecutive cyberattacks.

### **6.1.1 Answering Research Questions and Meeting Hypotheses**

The answering research questions were formulated to address the research objectives and meet their associated hypotheses listed in Chapter 1, handling the secondary data gathered from published sources and literature review findings in Chapter 2. Besides, dealing with the information of the conceptual framework and the technology stack for the novel proposed solution to fulfill the research gaps in Chapter 3.

In addition, the processing of the collected primary data using primary sources significantly, computing simulations, and emulated experiments in Chapter 4, the carried-out investigations on the data analysis, primary and optimized results, and final research findings in Chapter 5.

- Answering Research Question 1 (RQ1): Theoretically, how can the conceptual framework of the proposed solution bridge the critical research gaps and underpin dynamic cyber resilience?

The first research gap was limited studies on critical information infrastructures compared to critical infrastructures. The primary and optimized conceptual frameworks of the proposed solution in this thesis enrich the research studies of critical information infrastructures area and focus on handling cyber resilience issues, not physical resilience or cyber-physical resilience.

The second research gap was the lack of conducted research on the cyber interdependency of heterogeneous critical information infrastructures. Therefore, this study's conceptual framework is a scientific effort to consternate the cyber interdependency of heterogeneous CII (ICS-based CII with ICT-based CII together), not homogeneous CII (ICS-based CII or ICT-based CII separately).

The third research gap was the dearth of works dealing with the scale-free topology vulnerability of coupled networks of critical information infrastructures. Theoretically, the conceptual framework of the proposed solution resolves the vulnerability of single hub node failure within the coupled CII networks resulting from the scale-free topology and decentralized structure. The other research works discuss only the technical vulnerabilities of CII such as operating systems, legacy characteristics, and administration issues.

- Testing RQ1 Hypothesis:
  - H<sub>1</sub>: The conceptual framework of the proposed solution can theoretically bridge the critical research gaps and underpin dynamic cyber resilience.

There is significant evidence based on the positive correlation in the detailed answer to the first research question to accept the RQ1 hypothesis. H<sub>1</sub> is accepted and fulfilled by developing the primary and optimized conceptual frameworks presented in Chapter 3 to theoretically bridge the critical research gaps and underpin dynamic cyber resilience.

- Answering Research Question 2 (RQ2): Empirically, how can the technology stack of the proposed solution bridge the critical research gaps and underpin dynamic cyber resilience?

The fourth research gap was the shortage of recent discussions because they were dedicated only to the single or multiple cyberattacks with spaced time intervals and cascading failures.

Implementing the technology stack in this thesis is concerned with the concurrent and consecutive cyberattacks against CIIs cause common, escalating, and cascading failures.

The fifth research gap was the no research papers were presented the dynamic cyber resilience for CIIs using cyber zero-trust engineering, most of them using cyber trustfulness engineering. This technology stack is the first and only one using cyber zero-trust engineering to develop and implement the proposed solution of dynamic cyber resilience for CIIs compared to existing standard solutions using cyber zero-trust engineering.

- Testing RQ2 Hypothesis:
  - H<sub>2</sub>: The technology stack of the proposed solution can empirically bridge the critical research gaps and underpin dynamic cyber resilience.

There is significant evidence based on the positive correlation in the above answer of the second research question to accept the RQ2 hypothesis. Therefore, H<sub>2</sub> is accepted and fulfilled by implementing the primary and optimized technology stack displayed in Chapter 3 to bridge the critical research gaps and underpin dynamic cyber resilience.

- Answering Research Question 3 (RQ3): Does the proposed solution reduce the disruptive effects among coupled CII networks against concurrent and consecutive cyberattacks?

Yes. The reduction of the disruptive effects, whether cascading, escalating, or common cause effects, correlates with two factors of dynamic cyber resilience. These factors are the recovery factor and recovery time factor. Although the primary results of both factors for the primary proposed solution have second and third ranks in three scenarios of core-core, core-edge, and edge-edge compared to the standard solutions, but the optimized results of the same factors were ranked up for the optimized proposed solution to become the first ranking in three scenarios

compared to other solutions. The proposed solution's ranking was validated throughout computing simulations and emulated experiments. The primary and optimized results indicate that the proposed solution reduced the disruptive effects among coupled CII networks against concurrent and consecutive cyberattacks.

- Testing RQ3 Hypothesis:
  - H<sub>3</sub>: The proposed solution reduces the disruptive effects among coupled CII networks against concurrent and consecutive cyberattacks.

There is significant evidence based on the positive correlation in the overhead answer of the third research question to accept the RQ3 hypothesis. H<sub>3</sub> is accepted and fulfilled by the ranking results of the optimized proposed solution displayed in Chapter 5 to reduce disruptive effects among coupled CII networks against concurrent and consecutive cyberattacks.

- Answering Research Question 4 (RQ4): Can cyber resilience factors and networking metrics provide quantitative evaluation appropriately of dynamic cyber resilience capabilities for the proposed solution and enable comparisons with standard solutions?

Yes. Tran (2015) selected the quantification approach in this research compatible with all balanced quality distribution criteria, including quantitative, capability-based, dynamic, time-dependent, and failure-dependent, compared to other quantification approaches. The choosing of the dynamic cyber resilience factors consists of absorption, volatility, recovery, performance, and recovery time, and related standard simulation and emulation networking metrics. These factors and metrics appropriately measure the dynamic cyber resilience capabilities involve withstanding, mitigation, recovery, and normalization of the single dynamic cyber resilience  $R$  and the total dynamic cyber resilience  $R_{total}$  for the interdependent CII under different testing

scenarios against concurrent and consecutive cyber attacks. They were also enabling comparisons between proposed solution and standard solutions.

- Testing RQ4 Hypothesis:
  - H<sub>4</sub>: Cyber resilience factors and networking metrics appropriately evaluate dynamic cyber resilience capabilities for the proposed solution and enable comparisons with standard solutions.

There is significant evidence based on the positive correlation in the mentioned answer of the fourth research question to accept the RQ4 hypothesis. Therefore, H<sub>4</sub> is accepted and fulfilled by the chosen quantification approach demonstrated in Chapter 2 and Chapter 4 to provide a quantitative evaluation of dynamic cyber resilience factors and networking metrics that appropriately measure dynamic cyber resilience capabilities and enable comparisons among proposed and standard solutions.

- Answering Research Question 5 (RQ5): How can the proposed solution's improvements optimize the capabilities of dynamic cyber resilience for CIIs?

The improvements scheme is harmony combined based on the theoretical requirements indicated in the literature and the empirical observations obtained from the primary quantitative results and analyzed during the primary evaluation phase in this research. The proposed solution's conceptual framework was optimized by adding three new fundamental concepts: hubs coupling, encrypted transmission, and end-to-end service quality. These new concepts have algorithms and protocols re-evaluated through the iterative four-objective cycle to improve the modules of the technology stack of the proposed solution. The first added module contains the fundamental concept of encrypted transmission that uses the HTC algorithm integrated with three protocols:

TWINE protocol, RSA protocol, and SHA protocol. This improvement enhances the withstanding capability of dynamic cyber resilience and the decentralized registry concept, increases the coupled network robustness for reaction to cyber disturbances, and resists cyber failures to sustain its stability. The second added module consists of the fundamental concept of hubs coupling that uses the CSPF algorithm combined with MPLS protocol. This improvement enhances the mitigation capability of dynamic cyber resilience, together with delegated peers' concept, maintains regular redundancy among hub nodes, and replicates their core functions in CII networks to cut down the undesired effects after cyber failures occur. The third added module involves the fundamental concept of end-to-end service quality using the FRP algorithm included with the FRP protocol. This improvement enhances the recovery and normalization capabilities of dynamic cyber resilience, together with the concepts of the consensus rules and dynamic routing, handles resource reservation to different data flows between connected hub nodes, controls functionality requirements, and provides traffic prioritization to guarantee an overall performance level for the coupled network.

- Testing RQ5 Hypothesis:
  - H<sub>5</sub>: The improvements of the proposed solution can optimize dynamic cyber resilience capabilities for CII.

There is significant evidence based on the positive correlation in the declared answer of the fifth research question to accept the RQ5 hypothesis. Therefore, H<sub>5</sub> is accepted and fulfilled by the optimized conceptual framework and the technology stack of the proposed solution established in Chapter 3 to deliver heuristic improvements and reach optimum dynamic cyber resilience capabilities for the proposed solution compared to other standard solutions.

- Answering Research Question 6 (RQ6): Does the optimized proposed solution achieve optimal dynamic cyber resilience capabilities results than standard solutions?

Yes. In the core-core scenarios, the optimized proposed solution was ranked first in the recovery capability, second in the mitigation and the normalization capabilities, and third in the withstanding capability compared to the other standard solutions. Additionally, the optimized proposed solution throughout the core-edge scenarios was ranked first in the recovery capability, second in the normalization capability, and third in the withstanding and the mitigation capabilities contrasted with standard solutions. Lastly, the optimized proposed solution during the core-edge scenarios was ranked first in the recovery capability, third in the normalization capability, and fourth in the withstanding and mitigation capabilities compared to standard solutions. In summary, the optimized proposed solution achieves the optimal results in the recovery capability overall testing scenarios competed to other standard solutions. However, the optimized proposed solution achieves the second-optimal results in the normalization capability during core-core and core-edge scenarios compared to standard solutions. Moreover, the optimized proposed solution achieves the second-optimal results in mitigation capability, and the third-optimal results in normalization capability through the core-core scenario contrasted with the other standard solutions.

- Testing RQ6 Hypothesis:
  - $H_6$ : The optimized proposed solution achieves the optimal results in dynamic cyber resilience capabilities than standard solutions.

There is significant evidence based on the positive correlation in the mentioned answer of the sixth research question to accept the RQ6 hypothesis.  $H_6$  is accepted and fulfilled by the

optimized proposed solution results of the dynamic cyber resilience capabilities presented in Chapter 5. The optimized proposed solution achieves more optimal results in dynamic cyber resilience capabilities than standard solutions.

- Answering Research Question 7 (RQ7): Is the dynamic cyber resilience of the optimized proposed solution higher than the dynamic cyber resilience of standard solutions?

Yes. The optimized proposed solution was ranked first in the total resilience ( $R_{total}$ ) results through all core-core testing scenarios during the optimized evaluation phase in this research competed with the other standard solutions. Furthermore, the optimized proposed solution was ranked second in the total resilience ( $R_{total}$ ) results throughout all core-edge and edge-edge testing scenarios for the duration of the optimized evaluation phase in this study compared to standard solutions.

- Testing RQ7 Hypothesis:
  - $H_7$ : The dynamic cyber resilience of the optimized proposed solution is higher than the dynamic cyber resilience of standard solutions.

There is significant evidence based on the positive correlation in the above answer of the seventh research question to accept the RQ7 hypothesis.  $H_7$  is accepted and fulfilled by the total resilience ( $R_{total}$ ) results of the optimized proposed solution demonstrated in Chapter 5 to emphasize that the dynamic cyber resilience of the optimized proposed solution is partially higher than the dynamic cyber resilience of standard solutions.

### **6.1.2 Accomplishing of the Research Purpose**

In this thesis, the problem statement was still missing a comprehensive technology solution of dynamic cyber resilience using cyber zero-trust engineering in interdependent CIIs. Therefore,



the research purpose was to create a novel proposed solution at theoretical and empirical levels to resolve the problem statement that bridges the critical research gaps resulting from relevant literature.

Upon that, the research purpose was accomplished by achieving the research goal through an iterative four-objective cycle that includes four research objectives: proposed solution development, proposed solution implementation, proposed solution evaluation, and proposed solution optimization. Each research objective within the study has several research questions associated with hypotheses evaluated in detail as follows:

The first research objective (RO1) was developing a conceptual framework and prototyping the novel proposed solution to enhance dynamic cyber resilience capabilities for interdependent CII to continuously deliver their missions and core services continuously under concurrent and consecutive cyberattacks within acceptable timelines and performance levels. This research objective was fulfilled by answering the questions (RQ1) and research question (RQ2) after testing their associated hypotheses formulated to address the RO1.

The second research objective (RO2) implemented the proposed solution using analytical modeling, emulated experiments, and computing simulations. This set of research methods and preparing the generation requirements of testing scenarios and studying the influence of the scale-free topology structure of CII networks on its ability to successfully fulfill dynamic cyber resilience capabilities, understanding the cascading effects in the coupled network of interdependent CII against concurrent and consecutive cyberattacks. This research objective was fulfilled by answering the questions (RQ3) after testing the associated hypothesis formulated to address the RO2.

The third research objective (RO3) was evaluating dynamic cyber resilience capabilities for the

proposed solution based on the quantitative cyber resilience factors correlated with considered networking metrics. Also, performing results analysis of the proposed solution, comparing it with the results of previously standard solutions through identified specific scenarios with the defined network topology, potential cyberattacks, and research methods, and determined the impacts on interdependent CII failures in desired aspects of the proposed solution may be preferred over standard solutions commonly discussed in the literature. This research objective was fulfilled by answering the research question (RQ4) after testing the associated hypotheses formulated to address the RO3.

The fourth research objective (RO4) was to optimize the primary proposed solution after evaluation to enhance the dynamic cyber resilience capabilities of interdependent CII. The new improvements foster the optimized proposed solution by advancing knowledge of the primary proposed solution's strengths and weaknesses, additionally, redesigning the optimization alternatives of the proposed solution and their relations to each other to become more efficient, effective, and able to handle the potential cyberattacks' cascading failures and increase the dynamic cyber resilience to excel the standard solutions. This research objective was fulfilled by answering the research question (RQ5), research question (RQ6), research question (RQ7) after testing their associated hypotheses formulated to address the RO4.

### **6.1.3 Research Outcomes and Expected Implications**

The end-findings of this study are helpful to consider at the outset to streamline producing the thesis outcomes and ensure the accessibility to the research purpose. The primary and optimized results obtained from the research phases influenced how the primary and secondary data are collected, organized, validated, and analyzed.

The study outputs are reporting to might become supportive for the research community; more

focus could be put towards developing future narrative research, whereas academic researchers and professional experts might be more interested in the relevant expected implications. This research's outcomes are the entire reason for the thesis, so it guided each step of the research process from the beginning.

The research outcomes are straightforwardly structured to recapitulate the overall research questions and the associated hypotheses in the above sections and foreshadow the key findings that helped answer these questions. This study's goal and objective are outlined explicitly in the logical sequence that leads directly into the topic research outcomes and their likely identified impacts. Then, the outcomes are synthesized, elaborated, and, most appropriately, summarized substantiations to provide the implications and consistently brought together to reach the research purpose.

Based on the observations were presented in Chapter 5, the research was able to identify and analyze the key findings of this study as per the proposed solution in Chapter 3. As a result, the primary conceptual framework and the technology stack were revisited, examined, and optimized.

Moreover, the development, implementation, evaluation, and optimization of the proposed solution linked with identified research goal and four objectives for this thesis to answer research questions and test the formulated hypotheses, and correlated with their research outcomes and expected implications as followings:

1. The first outcome of this thesis is the bridging of the critical research gaps resulting from relevant literature. Moreover, pay sufficient attention to addressing the related issues properly to shift paradigms towards dynamic cyber resilience and balance proactive and reactive perspectives. This outcome is related to this research goal and purpose. It potentially

influences the theory and practice of cyber resilience research in general and dynamic cyber resilience for critical information infrastructures in particular.

2. The second outcome of this study is the development of the primary conceptual framework and the technology stack of the proposed solution using cyber zero-trust engineering for the first time as a novel solution to enhance dynamic cyber resilience capabilities for interdependent critical information infrastructures against concurrent and consecutive cyberattacks to deliver their core services continuously. This outcome is relevant to the first research objective. Furthermore, it has expected impacts on the interdependent CII networks' capabilities by introducing another unconventional alternative solution not based on cyber trustfulness engineering like the current standard solutions and coping with their shortcomings.
3. The third outcome of this research is implementing the primary proposed solution throughout quantitative research methods of the computing simulations and the emulated experiments for secondary data collecting and validating. This outcome is interrelated to the second research objective. It affects the predictable studying of the coupled CII networks' capabilities with their scale-free topology and decentralized structure to successfully fulfill dynamic cyber resilience and understand their cyber failures under sophisticated cyberattacks.
4. The fourth outcome of this work is evaluating the proposed solution via both intrinsic and extrinsic evaluations. The intrinsic evaluation demonstrated that the proposed solution works appropriately, and the extrinsic evaluation demonstrated the efficiency and effectiveness of the proposed solution for dynamic cyber resilience capabilities in the context of interdependent CIIs. The output data of the testing scenarios for the proposed solution were analyzed using analytical modeling and then compared its results to other standard solutions.

This outcome is correlated with the third research objective. It has prospective effects on the research community. The thesis can ascertain that there are no studies exclusively evaluating capabilities of the proposed solution on the basis of the cyber zero-trust engineering competed with standard solution based on cyber trustfulness engineering.

5. The fifth outcome of this thesis is the optimization of the conceptual framework and technology stack of the proposed solution after evaluation. The new improvements fostered advanced knowledge to enhance the strengths and handle the weaknesses. This outcome is associated with the fourth research objective. It helps widen the outlooks of redesigning the optimization alternatives for the novel adaptive solutions to become more efficient, effective and present significant theoretical and practical influences.

## **6.2 Research Recommendations**

As stated at the beginning of this Chapter, this thesis focused on bridging the critical research gaps and creating a novel proposed solution in the context of dynamic cyber resilience for critical information infrastructures. It puts forward the thesis by analyzing the research results encompassed in the study and extracting conclusions. The success prediction reliability of the research outcomes was represented through further enhanced by final discussions and findings.

In many respects, this research has provided a starting point for using cyber zero-trust engineering for interdependent CII networks by shifting the paradigm toward dynamic cyber resilience. It ensures that the proposed solution's successful production is developed, implemented, evaluated, and optimized.

The following subsections also summarize, in brief, the research limitations that were established, the possible continuations of this work wherein future studies that include more

research inputs of the dynamic cyber resilience capabilities for other new solutions may also add valuable insight.

### **6.2.1 Research Limitations and Alternatives**

In the context of self-criticism of this methodological thesis that looks forward to a new solution and its potential advantages in contradiction of current solutions, focus on the characteristics considered and particular issues that influenced the study findings utilization and their interpretations generalization to establish internal and external validity.

This subsection points out the research limitations and addresses the potential weaknesses. It offers reasons for constraints and discusses common alternatives deeply to present the viable and add-value perspectives. Besides, affect the drawn conclusions and help apply future research opportunities and directions by revising the deficiencies.

Remarkably, some possible limitations in this work that are out of control are not rare; the current study, however, as with the majority of studies, is subject to multiple limitations mentioned below and has to be seen in the light of the design concerns for the methodological research and describe knowledge gaps that can be addressed in the outlook research as the following:

1. The thesis topic is not open, so the previous works were diminutive, and the earlier literature findings were not always published publicly. In particular, no significant papers have existed concerning the dynamic cyber resilience for interdependent CII using cyber zero-trust engineering. The secondary data meta-analysis shortage on cyber interdependency of heterogeneous CII and the scale-free topology vulnerability of coupled CII networks. Likewise, the scarcity of reliable and available prior studies on cyber resilience impacts of concurrent and consecutive cyberattacks against CII causes common, escalating, and cascading failures; it also is among the hardest to rectify and quantify. However, it allows to

add meaningfully to date and formulate an important research methodology for the thesis topic at hand.

2. During this study, the limited access to relevant datasets from official online portals was a rather challenging task because of relatively considered governmentally sensitive and unwilling to disclose with bounding data security and integrity. Due to this limitation, the research has an implementation scope of appropriate measures and primary data collection methods. It was necessary to discover how gathered data help conduct a detailed analysis of the primary and optimized results and reflect on the findings' interpretation in various CIIs scenarios. Amassing dataset values is vital but difficult to obtain and requires deep data processing of all possible causes supported by computational abilities. In similar cases, it needs to redesign the research process differently and ensure that the final findings are valid and reliable.
3. The unforeseen technical challenges limit the research instrumentations during research implementation, such as coverage of execution time, does not examine the direct effects of software packages' testing platforms at the definite cross-experimental period causing delays. If the proposed solution and standard solutions do not reach the specific point of execution or even stoppages, no data can be collected at those points. The research method of computing simulations and emulated experiments are flexible enough and have forecasting power, but they are not standardized and need data to build internal validity of the simulations and emulations within the configuration settings.
4. This empirical research is limited by the applied cyber resilience factors and networking metrics because the interdependent critical information infrastructures comprise different uncorrelated variables, unanticipated aspects, and unexpected events. Furthermore, it

emphasizes the quantitative understanding of the research purpose rather than the quantitative prediction. Therefore, the empirical results reported must be analyzed and discussed given the complexity of coupled CII networks, and the final findings need to be interpreted precisely with caution.

5. The important limitation to the generalization of the research results is the difficulties in running the pilot showcase testing scenarios into the real-world production environment because of high cost and poor accessibility. Additionally, considering that this study was conducted in Dubai, it is regarded as the leading city for technology readiness globally. Therefore, with this showcase acknowledged, the research generalization needs to expand the horizons for interdependent CII networks to transform into the full smart city laid the thesis foundation.

### **6.2.2 Suggestions for Future Works**

In line with the research purpose of contributing to the iterative four-objective cycle of the comprehensive proposed solution, the optimized conceptual framework, technology stack improvements, quantitative methods used, technical instrumentation, testing scenarios setups, and final findings are presented in this thesis is appropriate to follow up and take further applications beyond dynamic cyber resilient CIIs.

It is valuable for the research community to be familiar with the cyber zero-trust engineering in the CIIs space and envision other academic scholars replicate the study results, likely challenges envisage, adapt findings to fit future needs and expectations, broader implications for different parts of the discipline and progress these areas developing over the next years.

Still, there are work scopes for elaborative study on the topic, from the optimized proposed solution to the more optimized solution that could be developed to align with future trends.



Collectively, the researchers might conduct even more collaborative efforts and detailed studies to enhance dynamic cyber resilience implementation to realize that developments into reality with the ever-increasing advancements of the numerous standard solutions or discovering new solutions.

Many recommendations are raised to help future studies expand the proposed solution of dynamic cyber resilience and sharp analysis of various related factors. The following points are the suggestions for future works on the basis of the research outcomes, limitations, and alternatives:

1. Future researches might focus on the dynamic cyber resilience for interdependent CIIs using cyber zero-trust engineering. Given the obstacles to dynamic cyber resilience adoption and implementation, the exploited topology vulnerabilities need to be broadened in coupled CII networks. Likewise, cyber interdependency is an important area of potential investigation in heterogeneous CIIs. Researchers can also strengthen the examining and analyzing the cyber resilience impacts under the likelihood of occurrence for other cyber-attacks across CIIs different cyber failures.
2. Open data available via public and private online portals regarding diverse aspects of critical information infrastructures for research purposes is an additional crucial subject to be studied; sharing the open datasets serves these purposes to examine how dynamic cyber resilience affects national security. Thereby, this study uses several research methods, software tools, and evaluation measures to generate, collect and validate primary data to analyze the proposed solution's capabilities. There is a deeper need for further works by the research community to benefit from the research primary data and provide a profound understanding

for addressing the emerging trends to improve the architecture design of dynamic cyber resilience that directly affects the overall aspects of the CII life cycle.

3. Future researchers recommend adopting mixed methods research (i.e., quantitative and qualitative research methods) to implement the proposed solutions across similar studies. The application of mixed methods research provides an integral overview and considers a consistent alternative for multi-method research used in this thesis. Furthermore, besides quantitative research efficiency, qualitative research improves the primary data reliability through professional knowledge that stems from the expert practices of cyber protection in the CII to overcome the limitations of standard solutions and enhance the study results.
4. Another recommendation is to study the conceptual framework and test the technology stack with different cyber zero-trust algorithms and protocols. Future researchers can focus on examining more fundamental concepts described in this research and refine new proposed solutions to strengthen the cyber resilience aspects of interdependent CII networks. The dynamic cyber resilience is the potential domain of prospect research identified in this thesis that progresses rapidly to play a significant role in the smart city worldwide to help reach CII to become cyber resilient against sophisticated cyberattacks.
5. This study was undertaken in Dubai, targeting effective development and implementing the proposed solution for dynamic cyber resilience. The conceptual framework characteristics success or the validation of the technology stack for other cities is still not tested and requires further support from academic scholars. Hence, they might expand research findings applied to Dubai showcase because it is a pioneer city on future technologies adoptions and implementations. These findings can be generalized across cities in a similar context despite vast technology readiness differences.

## REFERENCES

- Abdelgawad, A., Farstad, T. E., & Gonzalez, J. (2019). *Vulnerability Analysis of Interdependent Critical Infrastructures upon a Cyber-Attack*. In Proceedings of the 52<sup>nd</sup> Hawaii International Conference on System Sciences.
- Abdel-Razeq, S., Zhao, M., Zhou, S., & Wang, Z. (2018). *Optimization of a Two-Hop Network with Energy Conferencing Relays*. International Journal of Wireless & Mobile Networks, 10(1).
- Abdin, I. F., Fang, Y. P., & Zio, E. (2019). *A Modeling and Optimization Framework for Power Systems Design with Operational Flexibility and Resilience against Extreme Heat Waves and Drought Events*. Renewable and Sustainable Energy Reviews, 112(2), pp.706-719.
- Aboshosha, B. W., Dessouky, M. M., Ramadan, R., El-Sayed, A., & Galalb, F. H. (2020). *Evaluation of Lightweight Block Ciphers Based on General FEISTEL Structure (GFS)*. WAS Sci. Nat, 2(1), pp.1-8.
- Acheson, P., and Dagli, C. (2016). *Modeling Resilience in System of Systems Architecture*. Procedia Computer Science, 95(1), pp.111–118.
- Afanador, J., Baptista, M. S., & Oren, N. (2019). *Algorithms for Recursive Delegation*. AI Communications, 32(4), pp.303-317.
- Ajila, S. A. and Chang, Y. (2017). *Using Modified Floyd-Warshall Algorithm to Implement SPB IEEE 802.1 aq Protocol Simulator on NS-3*. International Journal of Computer and Communication Engineering, 6(1), pp.1-8.
- Alcaraz, C. (2018). *Cloud-Assisted Dynamic Resilience for Cyber-Physical Control Systems*. IEEE Wireless Communications, 25(1), pp.76-82.
- Alderson, D. L., Brown, G. G., & Carlyle, W. M. (2015). *Operational Models of Infrastructure Resilience*. Risk Analysis, 35(4), 562-586.
- AlHamdani, W. A. (2020). *Resilient Cybersecurity Architecture*. In 15<sup>th</sup> International Conference on Cyber Warfare and Security. Academic Conferences and publishing limited, pp.23-33.
- AlMajali, A., Viswanathan, A., & Neuman, C. (2012). *Analyzing Resiliency of the Smart Grid Communication Architectures under Cyber-Attack*. In CSET.
- Almoghathawi, Y., Barker, K., & Albert, L. A. (2019). *Resilience-Driven Restoration Model for Interdependent Infrastructure Networks*. Reliability Engineering & Safety, 185(1), pp.12-23.
- Alqahtani, A. (2020). *Smart Interdependent Critical Infrastructures Resilience Enhancement*. Doctoral Dissertation, University of Pittsburgh.
- An, H., Na, Y., Lee, H., & Perrig, A. (2021). *Resilience Evaluation of Multi-Path Routing against Network Attacks and Failures*. Electronics, 10(11), pp.1240.
- Angelo, R. (2019). *Secure Protocols and Virtual Private Networks: An Evaluation*. Issues in Information Systems, 20(3).

- Ani, U. D., Watson, J. M., Nurse, J. R., Cook, A., & Maples, C. (2019). *A Review of Critical Infrastructure Protection Approaches: Improving Security through Responsiveness to the Dynamic Modelling Landscape*. PETRAS/IET Conference Cybersecurity of the IoT, pp.345-368.
- Anne, I., Foros, J., Skaufel, S., Hokstad, P., & Gilje, M. (2018). *Applied Computing and Informatics Interdependencies and Reliability in the Combined ICT and Power System: An Overview of Current Research*. Applied Computing and Informatics, 14(1), pp.17–27.
- Arai, K. (2020). *Routing Protocol Based on Floyd-Warshall Algorithm Allowing Maximization of Throughput*. International Journal Advanced Computing Scientific Application.11(6), pp.436–41.
- Arghandeh, R., Meier, A., Mehrmanesh, L., & Mili, L. (2016). *On Definition of Cyber-Physical Resilience in Power Systems*. Renewable & Sustainable Energy Reviews, 58(1), pp.1060-1069.
- Ashwood-Smith, P. (2010). *Shortest Path Bridging IEEE 802.1 aq Overview and Applications*. In UK Network Operators Forum.
- Assenza, G., Cozzani, V., Flammini, F., Gotcheva, N., Gustafsson, T., Hansson, A., & Oliva, G. (2019). *White Paper on Industry Experiences in Critical Information Infrastructure Security*. International Conference on Critical Information Infrastructures Security, pp.197-207. Springer.
- Aweya, J. (2021). *IP Routing Protocols: Fundamentals and Distance-Vector Routing Protocols*.
- Azhar, N. and Haroon, M. (2019). *Dynamic Load Balancing by Round Robin and Warshall Algorithm in Cloud Computing*. International Journal Innovation Technology Explorer Engineering, 8(9), pp.953–63.
- Baird, L. (2016). *Hashgraph Consensus: Fair, Fast, Byzantine Fault Tolerance*. Swirllds Technical Report, 552(7685), pp.1–28.
- Balchanos, M. G. (2012). *A Probabilistic Technique for the Assessment of Complex Dynamic System Resilience*. Doctoral Dissertation, Georgia Institute of Technology.
- Banerjee, J., Basu, K., & Sen, A. (2018). *On Hardening Problems in Critical Infrastructure Systems*. International Journal of Critical Infrastructure Protection, 23(1), pp.49-67.
- Banescu, S., Wuchner, T., Salem, A., Guggenmos, M., Ochoa, M. & Pretschner, A. (2015). *A Framework for Empirical Evaluation of Malware Detection Resilience against Behavior Obfuscation*. Malicious and Unwanted Software, 10<sup>th</sup> International Conference, pp.40-47. IEEE.
- Bao, F., Chen, R., Chang, M. & Cho, J.H. (2014). *Dynamic Trust Management for Delay Tolerant Networks and its Application to Secure Routing*. IEEE Transactions on Parallel and Distributed Systems, 25(5), pp.1200-1210.
- Barabási, A. L. (2016). *Network science*. Cambridge University Press.
- Barami, B. (2013). *Infrastructure Resiliency: A Risk-Based Framework*. (No.DOT-VNTSC-RITA-13-01). John A. Volpe National Transportation Systems Center (US).
- Barker, K., Lambert, J. H., Zobel, C. W., Tapia, A. H., Albert, L., Nicholson, C. D.(2017). *Defining Resilience Analytics for Interdependent Cyber-Physical-Social Networks*. Sustainable and Resilient Infrastructure, 2(2), pp.59-67.

- Baroud, H., Barker, K., Ramirez-Marquez, J.E. & Rocco, C.M. (2015). *Inherent Costs and Interdependent Impacts of Infrastructure Network Resilience*. Risk Analysis, 35(4), pp.642-662.
- Barrett, B., and Conostas, A. (2014). *Toward a Theory of Resilience for International Development Applications*. National Academy of Sciences, 111(40), pp.14625-14630.
- Başar, T., and Zhu, Q. (2012). *A Dynamic Game-Theoretic Approach to Resilient Control System Design for Cascading Failures*. In Proceedings of the 1<sup>st</sup> International Conference on High Confidence Networked Systems, pp.41-46. ACM.
- Bashan, A., Parshani, R., & Havlin, S. (2011). *Percolation in Networks Composed of Connectivity and Dependency Links*. Physical Review E, 83(5), 051127.
- Begishev, R., Khisamova, I., & Mazitova, I. (2019). *Criminal Legal Ensuring of Security of Critical Information Infrastructure of Russian Federation*. Revista Gêne Direito, 8(6), pp.283-292.
- Behal, S., and Kumar, K. (2016). *Trends in Validation of DDoS Research*. Procedia Computer Science, 85(CMS), pp.7–15.
- Benčić, F. M., and Žarko, I. P. (2018). *Distributed Ledger Technology: Blockchain Compared to Directed Acyclic Graph*. Proceedings of the IEEE 38<sup>th</sup> International Conference on Distributed Computing Systems (ICDCS), pp.1569-1570. IEEE.
- Bensalem, H., Blaquièrre, Y., & Savaria, Y. (2021). *Acceleration of the secure hash algorithm-256 (SHA-256) on an FPGA-CPU cluster using OpenCL*. In 2021 IEEE International Symposium on Circuits and Systems (ISCAS), pp.1-5. IEEE.
- Bergström, J., Van Winsen, R., & Henriqson, E. (2015). *The Rationale of Resilience in the Domain of Safety: A Literature Review*. Reliability Engineering & Safety, 141(2), pp.131-141.
- Beyza, J., Garcia-Paricio, E., & Yusta, J. M. (2019). *Applying Complex Network Theory to the Vulnerability Assessment of Interdependent Energy Infrastructures*. Energies, 12(3), pp.421-432.
- Bhamra, R., Dani, S., & Burnard, K. (2011). *Resilience: The Concept, a Literature Review, and Future Directions*. International Journal of Production Research, 49(18), pp.5375-5393.
- Bhattacharya, R., Nabi, R., Shpitser, I., & Robins, J. M. (2020). *Identification in Missing Data Models Represented by Directed Acyclic Graphs*. In Uncertainty in Artificial Intelligence, pp.1149-1158. PMLR.
- Bhuvaneshwari, T., and Prabakaran, S. (2013). *A Survey on Software Development Life Cycle Models*. International Journal of Computer Science and Mobile Computing, 2(5), pp.262-267.
- Bhuyan, H., Bhattacharya, K. & Kalita, K. (2015). *Empirical Evaluation of Information Metrics for Low-Rate & High-Rate DDoS Attack Detection*. Pattern Recognition Letters, 51(2), pp.1-7.
- Bimonte, S., Sautot, L., Journaux, L., & Faivre, B. (2017). *Multidimensional Model Design using Data Mining: A Rapid Prototyping Methodology*. International Journal of Data Warehousing and Mining (IJDWM), 13(1), pp.1-35.
- Bissell, K., Lasalle, R. M. & Dal, C. P. (2020). *Innovate for Cyber Resilience: Lessons from Leaders to Master Cybersecurity Execution*. 3<sup>rd</sup> Annual State of Cyber Resilience. Technical

Report. Accenture Security.

Björck, F., Henkel, M., Stirna, J. & Zdravkovic, J. (2015). *Cyber Resilience: Fundamentals for a Definition*. New Contributions in Information Systems and Technologies, pp.311-316. Springer.

Blokus, A., and Dziula, P. (2019). *Safety Analysis of Interdependent Critical Infrastructure Networks*. International Journal on Marine Navigation and Safety and Sea Transportation, 13(4).

Bloomfield, R. E., Popov, P., Salako, K., Stankovic, V., & Wright, D. (2017). *Preliminary Interdependency Analysis: An Approach to Support*. Reliability Engineering and System Safety, 167(1), pp.198–217.

Bochkov, A., Lesnykh, V., Zhigirev, N., & Lavrukhin, Y. (2015). *Some Methodical Aspects of Critical Infrastructure Protection*. Safety Science, 79(2), pp.229–242.

Bodeau, D., and Graubart, R. (2013). *Cyber Resiliency Assessment: Enabling Architectural Improvement*. MITRE Technical Report.

Bodeau, D., and Graubart, R. (2016). *Cyber Resiliency Metrics: Key Observations*. MITRE Corporation. (PR Case No. 16-0779).

Bosetti, L., Munshey, M., and Ivanovic, A. (2016). *Fragility, Risk, and Resilience: A Review of Existing Frameworks*. UN University Centre for Policy Research, Background Paper, pp.3-8.

Boumhaout, E. B., Danielsen, A. S., Pedersen, O. B. E., & Shahid, M. (2018). *Towards Zero Trust for Critical Infrastructure: Rethinking the Industrial Demilitarized Zone*. Massachusetts Institute of Technology, pp.1-7.

Bowker, S. L., Stelfox, H. T., & Bagshaw, S. M. (2019). *Critical Care Strategic Clinical Network: Information Infrastructure Ensures a Learning Health System*. CMAJ, 191(Supply), pp.S22-S23.

Bradley, J. M., and Atkins, E. M. (2015). *Optimization and Control of Cyber-Physical Vehicle Systems*. Sensors, 15(9), pp.23020-23049.

Brechbühl, H., Bruce, R., Dynes, S. & Johnson, M.E. (2010). *Protecting Critical Information Infrastructure*. Developing Cybersecurity Policy, pp.83-91.

Brennan, G., Joiner, K., & Sitnikova, E. (2019). *Architectural Choices for Cyber Resilience*. Australian Journal of Multi-Disciplinary Engineering, 15(1), pp.68-74.

Brigantic, R. T., Chatterjee, S., Perkins, C. J., & MacDonald, D. G. (2020). *A Mathematical Framework for Representing Cyber-Physical System Interdependencies and Resilience* (No. PNNL-SA-115668). Pacific Northwest National Lab. (PNNL), Richland, WA (United States).

Broeders, D., and van den Berg, B. (2020). *Governing Cyberspace*. Book. Governing Cyberspace: Behavior, Power, and Diplomacy, 1(2).

Brown, N. J. Vugrin, E. D. & Turnquist, M. A. (2010). *Optimal Recovery Sequencing for Critical Infrastructure Resilience Assessment*. Sandia National Laboratories, Report SAND2010-6237.

Brtis, J., Bodeau, D., Graubart, R., & Salwen, J. (2013). *Resiliency Techniques for Systems-of-*

*Systems*. The MITRE Corporation: Bedford, MA, USA.

Brummitt, C. D., D'Souza, R. M., & Leicht, E. (2012). *Suppressing Cascades of Load in Interdependent Networks*. Proceedings of the National Academy of Sciences of the United States of America, 109(12), pp.E680-E689.

Bucovechi, O. (2020). *Resilience of Critical Infrastructure Index Design between Diversification & Uniformization*. Space Infrastructures: From Risk to Resilience Governance, 57(1), pp.181-202.

Buldyrev, S. V., Gao, J., Stanley, H. E., & Havlin, S. (2012). *Networks Formed from Interdependent Networks*. Nature Physics, 8(1), pp.40-48.

Buldyrev, S. V., Parshani, R., Paul, G., Stanley, H. E., & Havlin, S. (2010). *The Catastrophic Cascade of Failures in Interdependent Networks*. Nature, 464(7291), 1025-1028.

Burla, P., Lindner, C., and Vallée, D. (2016). *Behavior Analysis of Interdependent Critical Infrastructure Components upon Failure*. Reviewed Paper. Proceedings of 21<sup>st</sup> International Conference on Urban Planning, Regional Development and Information Society, pp.107-116.

Cai, B., Xie, M., Liu, Y., Liu, Y. & Feng, Q. (2018). *Availability-Based Engineering Resilience Metric and its Corresponding Evaluation Methodology*. Reliability Engineering & System Safety, 172(2), pp.216-224.

Camphouse, R. C., and Vugrin, E. D. (2011). *Infrastructure Resilience Assessment through Control Design*. International Journal of Critical Infrastructures, 7(3), pp.243-260.

Canzani, E. (2016). *Modeling Dynamics of Disruptive Events for Impact Analysis in Networked Critical Infrastructures*. In ISCRAM.

Canzani, E. (2017). *Dynamic Interdependency Models for Cybersecurity of Critical Infrastructures*. Doctoral Dissertation, Universität Bundeswehr München.

Cao, C., Zhang, Z., Sun, J., Wang, X., & Huang, M. (2017). *Vulnerability Analysis of Interdependent Scale-Free Networks with Complex Coupling*. Reviewed Paper. Journal of Electrical and Computer Engineering.

Carias, J. F., Labaka, L., Sarriegi, J. M., Tapia, A. H., & Hernantes, J. (2019). *The Dynamics of Cyber Resilience Management*. In ISCRAM.

Carlson, J.L., Haffenden, R.A., Bassett, G.W., Buehring, W.A., Collins III, M.J., Folga, S.M., Petit, F.D., Phillips, J.A., Verner, D.R. & Whitfield, R.G. (2012). *Resilience: Theory and Application*. (No. ANL/DIS-12-1). Argonne National Lab. (ANL), Argonne, IL (United States).

Caron, F. (2019). *Obtaining Reasonable Assurance on Cyber Resilience*. Managerial Auditing Journal. Emerald Publishing Limited.

Castillo, A., Arguello, B., Cruz, G., & Swiler, L. (2019). *Cyber-Physical Emulation and Optimization of Worst-Case Cyber Attacks on the Power Grid*. In 2019 Resilience Week (RWS), 1(1), pp.14-18. IEEE.

Caverzan, A., and Solomos, G. (2014). *Review of Resilience in Literature and Standards for Critical Built-Infrastructure*. EC JRC, 90900.

- Cazorla, L., Alcaraz, C., & Lopez, J. (2016). *Cyber Stealth Attacks in Critical Information Infrastructures*. IEEE Systems Journal, 12(2), pp.1778-1792.
- Cedergren, A., Johansson, J. & Hassel, H. (2018). *Challenges to Critical Infrastructure Resilience in an Institutionally Fragmented Setting*. Safety Science, 110(4), pp.51-58.
- Cetinkaya, E.K., Alenazi, M.J., Rohrer, J.P. & Sterbenz, J.P. (2017). *Topology Connectivity Analysis of Internet Infrastructure Using Graph Spectra*. In Ultra-Modern Telecommunications and Control Systems and Workshops (ICUMT), International Congress on IEEE, pp.752-758.
- Chaves, A., Rice, M., Dunlap, S., & Pecarina, J. (2017). *Improving Cyber Resilience of Industrial Control Systems*. International Journal of Critical Infrastructure Protection, 17(3), pp.30-48.
- Chen, L., and Atwood, J. W. (2018). *Performance Evaluation for Secure Internet Group Management Protocol and Group Security Association Management Protocol*. Proceedings of the IEEE Canadian Conference on Electrical & Computer Engineering (CCECE), pp.1-5. IEEE.
- Chen, X. (2016). *System Vulnerability Assessment and Critical Nodes Identification*. Expert Systems with Applications, 65(2), pp.212–220.
- Chmutina, K., Lizarralde, G., Dainty, A., & Bosher, L. (2016). *Unpacking Resilience Policy Discourse*. Cities, 58(1), pp.70-79.
- Choi, S. M., Park, J., Jang, K., & Park, C. (2020). *Rapid Consensus Structure: Continuous Common Knowledge in Asynchronous Distributed Systems*. Mathematics, 8(10), pp.1673.
- Choras, M., Kozik, R., Bruna, M. T., Yautsiukhin, A., Churchill, A., Maciejewska, I. & Jomni, A. (2015). *Comprehensive Approach to Increase Cyber Security and Resilience*. In 10<sup>th</sup> International Conference on Availability, Reliability, and Security, pp.686-692. IEEE.
- Choudhury, S., Rodriguez, L., Curtis, D., Oler, K., Nordquist, P., Chen, P.Y. & Ray, I. (2015). *Action Recommendation for Cyber Resilience*. In Proceedings of the 2015 Workshop on Automated Decision Making for Active Cyber Defense, pp.3-8. ACM.
- Chowdhury, S., Zhu, J., & Zhang, W. (2020). *Optimized Restoration Planning of Infrastructure System-of-Systems using Heterogeneous Network Flow Simulation*. Journal of Computing in Civil Engineering, 34(5), 04020032.
- Conklin, W. A., and Kohnke, A. (2017). *Teaching Cyber Resilience for Critical Infrastructure Systems*. In Journal of Colloquium for Information System Security Education, 5 (1), pp.15-15.
- Conti, M., Dargahi, T., & Dehghantanha, A. (2018). *Cyber Threat Intelligence: Challenges and Opportunities*. In Cyber Threat Intelligence, pp.1-6. Springer, Cham.
- Couteau, G., Peters, T., & Pointcheval, D. (2016). *Encryption Switching Protocols*. In Annual International Cryptology Conference, pp.308-338. Springer, Berlin, Heidelberg.
- Crary, K. (2020). *Verifying the Hashgraph Consensus Algorithm*. arXiv preprint arXiv:2102.01167.
- Creese, S., Goldsmith, M. H., & Adetoye, A. O. (2011). *A Logical High-Level Framework for Critical Infrastructure Resilience and Risk Assessment*. In 2011 Third International Workshop on



Cyberspace Safety and Security (CSS), pp.7-14. IEEE.

Dan-Suteu, S. A., and Gânsac, V. (2020). *The platform for Simulating Cyber Resilience of Critical Industrial Infrastructures ICS-SCADA*. In International Scientific Conference "Strategies XXI," pp.356-360. "Carol I" National Defense University.

Danziger, M., Shekhtman, L., Bashan, A., Berezin, Y., & Havlin, S. (2016). *Vulnerability of Interdependent Networks & Networks-of-Networks*. Interconnected Networks, pp.79-99. Springer.

Das, L., Munikoti, S., Natarajan, B., & Srinivasan, B. (2020). *Measuring Smart Grid Resilience: Methods, Challenges & Opportunities*. Renewable & Sustainable Energy Reviews, 130(2), 10991.

Davendralingam, N., and DeLaurentis, D. (2013). *A Robust Optimization Framework to Architecting System of Systems*. Procedia Computer Science, 16(1), pp.255-264.

De Florio, V. (2015). *On Resilient Behaviors in Computational Systems and Environments*. Journal of Reliable Intelligent Environments, 1(1), pp.33-46.

Deng, Y., Song, L., Zhou, Z., & Liu, P. (2017). *Complexity and Vulnerability Analysis of Critical Infrastructures: A Methodological Approach*. Mathematical Problems in Engineering.

DhivyaShree, M., and Sandhiya, C. (2016). *Virtual Voting using Visual Cryptography*. COMPUSOFT: An International Journal of Advanced Computer Technology.

Di Pietro, A., Foglietta, C., Palmieri, S. & Panzieri, S. (2017). *Assessing the Impact of Cyber Attacks on Interdependent Physical Systems*. In International Conference on Critical Infrastructure Protection, pp.215-227. Springer, Berlin, Heidelberg.

Dibaji, S.M., and Ishii, H. (2015). *Resilient Multi-Agent Consensus with Asynchrony and Delayed Information*. IFAC-Papers Online, 48(22), pp.28-33.

Dimase, D., Collier, Z. A., Heffner, K., & Linkov, I. (2015). *Systems Engineering Framework for Cyber-Physical Security and Resilience*. Environment Systems & Decisions, 35(2), pp.291–300.

Dinitz, Y., and Itzhak, R. (2017). *Hybrid Bellman-Ford–Dijkstra Algorithm*. Journal of Discrete Algorithms, 42(2), pp. 35-44.

Divakaran, D. M., Ko, L. L., Su, L., & Thing, V. L. (2017). *REX: Resilient and Efficient Data Structure for Tracking Network Flows*. Computer Networks, 118(3), pp. 37-53.

Djojo, M. A., and Karyono, K. (2013). *Computational Load Analysis of Dijkstra, A\*, and Floyd-Warshall Algorithms in Mesh Network*. International Conference on Robotics, Bioinformatics, Intelligent Computational Systems, pp.104-108. IEEE.

Dong, G., Gao, J., Du, R., Tian, L., Stanley, H. E., & Havlin, S. (2013). *Robustness of Network of Networks under Targeted Attack*. Physical Review E, 87(5), 052804.

Dong, G., Gao, J., Tian, L., Du, R., & He, Y. (2012). *Percolation of Interdependent Networks Partially under Targeted Attack*. Physical Review E, 85(1), 016112.

Dowling, B., Fischlin, M., Günther, F., & Stebila, D. (2020). *A Cryptographic Analysis of the TLS 1.3 Handshake Protocol*. Journal of Cryptology, pp.197-210.

- Dsouza, G., Hariri, S., Al-Nashif, Y., & Rodriguez, G. (2013). *Resilient Dynamic Data-Driven Application Systems (RDDDAS)*. *Procedia Computer Science*, 18(3), pp. 1929-1938.
- Du, W.B., Chen, Z., Cao, X.B. & Zhou, X.L. (2015). *Cascading Failure of Interdependent Networks with Different Coupling Preference under Targeted Attack*. *Chaos, Solitons & Fractals*, 80(3), pp.7-12.
- Dueñas-Osorio, L., and Ouyang, M. (2011). *An Approach to Design Interface Topologies across Interdependent Urban Infrastructure Systems*. *Reliability Engineering & System Safety*, 96(11), pp.1462-1473.
- Dunn Caveltly, M., Kaufmann, M. & Sjøby Kristensen, K. (2015). *Resilience and (in) Security: Practices, Subjects, Temporalities*. *Security Dialogue*, 46(1), pp.3-14.
- Dunn, M. A., and Kristensen, K. S. (2020). *Securing 'The Homeland': Critical Infrastructure, Risk, and (in) Security*. Routledge.
- Dünner, C., Lucchi, A., Gargiani, M., Bian, A., Hofmann, T., & Jaggi, M. (2018). *A Distributed Second-Order Algorithm can Trust*. arXiv preprint arXiv:1806.07569.
- Dupont, B. (2019). *The Cyber-Resilience of Financial Institutions: Significance and Applicability*. *Journal of Cybersecurity*, 5(1), tyz013.
- Eidle, D., Ni, S. Y., DeCusatis, C., & Sager, A. (2017). *Autonomic Security for Zero Trust Networks*. In 8<sup>th</sup> Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), pp.288-293. IEEE.
- El Ioini, N., and Pahl, C., (2018). *A Review of Distributed Ledger Technologies*. *Lectures Note Computing Science. Bioinformatics*, 11230 LNCS, pp.277–88.
- Eldosouky, M. (2019). *Security of Critical Cyber-Physical Systems: Fundamentals and Optimization*. Doctoral Dissertation, Virginia University.
- Emiliano, R., and Antunes, M. (2015). *Automatic Network Configuration in Virtualized Environment using GNS3*. In 2015 10<sup>th</sup> International Conference on Computer Science & Education (ICCSE), pp.25-30. IEEE.
- Erokhin, S. D. (2019). *Managing Security of Critical Information Infrastructure*. In *Systems of Signal Synchronization, Generating and Processing in Telecommunications*, pp.1-4. IEEE.
- Etigowni, S., Tian, D., Hernandez, G., Zonouz, S., & Butler, K. (2016). *CPAC: Securing Critical Infrastructure with Cyber-Physical Access Control*. In *Proceedings of the 32<sup>nd</sup> Annual Conference on Computer Security Applications*, pp.139-152.
- Etzioni, A. (2019). *Cyber Trust*. *Journal of Business Ethics*, 156(1), pp.1-13.
- Fan, W.L., Liu, Z.G. & Hu, P. (2014). *A High Robustness and Low-Cost Cascading Failure Model Based on Node Importance in Complex Networks*. *Modern Physics Letters B*, 28(02), pp.1450011.
- Fan, X., Liu, L., Zhang, R., Jin, Q., & Bi, J. (2020). *Decentralized Trust Management: Risk Analysis and Trust Aggregation*. *ACM Computing Surveys (CSUR)*, 53(1), pp.1-33.

- Fang, Y., and Ouyang, M. (2017). *A Mathematical Framework to Optimize Critical Infrastructure Resilience against Intentional Attacks*. *Computer-Aided Civil and Infrastructure Engineering*, 32(11), pp.909-929.
- Fang, Y., and Sansavini, G. (2017). *Optimizing Power System Investments and Resilience against Attacks*. *Reliability Engineering & System Safety*, 159(3), pp.161-173.
- Fang, Y., and Sansavini, G. (2018). *Emergence of Antifragility by Optimum Post Disruption Restoration Planning of Infrastructure Networks*. *Journal of Infrastructure Systems*, 23(4), pp.04702.
- Faramondi, L., Oliva, G., & Setola, R. (2020). *Multi-Criteria Node Criticality Assessment Framework for Critical Infrastructure Networks*. *International Journal of Critical Infrastructure Protection*, 28(100338).
- Fernando, T., Guo, H., Zheng, C. & Iu, H. (2017). *Critical Review of Cascading Failure Analysis and Modeling of Power System*. *Renewable & Sustainable Energy Reviews*, 80(5), pp.9-22.
- Ferrari, P., Flammini, A., Rinaldi, S., Prytz, G., & Hussain, R. (2014). *Multipath Redundancy for Industrial Networks using IEEE 802.1aq Shortest Path Bridging*. In 2014 10<sup>th</sup> IEEE Workshop on Factory Communication Systems (WFCS 2014), pp.1-10. IEEE.
- Ferreira, A. (2019). *Vulnerability Analysis in Critical Infrastructures: A Methodology*. *Security and Defense Quarterly*, 24(2), pp.65-86.
- Filippini, R., and Silva, A. (2012). *Resilience Analysis of Networked Systems-of-Systems based on Structural and Dynamic Interdependencies*. In PSAM 11(2), pp.10-22.
- Fotouhi, H., Moryadee, S., & Miller-hooks, E. (2017). *Quantifying the Resilience of an Urban Traffic-Electric Power Coupled System*. *Reliability Engineering & Safety*, 163(12), pp.79–94.
- Fraccascia, L., Giannoccaro, I., & Albino, V. (2018). *The Resilience of Complex Systems: State of the Art and Directions for Future Research*. *Complexity*, 2018.
- Francia, G., Ertaul, L., Encinas, L. H., & El-Sheikh, E. (2018). *Computer and Network Security Essentials*. Book. Springer.
- Francis, R., and Bekera, B. (2014). *Resilience Analysis for Engineered & Infrastructures under Deep Uncertainty or Emergent Conditions*. *Reliability Engineering & Safety*, 121(4), pp.90-103.
- Friedman, C. P., Rubin, J. C., & Sullivan, K. J. (2017). *Toward an Information Infrastructure for Global Health Improvement*. *Yearbook of Medical Informatics*, 26(1), pp.16-38.
- Gągol, A., and Świątek, M. (2018). *Aleph: A Leaderless, Asynchronous, Byzantine Fault Tolerant Consensus Protocol*. *arXiv preprint arXiv:1810.05256*.
- Galar, Z. (2018). *Distributed Ledger Technology as an Instrument of Decentralized Management*. *Przegląd Nauk Ekonomicznych*, 1(28), pp.129-139.
- Gamboa, Y. B. G., Ramírez-Cabrales, F., & Jiménez, J. A. M. (2020). *Cyber Security Vulnerabilities in Colombia's Maritime Critical Infrastructure (MCI)*. In *International Conference of Research Applied to Defense and Security*, pp.3-15. Springer, Singapore.

- Gao, J., Barzel, B. & Barabási, A.L. (2016). *Universal Resilience Patterns in Complex Networks*. *Nature*, 530(7590), pp.307-315.
- Gasser, P., Lustenberg, P., Cineli, M., Kim, W., Spada, M., Burgher, P. & Sun, Y. (2019). *Review of Resilience Assessment of Energy Systems*. *Sustainable & Resilient Infrastructure*, pp.1-27.
- Gatchin, Y. A., and Sukhostat, V. V. (2019). *Research of Vulnerabilities of Information Processing Processes Systems of Critical Information Infrastructure*. *Wave Electronics and Its Application in Information and Telecommunication Systems (WECONF)*, pp.1-4. IEEE.
- Georgiev, I. and Nikolova, K. (2017). *An Approach of DNS Protection against DDoS Attacks*. In *Proceeding 13<sup>th</sup> International Conference Advanced Technologies, Systems & Services in Telecommunications*, pp.140–143, IEEE.
- Ghanbari, R., Jalili, M., & Yu, X. (2018). *Correlation of Cascade Failures and Centrality Measures in Complex Networks*. *Future Generation Computer Systems*, 83(3), pp.390-400.
- Gilman, E. and Barth, D. (2017). *Zero Trust Networks*. O'Reilly Media, Incorporated.
- Giri, K., Saxena, N., Srivastava, Y. & Saxena, P. (2020). *End-to-End Encryption Techniques*. 1089(1), pp.93.
- Gisladottir, V., Ganin, A. A., Keisler, J. M., Kepner, J., & Linkov, I. (2017). *The Resilience of Cyber Systems with over-and-under Regulation*. *Risk Analysis*, 37(9), pp.1644-1651.
- Gissibl, N., and Klüppelberg, C. (2018). *Max Linear Models on Directed Acyclic Graphs*. *Bernoulli*, 24(4A), pp.2693-2720.
- Glesk, I., Abuhelala, M. & Masood, M. (2016). *Detailed Analysis of Routing Protocols with Different Network Limitations*. In *20<sup>th</sup> Slovak-Czech-Polish Optical Conference on Wave and Quantum Aspects of Contemporary Optics (1)10142*, pp.101421T.
- Gnatyuk, S., Polishchuk, Y., Sydorenko, V., & Sotnichenko, Y. (2019). *Determining the Level of Importance for Critical Information Infrastructure Objects*. In *International Scientific-Practical Conference Problems of Info Communications, Science & Technology*, pp.829-834. IEEE.
- Godán, F., Colman, S., & Grampín, E. (2016). *Multicast BGP with SDN Control Plane*. *Proceedings of 7<sup>th</sup> International Conference on the Network of the Future (NOF)*, pp.1-5. IEEE.
- Goebel, K., Zhang, X., Mahadevan, S. & Sankararaman, S. (2018). *Resilience-Based Network Design under Uncertainty*. *Reliability Engineering & System Safety*, 169(2), pp.364-379.
- Goldbeck, N., Angeloudis, P., & Ochieng, W. Y. (2019). *Resilience Assessment for Interdependent Urban Infrastructure Systems using Dynamic Network Flow Models*. *Reliability Engineering & System Safety*, 188(2), pp.62-79.
- Golnari, G., and Zhang, Z. L. (2015). *The Effect of Different Couplings on Mitigating Failure Cascades in Interdependent Networks*. In *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHP)*, pp.677-682. IEEE.
- González, A. D., Dueñas-Osorio, L., Sánchez-Silva, M., & Medaglia, A. L. (2016). *The Interdependent Network Design Problem for Optimal Infrastructure System*

- Restoration*. Computer-Aided Civil and Infrastructure Engineering, 31(5), pp.334-350.
- Grachkov, I. A. and Malyuk, A. A. (2020). *Development Problems of Trusted Software in Critical Information Infrastructure Systems*. In *Advanced Technologies in Robotics and Intelligent Systems*, pp.55-62. Springer, Cham.
- Grafenauer, T., König, S., Rass, S., & Schauer, S. (2018). *A Simulation Tool for Cascading Effects in Interdependent Critical Infrastructures*. In *Proceedings of the 13<sup>th</sup> International Conference on Availability, Reliability, and Security*, pp.1-8.
- Graubart, R., and Bodeau, D. (2016). *Structured Cyber Resiliency Analysis Methodology*. (SCRAM), (PR Case, No. 6-0777).
- Graubart, R., and Bodeau, D. (2017). *Cyber Resiliency Design Principles: Selective use throughout the Lifecycle and Conjunction with Related Disciplines*, 3(17), pp.90-98.
- Green, O. (2019). *HashGraph - Scalable Hash Tables Using a Sparse Graph Data Structure*. arXiv preprint arXiv:1907.02900.
- Greenhalgh, T., Wherton, J., Shaw, S., Papoutsis, C., Vijayaraghavan, S., & Stones, R. (2019). *Infrastructure Revisited an Ethnographic Case Study of how Health Information Infrastructure Shapes and Constraints Technological Innovation*. *Journal of Medical Internet Research*, 21(12).
- Gritzalis, D., Theocharidou, M., & Stergiopoulos, G. (2019). *Critical Infrastructure Security and Resilience*. Book. Cham: Springer.
- Guo, J. (2010). *A Network-Based System for Assessment and Management of Infrastructure Interdependency*. Doctoral Dissertation. Concordia University.
- Gupta, P. and Kumar, S. (2014). *A Comparative Analysis of SHA and MD5 Algorithm*. *Architecture*, 1(1), pp.5.
- Gutfraind, A. (2010). *Optimizing Topological Cascade Resilience Based on the Structure of Terrorist Networks*. *PloS one*, 5(11), e13448.
- Hadjoannou, V. (2015). *The Performance Comparison of RIP, OSPF, IS-IS, and EIGRP Routing Protocols*. arXiv preprint arXiv:1502.07133.
- Hadjsaid, N., Viziteu, M., Rozel, B., Caire, R., Sabonnadière, J. C., Georges, D., & Tranchita, C. (2010). *Interdependencies of Coupled Heterogeneous Infrastructures: Case of ICT & Energy*.
- Han, D., Mo, Y. & Xie, L. (2016). *Resilience and Performance Analysis for State Estimation against Integrity Attacks*. *IFAC-Papers Online*, 49(22), pp.55-60.
- Hansen, M. S. (2019). *A Study of the Danish Critical Information Infrastructure Protection Systems of Governance*. A Multi-Scale Systems Representation of the Danish Critical Information Infrastructure. Aalborg University, Denmark.
- Haque, M. A., De Teyou, G. K., Shetty, S., & Krishnappa, B. (2018). *Cyber Resilience Framework for Industrial Control Systems: Concepts, Metrics, and Insights*. In *2018 IEEE International Conference on Intelligence and Security Informatics (ISI)*, pp.25-30. IEEE.

- Haque, M. A., Shetty, S., & Krishnappa, B. (2019). ICS-CRAT: A Cyber Resilience Assessment Tool for Industrial Control Systems. In 2019 IEEE 5<sup>th</sup> Intl Conference on Intelligent Data and Security (IDS), pp.273-281. IEEE.
- Häring, I., Ebenhöch, S., and Stolz, A. (2016). *Quantifying Resilience for Resilience Engineering of Socio-Technical Systems*. European Journal for Security Research, 1(1), pp.21-58.
- Harrison, T. P., Zhao, K., & Yen, J. (2011). *Analyzing the Resilience of Complex Supply Network Topologies against Random and Targeted Disruptions*. IEEE Systems Journal, 5(1), pp.28-39.
- Harrop, W., and Matteson, A. (2015). *Cyber Resilience: A Review of Critical National Infrastructure and Cyber-Security Protection Measures Applied in the UK and USA*. In Current and Emerging Trends in Cyber Operations, pp.149-166. Palgrave Macmillan, London.
- Hausken, K. (2020). *Cyber Resilience in Firms, Organizations, and Societies*. IoT, 100204.
- Hayel, Y., and Zhu, Q. (2015). *Resilient and Secure Network Design for Cyber Attack-Induced Cascading Link Failures in Critical Infrastructures*. In Information Sciences and Systems (CISS), 2015 49<sup>th</sup> Annual Conference on IEEE, pp.1-3.
- Häyhtiö, M., and Zaerens, K. (2017). *A Comprehensive Assessment Model for Critical Infrastructure Protection*. Management and Production Engineering Review, 8(3).
- Hehenberger, P., Vogel-Heuser, B., Bradley, D., Eynard, B., Tomiyama, T. & Achiche, S. (2016). *Design, Modelling, Simulation, and Integration of Cyber-Physical Systems: Methods and Applications*. Computers in Industry, 82(1), pp.273-289.
- Heinbockel, W., Graubart, R. & Bodeau, D. (2013). *Characterizing Effects on the Cyber Adversary*. MTR130432, MITRE Corporation.
- Helfgott, A. (2018). *Operationalizing Systemic Resilience*. European Journal of Operational Research, 268(3), pp.852-864.
- Herrera, L. C., and Maennel, O. (2019). *A Comprehensive Instrument for Identifying Critical Information Infrastructure Services*. International Journal of Critical Infrastructure Protection, 25(2), pp.50-61.
- Herrington, L., and Aldrich, R. (2013). *The Future of Cyber-Resilience in an Age of Global Complexity*. Politics, 33(4), pp.299-310.
- Herrmann, H. J., Schneider, C. M., Moreira, A. A., Andrade Jr, J. S., & Havlin, S. (2011). *Onion-Like Network Topology Enhances Robustness against Malicious Attacks*. Journal of Statistical Mechanics: Theory and Experiment, 2011(01), P01027.
- Herrmann, J., Ozkaya, M. Y., Uçar, B., Kaya, K., & Çatalyürek, U. V. (2019). *Multilevel Algorithms for Acyclic Partitioning of Directed Acyclic Graphs*. SIAM Journal on Scientific Computing, 41(4), pp.A2117-A2145.
- Hofreiter, L., and Zvaková, Z. (2017). *Theoretical Aspects of Critical Infrastructure Protection*. Durability of Critical Infrastructure, Monitoring, and Testing, pp.139-147. Springer, Singapore.
- Hokstad, P., Utne, I. B., & Vatn, J. (2012). *Risk and Interdependencies in Critical*

*Infrastructures*. Book. London: Springer.

Holden, R., Val, D. V., Burkhard, R., & Nodwell, S. (2013). *A Network Flow Model for Interdependent Infrastructures at the Local Scale*. *Safety Science*, 53(6), pp.51-60.

Hong, L. Wang, S., & Chen, X. (2012). *Vulnerability Analysis of Interdependent Infrastructure Systems: A Methodological Framework*. *Physica A: Statistical Mechanics and its Applications*, 391(11), pp.3323-3335.

Hoxha, L. (2018). *Hashgraph The Future of Decentralized Technology and The End of Blockchain*. *European Journal of Engineering and Formal Sciences*, 86(1), pp.68-84.

Hromada, M., Rehak, D., Senovsky, P., Lovecek, T., & Novotny, P. (2018). *Cascading Impact Assessment in a Critical Infrastructure System*. *International Journal of Critical Infrastructure Protection*, 22(1), pp.125-138.

Huang, X., Gao, J., Buldyrev, S. V., Havlin, S., & Stanley, H. E. (2011). *Robustness of Interdependent Networks under Targeted Attack*. *Physical Review E*, 83(6), 065101.

Hui, Q., Zeng, X., & Liu, Z. (2014). *Energy Equipartition Stabilization and Cascading Resilience Optimization for Geospatially Distributed Cyber-Physical Network Systems*. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 45(1), pp.25-43.

Igor, B., and Aleksandr, R. (2018). *The Methodology of Security Assessment Automated Systems as Objects Critical Information Infrastructure*. *Вопросы кибербезопасности*, 1(25).

Ip, W. H., and Wang, D. (2011). *Resilience and Friability of Transportation Networks: Evaluation, Analysis, and Optimization*. *IEEE Systems Journal*, 5(2), pp.189-198.

Ishii, H., and Dibaji, S. M. (2017). *Resilient Consensus of Second-Order Agent Networks: Asynchronous Update Rules with Delays*. *Automatica*, 81(123), pp.32.

Jahromi, A. A., Kemmeugne, A., Kundur, D., & Haddadi, A. (2019). *Cyber-Physical Attacks Targeting Communication-Assisted Protection Schemes*. *IEEE Transactions on Power Systems*, 35(1), pp.440-450.

James, J., Hawthorne, D., Duncan, K., St. Leger, A., Sagisi, J., & Collins, M. (2019). *An Experimental Framework for Investigating Hashgraph Algorithm Transaction Speed*. *Proceedings of the Second Workshop on Blockchain-enabled Networked Sensor*, pp.15-21.

Jarry, A. (2013). *Fast Reroute Paths Algorithms*. *Telecommunication Systems*, 52(2), pp.881-888.

Jiang, W., Liu, B., Wang, C., & Yang, X. (2021). *Security-Oriented Network Architecture*. *Security and Communication Networks*, 2021.

Jiang, Y., Ding, J., Atif, Y., Jeusfeld, M., Andler, S., Lindström, B., & Haglund, D. (2018). *Complex Dependencies Analysis: Technical Description of Complex Dependencies in Critical Infrastructures*. The University of Skövde.

Jin, Y. (2021). *Systems for Analyzing Routing Policies and Localizing Faults on the Internet*. Doctoral dissertation, University of Washington.

- Johnson, P., Lagerström, R., & Ekstedt, M. (2018). *A Meta Language for Threat Modeling and Attack Simulations*. In Proceedings of the 13<sup>th</sup> International Conference on Availability, Reliability, and Security, pp.1-8.
- Johnson, T. A. (2015). *Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare*. CRC Press.
- Johnston, M., Lee, W., & Modiano, E. (2014). *A Robust Optimization Approach to Backup Network Design with Random Failures*. IEEE/ACM Transactions on Networking, 23(4), pp.1216-1228.
- Joshi, V. C. (2020). *Cyber-Risk Management*. In Digital Finance, Bits and Bytes, pp.131-150. Palgrave Macmillan, Singapore.
- Junfeng, T. I. A. N., Xueqing, Q. U., Xinfeng, H. E., & Zhen, L. I. (2020). *The Method of Virtual Machine Live Migration Based on HashGraph*. Journal of Electronics and Information, 42(3), pp.712-719.
- Kalala, K. (2017). *Trust and Reputation Algorithms for Hierarchically Structured Peer-To-Peer Systems*. Doctoral Dissertation. The University of Ottawa.
- Kalashnikov, A., and Sakrutina, E. (2019). *"Safety Management System" and Significant Plants of Critical Information Infrastructure*. IFAC-Papers Online, 52(13), pp.1391-1396.
- Kalpna, M., and Tyagi, A. (2017). *Bellman-Ford Shortest Path Algorithm using Global Positioning System*. International Research Journal of Engineering & Technology, 4(4), pp.12-18.
- Kamissoko, D., Nastov, B., Benaben, F., Chapurlat, V., Bony-Dandrieux, A., Tixier, J. & Daclin, N. (2019). *Continuous and Multidimensional Assessment of Resilience Based on Functionality Analysis for Interconnected Systems*. Structure and Infrastructure Engineering, 15(4), pp.427-442.
- Karabacak, B., Yildirim, S.O. & Baykal, N. (2016). *A Vulnerability-Driven Cyber Security Maturity Model for Measuring National Critical Infrastructure Protection Preparedness*. International Journal of Critical Infrastructure Protection, 15(7), pp.47-59.
- Karakoc, D. B., Almoghathawi, Y., Barker, K., González, A. D., & Mohebbi, S. (2019). *Community Resilience-Driven Restoration Model for Interdependent Infrastructure Networks*. International Journal of Disaster Risk Reduction, 38(1), 101228.
- Karakoc, D. B., Barker, K., & Almoghathawi, Y. (2019). *Interdependent Infrastructure Network Restoration Optimization from Community and Spatial Resilience Perspectives*. In INOC, pp.1-6.
- Karjanto, N., and Husain, H. S. (2017). *Adopting Maxima as an Open-Source Computer Algebra System into Mathematics Teaching and Learning*. In Proceedings of the 13<sup>th</sup> International Congress on Mathematical Education, pp.733-734. Springer, Cham.
- Kempf, J., Whyte, S., Ellithorpe, J., Kazemian, P., Haitjema, M., Beheshti, N. & Green, H. (2011). *Open Flow MPLS and the Open-Source Label Switched Router*. Proceedings of the 23<sup>rd</sup> International Telecommunication Traffic Congress (ITC), pp.8-14. IEEE.
- Kerman, A., Borchert, O., Rose, S., & Tan, A. (2020). *Implementing A Zero Trust*



- Architecture*. The MITRE Corporation, Technical Report.
- Kessler, G. C. (2016). *An Overview of Cryptography*. Updated Version, pp.1-71.
- Khan, S. (2021). *CLIFD: A Novel Image Forgery Detection Technique using Digital Signatures*. *Journal of Engineering Research*, 9(1).
- Kindervag, J. (2010). *Build Security into your Network's DNA: The Zero Trust Network Architecture*. Forrester Research Inc, pp.1-26.
- Kindervag, J. (2016). *No More Chewy Centers: The Zero Trust Model of Information Security*. Forrester Research, Inc., pp.23-34.
- Kiss, I., Genge, B., & Haller, P. (2015). *A System Dynamics Approach for Assessing the Impact of Cyber-Attacks on Critical Infrastructures*. *International Journal of Critical Infrastructure Protection*, 10(4), pp.3-17.
- Kizza, J. M. (2020). *Guide to Computer Network Security*. Book, pp.387-411. Berlin: Springer.
- Klein, P., and Klein, F. (2019). *Dynamics of Interdependent Critical Infrastructures: A Mathematical Model with Unexpected Results*. *International Journal of Critical Infrastructure Protection*, 24(1), pp.69-77.
- Kochedykov, S. S., Novoseltsev, V. I., Kobzistyy, S. Y., Dushkin, A. V., & Smolyakova, S. D. (2020). *Algorithm and Method for Recognizing Critical Situations Using Semantic Networks on Critical Information Infrastructure Facilities because of Cyber Attacks*. In *Conference of Russian Young Researchers in Electrical and Electronic Engineering*, pp.2066-2071. IEEE.
- Kolokotronis, N., Shiaeles, S., Bellini, E., Charalambous, L., Kavallieros, D., Gkotsopoulou, O. & Sargsyan, G. (2019). *Cyber-Trust: The Shield for IoT Cyber-Attacks*. *Resilience and Hybrid Threats*; IOS Press: Amsterdam, Netherlands, pp.76-93.
- König, S., and Rass, S. (2017). *Stochastic Dependencies between Critical Infrastructures*. Rome, Italy, pp.106-110.
- Kott, A., and Linkov, I. (2019). *Cyber resilience of systems and networks*. Book, pp.381-401. Springer International Publishing.
- Koutsoukos, X., and Sundaram, S. (2013). *Robust Networks*. 31(4), pp.766–81.
- Krupp, J. and Rossow, C. (2021). *BGPeeek-a-Boo: Active BGP-based Traceback for Amplification DDoS Attacks*. arXiv preprint arXiv:2103.08440.
- Kulkarni, D., Sharma, N., Shinde, P., & Varma, V. (2015). *Parallelization of Shortest Path Finder on GPU: Floyd-Warshall*. *International Journal of Computer Applications*, 110(16).
- Kumar, B. K., Reddy, E. S. (2020). *Modified Floyd Warshall Algorithm for Cache Management in Information-Centric Network*. *International Journal for Intelligence Engineering Systems*, 13(1), pp.146–55.
- Kumar, D., Khan, A. H., Nayyar, H., & Gupta, V. (2020). *Cyber Risk Assessment Model for Critical Information Infrastructure*. In *2020 International Conference on Power Electronics &*

- IoT Applications in Renewable Energy and Control (PARC), pp.292-297. IEEE.
- Labaka, L., Hernantes, J. & Sarriegi, J.M. (2017). *A Framework to Improve the Resilience of Critical Infrastructures*. International Journal of Disaster Resilience in the Built Environment, 6(4), pp.409-423.
- Labaka, L., Hernantes, J., & Sarriegi, J. M. (2016). *A Holistic Framework for Building Critical Infrastructure Resilience*. Technological Forecasting and Social Change, 103(1), pp.21-33.
- Lade, S. J., and Peterson, G. D. (2019). *Comment on Resilience of Complex Systems: State of the Art and Directions for Future Research*. Complexity, 2019.
- Laderman, E., Heinbockel, W., Graubart, R. & Bodeau, D. (2015). *Cyber Resiliency Engineering Aid: The Updated Cyber Resiliency Engineering Framework and Guidance on Applying Cyber Resiliency Techniques*. MITRE Corporation, Technical Report No. MTR140499R1.
- Laishram, R., Sariyüce, A. E., Eliassi-Rad, T., Pinar, A., & Soundarajan, S. (2018). *Measuring and Improving the Core Resilience of Networks*. In Proceedings of the 2018 World Wide Web Conference, pp.609-618.
- Lamport, L., Shostak, R., & Pease, M. (2019). *The Byzantine Generals Problem*. In Concurrency: The Works of Leslie Lamport, pp.203-226.
- LaRocca, S. (2014). *Modeling the Reliability and Robustness of Critical Infrastructure Networks*. Doctoral Dissertation. Johns Hopkins University.
- Lasy, T. (2019). *From Hashgraph to a Family of Atomic Broadcast Algorithms*. arXiv preprint arXiv:1912.05895.
- Lazari, A. (2014). *European critical infrastructure protection*. Springer International Publishing.
- Ledesma, J. (2014). *Conceptual Frameworks and Research Models on Resilience in Leadership*. Sage Open, 4(3), 2158244014545464.
- Leslie, N.O., Harang, R.E., Knachel, L.P. & Kott, A. (2018). *Statistical Models for the Number of Successful Cyber Intrusions*. The Journal of Defense Modeling and Simulation, 15(1), pp.49-63.
- Levalle, R. R., and Nof, S. Y. (2017). *Resilience in Supply Networks: Definition, Dimensions, and Levels*. Annual Reviews in Control, 43(3), pp.224-236.
- Lewis, T. G. (2019). *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*. Book. John Wiley & Sons.
- Li, F., He, J., Huang, G., Zhang, Y., Shi, Y., & Zhou, R. (2015). *Node-Coupling Clustering Approaches for Link Prediction*. Knowledge-Based Systems, 89(1), pp.669-680.
- Li, J., Wang, J., Sun, S. & Xia, C. (2018). *Cascading Crashes Induced by the Individual Heterogeneity in Complex Networks*. Applied Mathematics & Computation, 323(2), pp.182-192.
- Lin, Y., and Bie, Z. (2016). *Study on the Resilience of the Integrated Energy System*. Energy Procedia, 103(1), pp.171-176.
- Linkov, I., and Kott, A. (2019). *Fundamental Concepts of Cyber Resilience: Introduction and*

- Overview*. In *Cyber resilience of systems and networks*, pp.1-25. Springer, Cham.
- Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., & Kott, A. (2013). *Resilience Metrics for Cyber Systems*. *Environment Systems and Decisions*, 33(4), pp.471-476.
- Liu, C., Wu, J. & Long, C. (2016). *Dynamic State Recovery for Cyber-Physical Systems under Switching Location Attacks*. *IEEE Transactions on Control of Network Systems*, 4(1), pp.14-22.
- Liu, H., Cao, W., & Asaeda, H. (2010). *Lightweight Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Version 2 (MLDv2) Protocols*. *RFC 5790*.
- Liu, L. J. (2016). *Optimization Design of Computer Network Reliability based on Genetic Algorithms*. *Chemical Engineering Transactions*, 51(5), pp.775-780.
- Liu, R. R., Li, M., & Jia, C. X. (2016). *Cascading Failures in Coupled Networks: The Critical Role of Node-Coupling Strength across Networks*. *Scientific reports*, 6(1), pp.1-6.
- Liu, W., and Song, Z. (2020). *Review of Studies on the Resilience of Urban Critical Infrastructure Networks*. *Reliability Engineering & System Safety*, 193(1), 106617.
- Liu, X., Ferrario, E., & Zio, E. (2017). *Resilience Analysis Framework for Interconnected Critical Infrastructures*. *Journal of Risk and Uncertainty in Engineering Systems, Part B*, 3(2).
- Liu, X., Gao, J., Li, D., & Havlin, S. (2015). *Recent Progress on the Resilience of Complex Networks*. *Energies*, 8(10), pp.12187-12210.
- Lopez, J., Alcaraz, C., & Choo, K. R. (2017). *Resilient Interconnection in Cyber-Physical Control Systems*. *Computers & Security*, 71(4), pp.2–14.
- Louzada, V. H., Daolio, F., Herrmann, H. J., & Tomassini, M. (2013). *Smart Rewiring for Network Robustness*. *Journal of Complex Networks*, 1(2), pp.150-159.
- Lozano, L., and Medaglia, A. L. (2013). *On An Exact Method for the Constrained Shortest Path Problem*. *Computers and Operations Research*, 40(1), pp.378-384.
- Lu, Z., and Yang, H. (2012). *Unlocking the Power of OPNET Modeler*. Book. Cambridge University Press.
- Luijff, E., Nieuwenhuijs, A., Klaver, M., van Eeten, M., & Cruz, E. (2018). *Empirical Findings on Critical Infrastructure Dependencies in Europe*. In *International Workshop on Critical Information Infrastructures Security*, pp.302-310. Springer, Berlin, Heidelberg.
- Lukas, L., and Hromada, M. (2011). *Resilience as Main Part of Protection of Critical Infrastructure*. *International Journal of Mathematical Models and Methods in Applied Sciences*, 3(1), pp.1135-1142.
- Luykx, A., and Baird, L. (2020). *The Hashgraph Protocol: Efficient Asynchronous BFT for High-Throughput Distributed Ledgers*. *International Conference on Omni-layer Intelligent Systems (COINS)*, pp.1-7. IEEE.
- Lyn, K.G. (2015). *Classification Of and Resilience to Cyber-Attacks on Cyber-Physical Systems*. Doctoral Dissertation, Georgia Institute of Technology.

- Madni, A. M., Madni, C. C., & Lucero, S. D. (2019). *Leveraging Digital Twin Technology in Model-Based Systems Engineering*. *Systems*, 7(1), pp.7.
- Maglaras, L. A., Kim, K. H., Janicke, H., Ferrag, M. A., Rallis, S., Fragkou, P., & Cruz, T. J. (2018). *Cyber Security of Critical Infrastructures*. *ICT Express*, 4(1), pp.42-45.
- Mahajan, P. and Sachdeva, A. (2013). *A Study of Encryption Algorithms AES, DES, and RSA for Security*. *Global Journal of Computer Science and Technology*.
- Malik, S., and Sahu, P. K. (2019). *A Comparative Study on Routing Protocols for VANETs*. *Heliyon*, 5(8), e02340.
- Manzoor, A., Hussain, M., & Mehrban, S. (2020). *Performance Analysis and Route Optimization: Redistribution between EIGRP, OSPF & BGP Routing Protocols*. *Computer Standards & Interfaces*, 68(103391).
- Marais, K., and Uday, P. (2015). *Designing Resilient Systems-of-Systems: A Survey of Metrics, Methods, and Challenges*. *Systems Engineering*, 18(5), pp.491-510.
- Marchese, D., Jin, A., Fox-Lent, C., & Linkov, I. (2020). *Resilience for Smart Water Systems*. *Journal of Water Resources Planning and Management*, 146(1), 02519002.
- Martí, R., and Reinelt, G. (2011). *Heuristic Methods*. In *The Linear Ordering Problem*, pp.17-40. Springer, Berlin, Heidelberg.
- Martin, R. L. (2020). *The Protection Officer's Role in Critical Information Infrastructure Protection*. In *The Professional Protection Officer*, pp.403-408. Butterworth-Heinemann.
- Masood, M., Abuhelala, M., & Glesk, I. (2016). A comprehensive study of routing protocols performance with topological changes in standard networks. *International Journal of Electronics, Electrical and Computational System*, 5(8), 31-40.
- Masood, M., Fouad, M. M., & Glesk, I. (2018). *Analysis of Artificial Intelligence-Based Metaheuristic Algorithm for MPLS Network Optimization*. *Proceedings of the 20<sup>th</sup> International Conference on Transparent Optical Networks (ICTON)*, pp.1-4. IEEE.
- Mattioli, R., and Moulinos, K. (2015). *Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors*. European Union Agency for Network and Information Security (ENISA).
- Mauthe, A., Hutchison, D., Cetinkaya, E. K., Ganchev, I., Rak, J., Sterbenz, J. P., & Gomes, T. (2016). *Disaster-Resilient Communication Networks: Principles and Best Practices*. In *2016 8<sup>th</sup> International Workshop on Resilient Networks Design and Modeling (RNDM)*, pp.1-10. IEEE.
- Maxima, M. (2019). *A Computer Algebra System*. Version 5.34. 1, 2019. URL <http://maxima.sourceforge.net>.
- Mbanaso, U., Kulugh, V., Musa, H., & Aimufua, G. (2019). *Conceptual Framework for the Assessment of the Degree of Dependency of Critical National Infrastructure on ICT in Nigeria*. In *15<sup>th</sup> International Conference on Electronics, Computer, and Computation*, pp.1-6. IEEE.
- McCollum, C., Bodeau, D., & Fox, D. (2018). *Cyber Threat Modeling Survey, Assessment, and Representative Framework*. Homeland Security Systems Engineering & Development Institute.

- McGill, K. (2011). *Operating System Support for Resilience*. Dartmouth College.
- Micali, S. (2018). *Byzantine Agreement, Made Trivially*. Cambridge University. Selected Scientific Papers, pp.1–10.
- Mikhalevich, I. F. and Trapeznikov, V. A. (2019). *Critical Infrastructure Security: Alignment of Views*. In 2019 Systems of Signals Generating and Processing in the Field of on-Board Communications, pp.1-5. IEEE.
- Milanović, J. V, Zhu, W., & Member, S. (2018). *Modeling of Interconnected Critical Infrastructure Systems Using Complex Network Theory*. IEEE Transactions on Smart Grid, 9(5), pp.4637-4648.
- Minematsu, K., Suzaki, T., Morioka, S., & Kobayashi, E. (2011). *Twine: A Lightweight, Versatile Block Cipher*. In ECRYPT Workshop on Lightweight Cryptography.
- Mirino, A. E. (2017). *Best Routes Selection using Dijkstra and Floyd-Warshall Algorithm*. Proceedings of the 11<sup>th</sup> International Conference on Information & Communication Technology and System (ICTS), pp.155-158. IEEE.
- Mitchell, R., and Chen, R. (2016). *Modeling and Analysis of Attacks and Counter Defense Mechanisms for Cyber-Physical Systems*. IEEE Transactions on Reliability, 65(1), pp.350-358.
- Mitra, S., Brelsford, K., & Sanda, P. N. (2010). *Cross-Layer Resilience Challenges: Metrics and Optimization*. Design, Automation, and Test in Europe Conference, pp.1029-1034. IEEE.
- Mo, H., Fang, Z., Wang, Y., & Xie, M. (2017). *Computers & Industrial Engineering Performance and Reliability Improvements of Cyber-Physical Systems Subject to Degraded Communication Networks through Robust Optimization*. Computers & Industrial Engineering, 114(2), pp.166–174.
- Mode, D. C. S. (2020). *Balancing Resistance and Resilience*. Network Security, 20(7), pp.20-26.
- Mohammad, Z., Abusukhon, A., Hnaif, A., & Al-Otoum, S. (2017). *Performance Analysis of Route Redistribution among Diverse Dynamic Routing Protocols based OPNET Simulation*. International Journal of Advance Computer Science & Applications, 8(3), pp.324-332.
- Moraitis, G., Nikolopoulos, D., Bouziotas, D., Lykou, A., Karavokiros, G., & Makropoulos, C. (2020). *Quantifying Failure for Critical Water Infrastructures under Cyber-Physical Threats*. Journal of Environmental Engineering, 146(9), 04020108.
- Mosharraf, N., Jayasumana, A. P., & Ray, I. (2015). *A Responsive Defense Mechanism against DDoS Attacks*. In International Symposium on Foundations and Practice of Security, 8930(1), pp. 347-355. Springer, Cham.
- Moyer, T., Chadha, K., Cunningham, R., Schear, N., Smith, W., Bates, A. & Cable, P. (2016). *Leveraging Data Provenance to Enhance Cyber Resilience*. In 2016 IEEE Cybersecurity Development (SecDev), pp.107-114. IEEE.
- Nakayama, Y., and Oota, N. (2013). *Path Selection Algorithm for Shortest Path Bridging in Access Networks*. IEICE Communications Express, 2(10), pp.396-401.

- Nan, C., and Sansavini, G. (2017). *A Quantitative Method for Assessing the Resilience of Interdependent Infrastructures*. Reliability Engineering & System Safety, 157(2), pp.35-53.
- Nan, C., Sansavini, G. & Kröger, W. (2014). *Building an Integrated Metric for Quantifying the Resilience of Interdependent Infrastructure Systems*. In International Conference on Critical Information Infrastructures Security, pp.159-171. Springer, Cham.
- Nazir, S., Patel, S., & Patel, D. (2017). *Assessing and Augmenting SCADA Cyber Security: A Survey of Techniques*. Computers & Security, 70(1), pp.436-454.
- Neumann, J. C. (2015). *The book of GNS3: build virtual network labs using Cisco, Juniper, and more*. No Starch Press.
- Nezamoddini, N., Mousavian, S., & Erol-Kantarci, M. (2017). *A Risk Optimization Model for Enhanced Power Grid Resilience against Physical Attacks*. Electric Power Systems Research, 143(5), pp.329-338.
- Nistor, M. S., Pickl, S., Raap, M., & Zsifkovits, M. (2019). *Network Efficiency and Vulnerability Analysis using the Flow-Weighted Efficiency Measure*. International Transactions in Operational Research, 26(2), pp.577-588.
- Njemaze, H., Stone, J., Martin, J., Chatila, K., Andrew, L., Green, M. & Nichols, A. (2019). *Cyber Resilience Oversight Guidelines for the Arab Countries concerning Financial Market Infrastructures*. Arab Monetary Fund, pp.1-86.
- O'Halloran, C., Robinson, T. G., & Brock, N. (2017). *Verifying Cyber-Attack Properties*. Reviewed Paper. Science of Computer Programming, 148(1), pp.3-25.
- O'Kelly, M. E. (2015). *Network Hub Structure and Resilience*. Networks and Spatial Economics, 15(2), pp.235-251.
- Ojo, O. E., Oluwatope, A. O., & Ajadi, S. O. (2021). *A Reliable Peer-to-Peer Streaming Protocol in Low-Capacity Networks*. Peer-to-Peer Networking and Applications, 14(2), pp.559-584.
- Oliva, G., Amideo, A. E., Starita, S., Setola, R., & Scaparra, M. P. (2019). *Aggregating Centrality Rankings: A Novel Approach to Detect Critical Infrastructure Vulnerabilities*. International Conference on Critical Information Infrastructures Security, pp.57-68. Springer.
- Olszewski, I. (2012). *An Algorithm of Choosing LSPS Based on the Dijkstra Algorithm in the MPLS Networks with Unreliable Links*. Przegląd Elektrotechniczny, 88(8), pp.334-338.
- Ormrod, D., and Turnbull, B. (2019). *Modeling and Simulation Approaches*. In Cyber Resilience of Systems and Networks, pp.171-193. Springer, Cham.
- Orojloo, H., and Azgomi, A. (2017). *Method for Evaluating Consequence Propagation of Security Attacks in Cyber-Physical Systems*. Future Generation Computer System, 67(2), pp.57-71.
- Ostfeld, A., Oliker, N., & Salomons, E. (2014). *Multi-Objective Optimization for Least Cost Design and Resiliency of Water Distribution Systems*. Journal of Water Resources Planning and Management, 140(12), 04014037.
- Ottenburger, S., Çakmak, K., Jakob, W., Blatman, A., Trybshnyi, D., Raskob, W. & Hagenmyer,

- V. (2020). *A Novel Optimization Method for Urban Resilient & Fair Power Distribution Preventing Critical Network States*. International Journal of Critical Infrastructure Protection.
- Ouyang, M. (2014). *Review on Modeling and Simulation of Interdependent Critical Infrastructure Systems*. Reliability Engineering & System Safety, 121(6), pp.43-60.
- Ouyang, M. (2017). *A Mathematical Framework to Optimize the Resilience of Interdependent Critical Infrastructure Systems Under Spatially Localized Attacks*. European Journal of Operational Research, 262(3), pp.1072-1084.
- Palleti, V. R., Joseph, J. V., & Silva, A. (2018). *A Contribution of Axiomatic Design Principles to the Analysis and Impact of Attacks on Critical Infrastructures*. International Journal of Critical Infrastructure Protection, 23(1), pp.21-32.
- Panzieri, S., Faramondi, L., Setola, R., & Oliva, G. (2019). *Assessing Node Criticality in Dynamical Distributed Systems*. In 18<sup>th</sup> European Control Conference, pp.1537-1543. IEEE.
- Papán, J., Segeč, P., Moravčík, M., Kontšek, M., Mikuš, L. U., & Uramová, J. (2018). *Overview Of IP Fast Reroute Solutions*. Proceedings of the 16<sup>th</sup> International Conference on Emerging eLearning Technologies and Applications (ICETA), pp.417-424. IEEE.
- Parshani, R., Buldyrev, S. V., & Havlin, S. (2010). *Interdependent Networks: Reducing the Coupling Strength Leads to a Change from a First to Second-Order Percolation Transition*. Physical Review Letters, 105(4), 048701.
- Patrman, D., Splichalova, A., Rehak, D., & Onderkova, V. (2019). *Factors Influencing the Performance of Critical Land Transport Infrastructure Elements*. Transportation Research Procedia, 40(1), pp.1518-1524.
- Pedroni, N., Fang, Y. P., & Zio, E. (2016). *Resilience-Based Component Importance Measures for Critical Infrastructure Network Systems*. IEEE Transactions on Reliability, 65(2), pp.502-512.
- Pedroni, N., Fang, Y., & Zio, E. (2015). *Optimization of Cascade-Resilient Electrical Infrastructures and its Validation by Power Flow Modeling*. Risk Analysis, 35(4), pp.594-607.
- Pereira, T. (2010). *Hub Synchronization in Scale-Free Networks*. Physical Review, 82(3), 036201.
- Pescaroli, G., and Alexander, D. (2016). *Critical Infrastructure, Panarchies, and the Vulnerability Paths of Cascading Disasters*. Natural Hazards, 82(1), pp.175-192.
- Petrenko, S. A., Makoveichuk, K. A., & Petrenko, A. S. (2019). *Intellectual Cyber Resilience Orchestration*. In Информационные Системы И Технологии В Моделировании И Управлении, pp.156-162.
- Petukhov, A. N., Pilyugin, P. L., & Pilyugina, K. N. (2019). *Harmonization of Critical Information Infrastructure Objects Threats*. In Proceedings of the International Conference Technology & Entrepreneurship in Digital Society (TEDS), pp.82-85.
- Pipyros, K. (2019). *A New Systematic Modelling Methodology for Improving Cyber-Attack Evaluation on States' Critical Information Infrastructure (CII)*. Doctoral Dissertation, Οικονομικό Πανεπιστήμιο Αθηνών. Σχολή Επιστημών και Τεχνολογίας Πληροφορίας.

- Pitt-Francis, J., and Whiteley, J. (2017). *Guide to Scientific Computing in C++*. Book. Second Edition. Springer.
- Polese, M., Chiariotti, F., Bonetto, E., Rigotto, F., Zanella, A., & Zorzi, M. (2019). *A Survey on Recent Advances in Transport Layer Protocols*. IEEE Communications Surveys and Tutorials, 21(4), pp.3584-3608.
- Potii, O., and Tsyplinsky, Y. (2020). *Methods of Classification and Assessment of Critical Information Infrastructure Objects*. In 2020 IEEE 11<sup>th</sup> International Conference on Dependable Systems, Services and Technologies (DESSERT), pp.389-393. IEEE.
- Pramudita, R., Heryanto, H., Handayanto, R. T., Setiyadi, D., Arifin, R. W., & Safitri, N. (2019). *Shortest Path Calculation Algorithms for Geographic Information Systems*. Proceedings of the Fourth International Conference on Informatics and Computing (ICIC), pp.1-5. IEEE.
- Prav, R. (2019). *Monitoring of the Development of Information Infrastructure in Ukraine*. Technology Audit and Production Reserves, 3(47), pp.12-18.
- Prior, T. (2015). *Measuring Critical Infrastructure Resilience: Possible Indicators*. Risk and Resilience Report, 9(1).
- Qiu, H., Zhao, S., Gu, R., Li, T. O., Wang, Y., Cui, H., & Yang, J. (2018). *Owl: Understanding and Detecting Concurrency Attacks*. In 2018 48<sup>th</sup> Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), pp.219-230. IEEE.
- Qiu, K., Zhao, J., Wang, X., Fu, X., & Secci, S. (2019). *Efficient Recovery Path Computation for Fast Reroute In Large-Scale Software-Defined Networks*. IEEE Journal on Selected Areas in Communications, 37(8), pp.1755-1768.
- Raab, C. D., Jones, R., & Székely, I. (2015). *Surveillance and Resilience in Theory and Practice*. Media and Communication, 3(2).
- Rahnamay-Naeini, M., and Hayat, M. M. (2016). *Cascading Failures in Interdependent Infrastructures: An Interdependent Markov-Chain Approach*. IEEE Transactions on Smart Grid, 7(4), pp.1997-2006.
- Rak, J. (2015). *Resilient Routing in Communication Networks*. Berlin: Springer, pp.1-181.
- Rasouli, M., Miehl, E., & Teneketzis, D. (2014). *A Supervisory Control Approach to Dynamic Cyber-Security*. In International Conference on Decision and Game Theory for Security, pp.99-117. Springer, Cham.
- Rauchs, M., Glidden, A., Gordon, B., Pieters, G. C., Recanatini, M., Rostand, F. & Zhang, B. Z. (2018). *Distributed Ledger Technology Systems: A Conceptual Framework*. SSRN 3230013.
- Rehak, D., Senovsky, P., & Slivkova, S. (2018). *The Resilience of Critical Infrastructure Elements and its Main Factors*. Systems, 6(2), pp.21.
- Reich, P. C. (2019). *Healthcare: A Critical Information Infrastructure*. Nanyang Technological University, Singapore.
- Ren, F., Zhao, T., Jiao, J., & Hu, Y. (2017). *Resilience Optimization for Complex Engineered*



- Systems based on the Multidimensional Resilience Concept*. IEEE Access, 5(1), pp.19352-19362.
- Reniers, G., and Zhang, L. (2018). *Security Vulnerability Analysis: Protecting Process Industries from Intentional Attacks: The State of the Art*. In-Game Theory for Managing Security in Chemical Industrial Areas, De Gruyter, Berlin, Germany, pp.1-24. Springer, Cham.
- Rescorla, E., and Dierks, T. (2018). *Transport Layer Security (TLS) Protocol Ver.1.3*. RFC 8446.
- Riaz, S., Rehan, M., Umer, T., Afzal, M. K., Rehan, W., & Munir, E. U. (2018). *FRP: A Novel Fast Rerouting Protocol with Multi-Link-Failure Recovery Mission-Critical WSN*. Future Generation Computing Systems, 89(148), pp.65.
- Robles, D. Á., Nuño, P., Bulnes, F. G., & Candás, J. C. G. (2021). *Performance Analysis of Packet Sniffing Techniques Applied to Network Monitoring*. IEEE Latin America Transactions, 19(3), pp.490-499.
- Rød, B., Lange, D., Theocharidou, M., & Pursiainen, C. (2020). *From Risk Management to Resilience Management in Critical Infrastructure*. Journal of Management in Engineering, 36(4).
- Rose, A. (2019). *Incorporating Cyber Resilience into Computable General Equilibrium Models*. In Advances in Spatial and Economic Modeling of Disaster Impacts, pp.99-120. Springer, Cham.
- Rose, S. W., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture*. No. NIST Special Publication (SP) (800-207). National Institute of Standards and Technology.
- Rozorinov, H., Trapezon, K., Vlasjuk, A., Chichikalo, N., Fendri, A., & Pilkevich, Y. (2017). *Features Virtualization Software Telecommunications Networks by Means of Simulation Riverbed Modeler*. 2<sup>nd</sup> International Conference on Advanced Info. & Comm, pp.246-249. IEEE.
- Rusi, T., and Lehto, M. (2017). *Cyber Threats Mega Trends in Cyber Space*. In ICMLG 2017 5<sup>th</sup> International Conference on Management Leadership and Governance. Academic Conferences and Publishing Limited, pp.323-333.
- Saidi, S., Kattan, L., Jayasinghe, P., Hettiaratchi, P. & Taron, J. (2018). *Integrated Infrastructure Systems: A Review*. Sustainable Cities and Society, 36(1), pp.1-11.
- Saini, A. S., Gupta, P., & Gupta, H. (2021). *Implementation of Secured Wired and WLAN Network Using eNSP*. In Advances in Smart Communication and Imaging Systems, pp.577-590. Springer, Singapore.
- Salve, S. M., Samreen, S. N., & Khatri-Valmik, N. (2018). *A Comparative Study on Software Development Life Cycle Models*. International Research Journal of Engineering and Technology (IRJET), pp.696-700.
- Sano, F., Okamoto, T., Winarno, I., Hata, Y. & Ishida, Y. (2016). *A Cyber-Attack-Resilient Server Using Hybrid Virtualization*. Procedia Computer Science, 96(2), pp.1627-1636.
- Sansavini, G. (2017). *Engineering Resilience in Critical Infrastructures*. In Resilience and Risk, pp.189-203. Springer, Dordrecht.
- Sansavini, G., and Fang, Y. (2016). *Optimum Post-Disruption Restoration for Enhanced Infrastructure Network Resilience: Fuzzy Programming Approach*. In Proceeding of the Annual

- European Safety and Reliability Conference (ESREL), pp.587-594.
- Sansavini, G., and Zio, E. (2011). *Modeling Interdependent Network Systems for Identifying Cascade-Safe Operating Margins*. IEEE Transactions on Reliability, 60(1), pp.94-101.
- Sapundzhi, F. I., and Popstoilov, M. S. (2018). *Optimization Algorithms for Finding the Shortest Paths*. Bulgarian Chemical Communications, 50(Special Issue B), pp.115-120.
- Sargent, M., Kristoff, J., Paxson, V., & Allman, M. (2017). *On the Potential Abuse of IGMP*. ACM SIGCOMM Computer Communication Review, 47(1), pp.27-35.
- Sarwat, A. I., Sundararajan, A., Parvez, I., Moghaddami, M., & Moghadasi, A. (2018). *Toward a Smart City of Interdependent Critical Infrastructure Networks*. In Sustainable Interdependent Networks, pp.21-45. Springer, Cham.
- Sathyasri, B., Janani, P., & Mahalakshmi, V. (2021). *Redistribution of Dynamic Routing Protocols (ISIS, OSPF, EIGRP), IPv6 Networks, and their Performance Analysis*. Recent Trends in Communication and Intelligent Systems: Proceedings of ICRTCIS 2020, pp.179.
- Scala, A., Lucentini, P. G. D. S., Caldarelli, G., & D'Agostino, G. (2016). *Cascades in Interdependent Flow Networks*. Physica D: Nonlinear Phenomena, 323(1), pp.35-39.
- Schaub, A., Bazin, R., Hasan, O., & Brunie, L. (2016). *A Trustless Privacy-Preserving Reputation System*. IFIP International Conference on ICT Systems Security and Privacy Protection, pp.398-411. Springer, Cham.
- Schneider, C. M., Yazdani, N., Araújo, N. A., Havlin, S., & Herrmann, H. J. (2013). *Towards Designing Robust Coupled Networks*. Scientific Reports, 3(1), pp.1969-1979.
- Schneider, M., Moreira, A., Andrade, S., Havlin, S., & Herman, J. (2015). *Mitigation of Malicious Attacks on Networks*. Proceedings of National Academy of Sciences, 108(10), pp.3838-3841.
- Schueffel, P. (2017). *Alternative Distributed Ledger Technologies Blockchain vs. Tangle vs. Hashgraph: A High-Level Overview and Comparison*. SSRN e-Library, pp.1-8.
- Schwind, N., Magnin, M., Inoue, K., Okimoto, T., Sato, T., Minami, K., & Maruyama, H. (2016). *Formalization of Resilience for Constraint-based Dynamic Systems*. Journal of Reliable Intelligent Environments, 2(1), pp.17-35.
- Scott, B. (2018). *How Zero Trust Approach Help to Secure AWS Environment*. Network Security, 2018(3), pp.5-8.
- Selifanov, V., Zvyagintseva, A., Isaeva, A., & Goldobina, S. (2020). *Main Aspects of Conformity Assessment of DLP-Systems used to ensure Security of Significant Objects of Critical Information Infrastructure of Russian Federation*. In IOP Conference Series Publishing, 734(1), pp.012094.
- Senovsky, P., Rehak, D., Hromada, M., & Lovecek, T. (2019). *Complex Approach to Assessing Resilience of Critical Infrastructure Elements*. International Journal of Critical Infrastructure Protection, 25(1), pp.125-138.
- Seppänen, H., Luukkala, P., Zhang, Z., Torkki, P., & Virrantaus, K. (2018). *Critical*

- Infrastructure Vulnerability: A Method for Identifying the Infrastructure Service Failure Interdependencies*. International Journal of Critical Infrastructure Protection, 22(1), pp.25-38.
- Sepúlveda-Estay, D. A., Sahay, R., Barfod, M. B., & Jensen, C. D. (2020). *A Systematic Review of Cyber-Resilience Assessment Frameworks*. Computers & Security, 101996.
- Sethi, A. S., and Hnatyshin, V. Y. (2012). *The Practical OPNET User Guide for Computer Network Simulation*. CRC Press.
- Setola, R., and Theocharidou, M. (2016). *Modeling Dependencies between Critical Infrastructures*. In managing the complexity of critical infrastructures, pp.19-41. Springer, Cham.
- Setola, R., Rosato, V., Kyriakides, E. & Rome, E. (2017). *Managing the Complexity of Critical Infrastructures: A Modelling and Simulation Approach*. Book eds. 90(1). Springer Nature.
- Severson, T., Rodriguez-Seda, E., Kiriakidis, K., Croteau, B., Krishnankutty, D., Robucci, R. & Banerjee, N. (2018). *Trust-Based Framework for Resilience to Sensor-Targeted Attacks in Cyber-Physical Systems*. Annual American Control Conference (ACC), pp.6499-6505. IEEE.
- Shaburov, A. S., and Alekseev, V. R. (2019). *Protection Models of Critical Information Infrastructure Objects from Targeted Computer Attacks*. In 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), pp.335-338. IEEE.
- Shafqat, N., and Masood, A. (2016). *Comparative Analysis of Various National Cyber Security Strategies*. International Journal of Computer Science & Information Security, 14(1), pp.129-139.
- Shah, S.S., and Babiceanu, R.F. (2015). *Resilience Modeling and Analysis of Interdependent Infrastructures*. Systems & Information Engineering Design Symposium, pp.154-158. IEEE.
- Shalamanov, V. (2019). *Organizing for IT Effectiveness, Efficiency, and Cyber Resilience in the Academic Sector: National and Regional Dimensions*. Information & Security: An International Journal, 42(1).
- Shang, Y., Tyra, A., Jiang, S., Zhao, Y. & Xu, S. (2017). *Robustness of Non-Interdependent & Interdependent Networks against Dependent & Adaptive Attacks*. Physica A, 482(1), pp.713-727.
- Sharif, M., and Sadeghi-Niaraki, A. (2017). *Ubiquitous Sensor Network Simulation & Emulation Environments: A Survey*. Journal of Network & Computer Applications, 93(3), pp.150-181.
- Shevchenko, N., Chick, T. A., O’Riordan, P., Scanlon, T. P., & Woody, C. (2018). *Threat Modeling: A Summary of Available Methods*. Carnegie Mellon University, Software Engineering Institute, Pittsburgh, United States.
- Shevchuk, P. S. (2019). *An Approach for Distributed Reasoning on Security Incidents in Critical Information Infrastructure with Intelligent Awareness Systems*. In Proceedings of 3<sup>rd</sup> Computational Methods in Systems and Software, 1(1), pp.248-262.
- Shi, N., Zhou, S., Wang, F., Tao, Y., & Liu, L. (2017). *The Multi-Criteria Constrained Shortest Path Problem*. Transportation Research: Logistics & Transportation Review, 101(2), pp.13-29.
- Shoemaker, D., Conklin, A. & Kohnke, A. (2017). *Cyber Resilience: Rethinking Cybersecurity Strategy to Build a Cyber Resilient Architecture*. 5<sup>th</sup> International Conference on Management

Leadership & Governance, pp.105-115. Academic Conferences & publishing limited.

Siddiqui, F., Hagan, M., & Sezer, S. (2019). *Establishing Cyber Resilience in Embedded Systems for Securing Next-Generation Critical Infrastructure*. In 2019 32<sup>nd</sup> IEEE International System-on-Chip Conference (SOCC), pp.218-223. IEEE.

Singh, A., and Mishra, P. K. (2014). *Performance Analysis of Floyd Warshall Algorithm vs. Rectangular Algorithm*. International Journal of Computer Applications, 107(16).pp.23–7.

Singh, J. B., and Tripathi, R. C. (2018). *Investigation of Bellman-Ford Algorithm, Dijkstra's Algorithm for the suitability of SPP*. Int. J. Eng. Dev. Res. 1 Dean Res, 6(1), pp.2321-9939.

Singh, K., Singh, P. & Kumar, K. (2016). *A Systematic Review of IP Trace Back Schemes for Denial-of-Service Attacks*. Computers & Security, 56(1), pp.111-139.

Sinha, A., Vyas, R., Subramanian, V., & Vyas, O. P. (2020). *Critical Infrastructure Security: Cyber-Physical Attack Prevention, Detection, and Countermeasures*. In Quantum Cryptography and the Future of Cyber Security, pp.134-162. IGI Global.

Sirika, S., and Mahajan, S. (2016). *Survey on Dynamic Routing Protocols*. Int. J. Eng. Res. Technology, 5(01), pp.10-14.

Sitti, M. (2015). *Mitigating DDoS Attack through Shortest Path Bridging: IEEE 802.1aq*. Journal of Applied Thought, ISSN 2026-691X Editorial Board, 4(2), pp.254-354.

Smart, N. P. (2016). *Cryptography Made Simple*. 481(1). Heidelberg: Springer.

Sokolov, S., Glebov, N., Natashova, K., & Gubernatorov, O. (2019). *Categorization of Objects of Critical Information Infrastructure of Water Transport*. In E3S Web of Conferences, 110(2), pp. 02003. EDP Sciences.

Spirin, V. A., Zenin, A. A., Pysin, S. A., & Zybin, D. G. (2020). *Conceptual Model in the System of Decision-Making Support for the Critical Informational Infrastructure of the Departmental Information Network*. In IOP Conference Series Publishing, 421(4), pp.042004.

Stafford, V. A. (2020). *Zero Trust Architecture*. NIST Special Publication, (800) pp.207-222.

Staggs, J., and Shenoi, S. (2019). *Critical Infrastructure Protection XIII*. 13<sup>th</sup> IFIP WG 11.10 International Conference, Arlington, USA, Revised Selected Papers. 570(1). Springer Nature.

Stanley, H. E., Liu, X., & Gao, J. (2016). *Breakdown of Interdependent Directed Networks*. Proceedings of the National Academy of Sciences, 113(5), pp.1138-1143.

Sterbenz, J. P., Çetinkaya, E. K., Hameed, M. A., Jabbar, A., Qian, S., & Rohrer, J. P. (2013). *Evaluation of Network Resilience, Survivability, and Disruption Tolerance: Analysis, Topology Generation, Simulation, and Experimentation*. Telecommunication Systems, 52(2), pp.705-736.

Sterbenz, J. P., Hutchison, D., Çetinkaya, E. K., Jabbar, A., Rohrer, J. P., Schöller, M., & Smith, P. (2010). *Resilience and Survivability in Communication Networks: Strategies, Principles, and Survey of Disciplines*. Computer Networks, 54(8), pp.1245-1265.

Strom, B. E., Battaglia, J. A., Kemmerer, M. S., Kupersanin, W., Miller, D. P., Wampler, C. &

- Wolf, R. D. (2017). *Finding Cyber Threats with ATT&CK-Based Analytics*. The MITRE Corporation, Bedford, MA, Technical Report No. MTR170202.
- Suciu, G., Nădrag, C., Istrate, C., Vulpe, A., Ditu, M. C., & Subea, O. (2018). *Comparative Analysis of Distributed Ledger Technologies*. Proceedings of the Global Wireless Summit (GWS), pp.370-373. IEEE.
- Sukach, S., Riznik, D., Zachepa, N., & Chencheyov, V. (2020). *Normalization of the Magnetic Fields of Electrical Equipment in Case of Unauthorized Influence on Critical Information Infrastructure Facilities*. In *Soft Target Protection*, pp.337-349. Springer, Dordrecht.
- Suzaki, T., Minematsu, K., Morioka, S., & Kobayashi, A. (2013). *Lightweight Block Cipher for Multiple Platforms*. Lectures Note Computing Scientific, Bioinformatics, 770 LNCS, pp.339–54.
- Swathika, O. G., and Hemamalini, S. (2017). *Prims Aided Floyd Warshall Algorithm for Shortest Path Identification in Microgrid*. In *Emerging Trends in Electrical, Communications and Information Technologies*, pp.283-291. Springer, Singapore.
- Syahputra, R., Kurnia, R., & Ferdian, R. (2020). *Analysis of FHRP Design and Implementation in RIPv2 and OSPF Routing Protocols*. Journal RESTI (Rekayasa Sistem Dan Teknologi Informasi), 4(1), pp.102-108.
- Tabansky, L. (2011). *Critical Infrastructure Protection against Cyber Threats*. Military and Strategic Affairs, 3(2), pp.2-22.
- Tatar, U. (2020). *Critical Space Infrastructures: Perspectives and a Critical Review*. Space Infrastructures: From Risk to Resilience Governance, 57(1), pp.3-18.
- Teodorescu, H. N., and Pickl, S. W. (2016). *Computing and Optimizing the Index of Resilience of Networks and Information Systems*. Science and Technology, 19(1-2), pp.116-126.
- Tetarave, S. K., Tripathy, S., & Peri, S. (2015). *S-Gossip: Security Enhanced Gossip Protocol for Unstructured P2P Networks*. In *International Conference on Distributed Computing and Internet Technology*, pp.288-298. Springer, Cham.
- Theron, P., and Bologna, S. (2013). *Critical Information Infrastructure Protection and Resilience in the ICT Sector*. Information Science Reference, 318(5). IGI Global.
- Thomas, E., Eisenberg, A., & Seager, T. P. (2018). *Holistic Infrastructure Resilience Research Requires Multiple Perspectives, Not Just Multiple Disciplines*. Infrastructures, 3(3), pp.30-40.
- Thompson, R., Freza, D., Necioglu, B., Cohen, L., Hofman, K., & Rosfjord, K. (2019). *Interdependent Critical Infrastructure Model (ICIM): Agent-Based Power & Water Infrastructure Model*. International Journal of Critical Infrastructure Protection, 24(2), pp.144-165.
- Thorisson, H., Baiardi, F., Angeler, D. G., Taveter, K., Vasheasta, A., Rowe, P. D. & Linkov, I. (2020). *The Resilience of Critical Infrastructure Systems to Hybrid Threats with Information Disruption*. Resilience and Hybrid Threats: Security and Integrity for the Digital World, 55(13).
- Tian, M., Wang, X., Dong, Z., Zhu, G., Long, J., Dai, D., & Zhang, Q. (2015). *Cascading Failures of Interdependent Modular Scale-Free Networks with Different Coupling*

- Preferences*. EPL (Europhysics Letters), 111(1), pp.18007.
- Tipper, D. (2014). *Resilient Network Design: Challenges and Future Directions*. Telecommunication Systems, 56(1), pp.5-16.
- Tonhauser, M., and Ristvej, J. (2019). *Disruptive Acts in Cyberspace, Steps to Improve Cyber Resilience at National Level*. Transportation Research Procedia, 40(1), pp.1591-1596.
- Torres, J. S., Caire, R., & Hadjsaid, N. (2013). *Towards a Complex Networks Modeling of Interdependent Critical Infrastructures*.
- Tran, H. T. (2015). *A Complex Networks Approach to Designing Resilient System-of-Systems*. Doctoral Dissertation, Georgia Institute of Technology.
- Tran, H., Campos-Nanez, E., Fomin, P. & Wasek, J. (2016). *Cyber Resilience Recovery Model to Combat Zero-Day Malware Attacks*. Computers & Security. Engineering Management and Systems Engineering, 61(3), pp.19-31.
- Triana, Y. S., and Syahputri, I. (2018). *Implementation Floyd-Warshall Algorithm for the Shortest Path of Garage*. International Journal of Innovative Science and Research Technology, 3(2), pp.871-878.
- Tschofenig, H., Rescorla, E., & Modadugu, N. (2019). *The Datagram Transport Layer Security (DTLS) Protocol Version 1.3*. IRTF, pp.13-33.
- Tsikin, I., and Melikhova, A. (2016). *A Delegation-Based Architecture for Collaborative Robotics*. Lectures Notes Computing Scientific, Bioinformatics, and LNCS 6788:205, pp.47.
- Tsochev, G. R., Yoshinov, R. D., & Iliev, O. P. (2019). *Key problems of the critical information infrastructure through SCADA systems research*. Труды СПИИРАН, 18(6), pp.1333-1356.
- Tundis, A., Cordero, C. G., Egert, R., Garro, A., & Mühlhäuser, M. (2017). *Increasing the Resilience of Cyber-Physical Systems in Smart Grid Environments using Dynamic Cells*. In Proceedings of the 19<sup>th</sup> International Conference on Cyber-Physical Systems (ICCPS).
- Turner, S. (2014). *Transport Layer Security*. IEEE Internet Computing, 18(6), pp.60-63.
- Turnquist, M. A., and Vugrin, E. D. (2012). *Design for Resilience in Infrastructure Distribution Networks*. Sandia Report: SAND2012, 6050 (39).
- Turskis, Z., Goranin, N., Nurusheva, A., & Boranbayev, S. (2019). *Information Security Risk Assessment in Critical Infrastructure: Hybrid MCDM Approach*. Informatica, 30(1), pp.187-211.
- Tyra, A. (2012). *A Characterization of Complex Network Attack Resilience*. Book. The University of Texas at San Antonio.
- Uday, P. (2015). *System Importance Measures: A New Approach to Resilient Systems-of-Systems*.
- Ullah, F., Edwards, M., Ramdhany, R., Chitchyan, R., Babar, A. & Rashid, A. (2018). *Data Exfiltration: A Review of External Attack Vectors and Countermeasures*. Journal of Network & Computer Applications, 101(2), pp.18-54.
- Ullah, S., Shetty, S., & Hassanzadeh, A. (2018). *Towards Modeling Attacker's Opportunity for*

- Improving Cyber Resilience in Energy Delivery Systems*. In Resilience Week, pp.100-107. IEEE.
- Van der Kleij, R., and Leukfeldt, R. (2019). *Cyber Resilient Behavior: Integrating Human Behavioral Models and Resilience Engineering Capabilities into Cyber Security*. In International Conference on Applied Human Factors and Ergonomics, pp.16-27. Springer, Cham.
- Vanickis, R., Jacob, P., Dehghanzadeh, S., & Lee, B. (2018). *Access Control Policy Enforcement for Zero-Trust-Networking*. 29<sup>th</sup> Irish Signals and Systems Conference (ISSC), pp.1-6. IEEE.
- Vasilyev, V. I., Kirillova, A. D., Sulavko, A. E., & Zhumazhanova, S. S. (2019). *Analysis of Confidential Data Protection in Critical Information Infrastructure and the Use of Biometric, Neural Network, and Cryptographic Algorithms*. Standards Review & Perspectives, pp.193-197.
- Ventresca, M., and Aleman, D. (2015). *Efficiently Identifying Critical Nodes in Large Complex Networks*. Computational Social Networks, 2(1), pp.6-18.
- Ventresca, M., and Aleman, D. (2015). *Network Robustness versus Multi-Strategy Sequential Attack*. Journal of Complex Networks, 3(1), pp.126-146.
- Vespignani, A. (2010). *Complex Networks: The Fragility of Interdependency*. Nature, 464(7291), pp.984-985.
- Viira, T. (2018). *Lessons Learned: Critical Information Infrastructure Protection: How to Protect Critical Information Infrastructure*. Book. IT Governance Ltd.
- Villate, J. E. (2014). *Introduction to Dynamical Systems: A Hands-on Approach with MAXIMA*.
- Viswanathan, A., AlMajali, A., & Neuman, C. (2017). *Resilience Evaluation of Demand Response as Spinning Reserve under Cyber-Physical Threats*. Electronics, 6(1), pp.2-12.
- Voros, N. S., Hübner, M., Becker, J., Kühnle, M., Thomaitiv, F., Grasset, A. & Putzke-Röming, W. (2013). *MORPHEUS: A Heterogeneous Dynamically Reconfigurable Platform for Designing Highly Complex Embedded Systems*. ACM Transactions on Embedded Computing Systems (TECS), 12(3), pp.1-33.
- Vugrin, E. D., Turnquist, M. A., & Brown, N. J. (2014). *Optimal Recovery Sequencing for Enhanced Resilience and Service Restoration in Transportation Networks*. International Journal of Critical Infrastructures, 10(3-4), pp.218-246.
- Wang, B., Li, Z., & Li, H. (2020). *Hybrid Consensus Algorithm based on Modified Proof-of-Probability and DPOS*. Future Internet, 12(8), pp.122.
- Wang, J., Zuo, W., Rhode-Barbarigos, L., Lu, X., Wang, J., & Lin, Y. (2019). *Literature Review on Modeling and Simulation of Energy Infrastructures from a Resilience Perspective*. Reliability Engineering & System Safety, 183(2), pp.360-373.
- Wang, W., Sun, K., Zeng, C., Chen, C., Qiu, W., You, S., & Liu, Y. (2021). *Information and Communication Infrastructures in Modern Wide-Area Systems*. Wide Area Power Systems Stability, Protection, and Security, pp.71-104.
- Wang, X. Z. (2018). *The Comparison of Three Algorithms in Shortest Path Issue*. In Journal of Physics Conference Series, 2(1087).

- Wang, Y., Li, X., & Wu, J. (2010). Multicasting in Delay Tolerant Networks: Delegation Forwarding. Global Telecommunications Conference GLOBECOM, pp.1-5. IEEE.
- Wang, Y., Li, X., & Wu, J. (2011). *Delegation Forwarding in Delay Tolerant Networks Multicasting*. JCM, 6(5), pp.384-392.
- Wang, Z. (2019). *An Elastic and Resiliency Defense against DDoS Attacks on the Critical DNS Authoritative Infrastructure*. Journal of Computer and System Sciences, 99(2), pp.1-26.
- Wang, Z., and Ouyang, M. (2015). *Resilience Assessment of Interdependent Infrastructure Systems: Focus on Joint Restoration Modeling and Analysis*. Reliability Engineering & System Safety, 141(1), pp.74-82.
- Wang, Z., Wang, Q., Zukerman, M., Guo, J., Wang, Y., Wang, G. & Moran, B. (2017). *Multi-Objective Path Optimization for Critical Infrastructure Links with Consideration to Seismic Resilience*. Computer-Aided Civil and Infrastructure Engineering, 32(10), pp.836-855.
- Webster-Clark, M. and Breskin, A. (2020). *Directed Acyclic Graphs, Effect Measure Modification, and Generalizability*. American Journal of Epidemiology, 190(2), pp.322-327.
- Welsh, C. (2013). *GNS3 Network Simulation Guide*. Packt Publisher.
- Wicks, R.T., Pescaroli, G., Giacomello, G. & Alexander, D.E. (2018). *Increasing Resilience to Cascading Events: The M. OR. D. OR. Scenario*. Safety Science.
- Wilner, A. (2017). *Cyber Deterrence and Critical-Infrastructure Protection: Expectation, Application, and Limitation*. Comparative Strategy, 36(4), pp.309-318.
- Wright, M., Venkatesan, S., Albanese, M. & Wellman, P. (2016). *Moving Target Defense against DDoS Attacks: Empirical Game-Theoretic Analysis*. In Proceedings ACM Workshop, pp.93-104.
- Wu, J., Wang, Y., & Li, X. (2011). *Delegation Forwarding in Delay Tolerant Networks Multicasting*. JCM, 6(5), 384-392.
- Wu, Z., Guo, W. & Wang, H. (2018). *Robustness Analysis of Complex Networks with Power Decentralization Strategy via Flow-Sensitive Centrality Against Cascading Failures*. Physica A: Statistical Mechanics and its Applications, 494(2), pp.186-199.
- Wu, Z., Lu, X., & Noori, M. (2020). *The Resilience of Critical Infrastructure Systems: Emerging Developments and Future Challenges*. Book. CRC Press.
- Xie, H. A., and Li, D. (2017). *Trusted Network Management Model based on Clustering Analysis*. In Computer Science, Technology and Application: Proceedings of the International Conference on Computer Science, Technology and Application (CSTA2016), pp.220-226.
- Xiong, W., and Lagerström, R. (2019). *Threat Modeling: A Systematic Literature Review*. Computers & Security, 84(4), pp.53-69.
- Xu, T., and Masys, A. J. (2016). *Critical Infrastructure Vulnerabilities: Embracing a Network Mindset*. In Exploring Security Landscape: Non-Traditional Security Challenges, pp.177-193.
- Yamin, M. M., Katt, B., & Gkioulos, V. (2020). *Cyber Ranges and Security Testbeds: Scenarios*,



- Functions, Tools, and Architecture*. Computers & Security, 88(1), pp.101636.
- Yang, J., Liu, X., & Bose, S. (2015). *Preventing Cyber-Induced Irreversible Physical Damage to Cyber-Physical Systems*. In Proceedings of the 10<sup>th</sup> Annual Cyber and Information Security Research Conference, pp.1-4.
- Yazdanparast, R., Hamid, M., Azadeh, M. A., & Keramati, A. (2018). *An Intelligent Algorithm for Optimization of Resource Allocation Problem by Considering Human Error in an Emergency Department*. Journal of Industrial and Systems Engineering, 11(1), pp.287-309.
- Yin, Y., Zhang, Z., Zhang, X., & Liu, L. (2018). *Optimization of Robustness of Interdependent Network Controllability by Redundant Design*. PloS One, 13(2), e0192874.
- Yong, S. Z., Foo, Q., & Frazzoli, E. (2016). *Robust and Resilient Estimation for Cyber-Physical Systems under Adversarial Attacks*. American Control Conference (ACC), pp.308-315. IEEE.
- Yonghui, T., and Hu, R. (2012). *A Resolution for IGMP v3 Protocol using Finite State Machine*. Proceedings of the International Conference on Computer Science and Electronics Engineering, (1) 2, pp.517-520. IEEE.
- Yu, J. (2013). *Computer Network Reliability Optimization Calculation based on Genetic Algorithm*. Telkomnika, 11(3).
- Yuan, W., Guan, D., Lee, Y. K., & Lee, S. (2017). *The Small-World Trust Network*. Applied Intelligence, 35(3), pp.399-410.
- Yuan, W., Wang, J., Qiu, F., Chen, C., Kang, C., & Zeng, B. (2016). *Robust Optimization-based Resilient Distribution Network Planning against Natural Disasters*. IEEE Transactions on Smart Grid, 7(6), pp.2817-2826.
- Yuan, W., Zhao, L., & Zeng, B. (2014). *Optimal Power Grid Protection through a Defender-Attacker-Defender Model*. Reliability Engineering & System Safety, pp.121, 83-89.
- Yusta, J. M., Correa, G. J., & Lacal-Arántegui, R. (2011). *Methodologies and Applications for Critical Infrastructure Protection: State-of-the-Art*. Energy Policy, 39(10), pp.6100-6119.
- Zafar, F., Khan, A., Suhail, S., Ahmed, I., Hameed, K., Khan, M., Jabeen, F. & Anjum, A. (2017). *Trustworthy Data: A Survey, Taxonomy, and Future Trends of Secure Provenance Schemes*. Journal of Network and Computer Applications, 94(1), pp.50-68.
- Zaheer, Z., Chang, H., Mukherjee, S., & Van der Merwe, J. (2019). *Eztrust: Network-Independent Zero-Trust Perimeterization for Microservices*. Proceedings of the 2019 ACM Symposium on SDN Research, pp.49-61.
- Zakwan, A. (2015). *Protocol Architecture*. Journal of Scientific Data (JSD), 5(1).
- Zeadaly, S., and Alcaraz, C. (2015). *Critical Infrastructure Protection Requirements & Challenges for 21<sup>st</sup> Century*. International Journal of Critical Infra. Protection, 8(1), pp.53-66.
- Zebrowski, C., and Sage, D. (2017). *Resilience and Critical Infrastructure: Origins, Theories, and Critiques*. In The Palgrave Handbook of Security, Risk, and Intelligence, pp.117-135. Palgrave Macmillan, London.

- Zhai, X., and Wang, N. (2019). *Multi-Agent Consensus Algorithm-based Optimal Power Dispatch for Islanded Multi-Microgrids*. *Processes*, 7(10), pp.679.
- Zhao, C., He, J., & Wang, Q. G. (2017). *Resilient Distributed Optimization Algorithm against Adversary Attacks*. 13<sup>th</sup> International Conference on Control & Automation, pp.473-478. IEEE.
- Zheng, K., and Albert, A. (2019). *Interdiction Models for Delaying Adversarial Attacks against Critical Information Technology Infrastructure*. *Naval Research Logistics*, 66(5), pp.411-429.
- Zhu, Q., and Chen, J. (2020). *Optimal Secure Interdependent Infrastructure Network Design*. In-Game and Decision-Theoretic Approach to Resilient Interdependent Network Analysis and Design, pp.75-102. Springer, Cham.
- Zimmer, B. (2018). *LISA: A Practical Zero Trust Architecture*. In *Enigma 2018*, pp.18-29.
- Zio, E., and Fang, Y. (2017). *Optimizing the Resilience of Interdependent Infrastructure Systems against Intentional Attacks*. In 2<sup>nd</sup> International Conference on System Reliability and Safety (ICSRS), pp.62-67. IEEE.
- Zio, E., and Fang, Y. P. (2019). *A Robust Adaptive Framework for Optimizing the Resilience of Interdependent Infrastructures under Natural Hazards*. *European Journal of Operational Research*, 276(3), pp.1119-1136.

## Appendix A: Research Background

Cyber risk management has three components: (1) cyber threat, (2) cyber vulnerability, and (3) cyber consequences, as shown in Figure 1.1 (Barami, 2013). The cyber threat is a synthetic action that can harm the function or data of the cyber network system (Karakoc et al., 2019). Cyber vulnerability is a susceptible cyber attribute that renders the network system exploited by the cyber threat. Finally, cyber consequences are the following effects of a cyber-event (Gisladdottir et al., 2017).



Figure 1.1: Cyber Risk Management Diagram

The interdependent critical information infrastructures can suffer most from cyber threats, which increased by 14% in 2019 because they have numerous cyber vulnerabilities (Kumar et al., 2020). The first cyber vulnerability is the inheriting holes in the generic operating systems (OS) that run over to manage the CIIs (Liu et al., 2017). The security patches are usually issued after OS vulnerabilities are discovered, but there is generally a time lag to release and apply those (Turskis et al., 2019). For example, the patch of vulnerability exploited by the Stuxnet worm in 2010 became available in 2012 (Zebrowski & Sage, 2017), and Code Red malware compromises 360 thousand servers, although a security patch had been released earlier (Creese et al., 2011). Furthermore, a cyberattack comes before OS vulnerability is discovered and is termed a zero-day attack (Bosetti et al., 2016). Besides, the legacy characteristics and their associated vulnerability since installing these

infrastructures are costly and time-consuming, with a very long operational life exceeding thirty years, many different manufacturers, and various standards (Alderson et al., 2015). Moreover, multiple and remote entry points are vulnerable, where critical information infrastructures geographically spread over a large area (Joshi, 2020).

The edge points of the infrastructure are more exploited by attackers and have not been protected against cyberattacks, similar to those in center points (Nezamoddini et al., 2017). However, critical information infrastructures have built-in cybersecurity mechanisms such as Kerberos, multiplexing proxy, user groups, historian, encryption features, and redundant servers (Zhu & Chen, 2020).

Nevertheless, cyber risk management presents no comprehensive solution with high-level encryption because most CIIs were designed for isolated networks (Baroud et al., 2015). As a result, cyber attackers can maliciously exploit an administrative backdoor to access the CII network controls for injecting dump data over the networking protocols that led to service interruptions or cascading failures (Kiss et al., 2015).

Furthermore, the underlying vulnerability is the very tight timing for accurate decision-making to avoid the sensitive deviations caused by the cyberattacks that negatively reflect the vital real-world processes with complex interactions and operational constraints of critical information infrastructures (Abdelgawad et al., 2019).

Finally, the conflicting priorities vulnerability dilemma ensures adequate cyber risk management in parallel with maintaining the sustained performance of running operations (Bhuyan et al., 2015). Typically, the cybersecurity procedures slow down communications and interfere with the ordinary functioning of the critical information infrastructures (Di Pietro et al., 2017).

In some cases, cybersecurity testing has been prevented due to associated risks resulting in undesired consequences for these infrastructures' operational environment (Han et al., 2016).

For example, Dudenhoeffer et al. (2006) progressed Critical Infrastructure Modeling Simulation

(CIMS) for rapid decision-making and prioritization of emergency operations (Hadjsaid et al., 2010). Also, the operational framework developed by Asia-Pacific Computer Emergency Response Team (APCERT) (2009) to encourage and support the cooperation between Computer Security and Incident Response Team (CSIRT) and Computer Emergency Response Team (CERT) organizations in the Asia Pacific region (Guo, 2010).

Additionally, Klein (2009) coordinated the project stages of Integrated Risk Reduction of Information-based Infrastructure Systems (IRRIIS), which is dedicated to interdependency and resilience modeling, analysis, and management of critical infrastructures at the supranational level of the European Union (Mitra et al., 2010).

In 2009, the American Society of Mechanical Engineers, for assessing risk and resilience and prioritization, presented Risk Analysis and Management for Critical Asset Protection Plus (RAMCAP-Plus) methodology across all critical infrastructure sectors (Buldyrev et al., 2010).

Moreover, Utne et al. (2009) worked on the approach of the Risk and Decision Systems for Critical Infrastructures (DECRIIS) to help policymakers for cyber risk and vulnerabilities assessment, prioritization of scenarios, and supporting resilience against all-hazards across sectors like power and water supply (Brechtbühl et al., 2010).

Furthermore, the national security agencies and governmental ICT entities issued policies and strategies like CARVER 2 (2012) and NIST (2013) by the U.S. Department of Homeland Security (DHS), and NCSP (2013) by National Critical Information Infrastructure Protection Centre (NCIIPC) India (Caverzan & Solomos, 2014). Also, NISD (2018) by the European Union Agency for Network & Information Security (ENISA).

The U.S. MITRE Corporation set an architect and implementer guide of Cyber Continuity of Operations Planning (Cyber COOP) in (2015) (Laderman et al., 2015). Additionally, it improved the Cyber Prep 2.0 Framework for motivating cyber organizational strategies in terms of threat

preparedness (2016) as well as enhanced Structured Cyber Resiliency Analysis Methodology (SCRAM) for enabling cyber resilience results under different circumstances (Bodeau & Graubart, 2016).

The international organizations and institutions released standardizations in the same area such as ISO/IEC 27000:2013 family by International Organization for Standardization (ISO), BS 7799-3:2017 by British Standards Institution (BSI) Group, and ACRPTB (2017) by World Economic Forum (WEF) (Vasilyev et al., 2019).

Moreover, the public-private partnerships, semi-private centers, and private firms distributed theoretical frameworks, for instance, ARC frameworks (2014) by Pacific Northwest National Laboratory (PNNL) (Brigantic et al., 2020) and the cybersecurity governance model (2017) by Information Sharing and Analysis Center (ISAC), CADDY (Conti et al., 2018).

The U.S. Department of Homeland Security (2018) launched the National Infrastructure Protection Plan – Risk Management Framework (NIPP-RMF) with a process methodology for risk management for protecting critical infrastructures. It combines threats, vulnerability, and consequence analysis to drive adequate control prioritization to minimize impacts (Bucovechi, 2020).

In addition, The Forum of Incident Response and Security Teams, Inc. (FIRST) in (2019) described a high-level Framework of the Computer Security Incident Response Team (CSIRT) to provide a structured collection of cybersecurity services and associated functions that related to incident management (Rød et al., 2020).

In parallel, the researchers developed and implemented many approaches for cyber risk management and technical frameworks for critical infrastructure protection supported by mathematical models and performance analysis methodologies in the technology perspective, such as the IRAM risk model developed by Ezell et al. (2000) to improve the efficiency of resource allocation for infrastructures (Brown et al., 2010). Besides, Critical Infrastructure Interdependencies Integrator (CI3) was designed

by Gillette et al. (2002) for modeling and estimating the time and costs for partial or complete restoration of critical infrastructures after disruptions or failures (Vespignani, 2010).

Baker et al. (2003) from James Madison University matured Network Security Risk Assessment Modeling (NSRAM) tools for critical infrastructure assessment through analysis of cyber and physical infrastructure security risks, determining the response nature of the system to attacks and incidents (Gutfraind, 2010). Then, Dobson et al. (2004) constructed CASCADE complex models for analyzing dynamic and probabilistic cascading failure within the entire infrastructure (Camphouse & Vugrin, 2011).

Moreover, Panzieri et al. (2005) tested CISIA agent-based simulations with various categories of infrastructure interdependencies (Sterbenz et al., 2010). Finally, Goodwin and Lee (2005) from Sparta, Inc. remodeled the Net-Centric Effects-based Operations Model tool (NEMO) for modeling impact cascades of events through multiple infrastructure networks and determining the results of the course of actions (Bhamra & Burnard, 2011).

In 2006, Ghorbani et al. created AIMS architecture, which contains extendable multi-agent analysis modules, and plugging visualization (Parshani et al., 2010). During the same year, Donzelli and Setola expanded GoRAF for integrating business and engineering perspectives to identify the risks related to enterprise interdependency (Ip & Wang, 2011).

In the same year, Outkin and Flaim (2006) presented a tool of Financial System Infrastructure (FinSIM) for modeling the financial service sector as a complex decentralized system with multiple interacting autonomous decision nodes or agents such as banks, traders, markets, and brokers (Tabansky, 2011).

Additionally, Trahan et al. (2015) presented that Healthcare Simulation (HCSim) developed a modeling tool for assessing the impact of mass casualties in health care and public health institutions. U.S. Los Alamos National Laboratory sponsors modeling tools (Lyn, 2015). Besides, Gertman et al.

(2006) used a Scenario-based Approach to Risk Analysis in support of cybersecurity (SARA) to support effective resource allocation in finances and personnel for critical attacks (Sansavini & Zio, 2011).

Besides the OGC CIPI framework that shares geospatial information for emergency response, Bagheri and Ghorbani (2007) also provided a UML-CI mean for communication modeling, knowledge transferring, and infrastructure understanding (Bashan et al., 2011). Likewise, Marti (2007) from the University of British Columbia worked on the Infrastructures Interdependencies Simulation Tool (I2Sim) to simulate scenarios for disaster responses at the system level with impact characterization (Dueñas-Osorio & Ouyang, 2011).

Henry et al. (2009) established an ERC-SCADA System-Petri Net Analysis tool to evaluate operational risks of cyberattacks on SCADA systems via Petri Net Analysis using a non-probabilistic metrics approach (Harrison et al., 2011).

In addition, U.S. Argonne National Laboratory launched in (2010) the Resilience Index (R.I.) and Better Infrastructure Risk and Resilience (BIRR) methodology for assessing infrastructure risk and resilience to various hazards (Lukas & Hromada, 2011).

The lab also built Critical Infrastructure Protection Modeling and Analysis (CIPMA) in (2012) for evaluating failures, dependencies, and resilience of critical infrastructure, as well as cascading impacts on other infrastructures. In addition, CIPMA supports the development of policies and regulations for national security (Sethi & Hnatyshin, 2012).

As well, Argonne Lab. demonstrated Enterprise Risk Assessment Technique (ERA) in (2013) for managing and mitigating risk using administrative procedures and resources (Sterbenz et al., 2013).

Under the same lab, Evans (2019) offered the Interdependent Repair and Restoration Processes (Restore©) tool for modeling the restoration and recovery of critical infrastructure systems from incidents. In addition, it was used to estimate the time and cost attributes of restoration goals



(Thompson et al., 2019).

Additionally, Lipol (2012) introduced Failure Mode Effect and Criticality Analysis (FMECA) is a technique for analyzing probable system failures, enumerating potential impacts, and classifying control and mitigation actions (Turnquist & Vugrin, 2012).

Similarly, Sandia National Laboratory (2012) in the United States delivered a Modular Dynamic Model (DMD) tool for modeling and simulating energy infrastructure interdependency operations, including generation, transmission, distributions, and trading (Filippini & Silva, 2012). Such a laboratory also assisted Jaeger et al. (2008) in utilizing Security Risk Assessment Methodology (S-RAM) for automated assessment of risks and resilience related to physical critical infrastructure attacks (Harrison et al., 2011).

Correspondingly, Stergiopoulos et al. (2015) developed a Critical Infrastructure Dependency Analysis tool (CIDA) to model and analyze the dynamics of cascading failures with time. They were also used to model and analyze interdependencies and risk reductions (Kalala, 2017). Lewis (2015) was supported by the Naval Center of Homeland Defense & Security to develop a Model-Based Risk Assessment (MBRA) for analysis of critical infrastructure network components and faults for efficient resource allocation (Labaka et al., 2016).

The project of NEXUS Fusion Framework (2017), funded by InnovateUK and conducted in partnership with IntePoint, LLC, established the tool for modeling, analyzing, and visualizing planned and unplanned effects and consequences of an event through multiple urban infrastructures in real-time (Malik & Sahu, 2019).

Scalable Network Technologies, Inc. (2018) updated and deployed the network simulation software (QualNet) as an all-embracing tool for modeling, analyzing, planning, testing, and training that mimics the behavior of real communications networks (Ormrod & Turnbull, 2019).

## Appendix B: Definition of Key Terminologies

This section studies linguistically and technically a particular set of important terms and expressions used in this research, whether it consists of a single word or multi-word with an intense focus on their specific meanings in the cyber context. However, some of the similar terms have different meanings across other disciplines (Levalle & Nof, 2017), as the followings:

- 1 Cyber: Prefix was derived from the Greek word *Kybernetes*, meaning "**governor**" or "**steersman**" (Haque et al., 2018). In 1992, the term was coined by Norbert Wiener and used for the first time to refer to "**person, thing, or idea as part of the computer and information age**" (Ren et al., 2017); it then developed into including networks, data, and at present with the internet (Linkov & Kott, 2019).
- 2 Resilience: Latin derivative word from "**resilio**" denotes "**to jump back**" (Sansavini, 2017). In the 1940s, the term initially had roots in psychology literature to describe the "**positive capacity of people to cope with stress and adversity**" Cleland and Cotton (2011) and gradually applied in different disciplines, especially risk management (Thomas et al., 2018). Many scientists proposed various definitions for resilience over the past decades based on the research domain (Viswanathan et al., 2017). First was Holling (1973), who characterized resilience as a "**measure of the persistence of systems and of their ability to absorb change and disturbance and still maintain the same relationships between populations or state variables.**" After that, Wildavsky (1988) defined it as the "**capacity to cope with unanticipated dangers after they have become manifest, learning to bounce back.**" Recently, Han et al. (2012) suggested a clearer one as "**the amount of the system can avoid maximum impact,**" while Ali et al. (2013) define it as "**the speed at the system recovers from a disruption.**" An additional example is Lyn (2015), the ability "**to withstand an extreme natural event without suffering devastating losses, damage,**

*diminished productivity, or quality of life.*" Beyond doubt, Nan and Kröger (2016) published a broad description of resilience as *"the ability of a system to resist the effects of disruptive forces and to reduce performance deviations"* (Zebrowski & Sage, 2017).

- 3 Cyber Resilience: The combination of *"cyber"* and *"resilience"* terms systematically leads to numerous definitions described by several researchers but in the same perspective, such as *"the ability to continuously deliver the intended outcome despite adverse cyber events"* Björck et al. (2015), and *"the ability of a computing system to recover quickly should it experience adverse conditions"* Bernstein (2017). The updated U.S. Presidential Policy Directive PPD-21 (2018) defines resilience in cyberspace as *"the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions"* (Caron, 2019). Generally, cyber resilience can be taken into consideration at different levels with unique challenges and methods for each: Global level (e.g., the internet), supranational level (e.g., European Union), national level (e.g., U.S.), local level (e.g., Dubai), organizational level (e.g., Central Bank), and technical level (e.g., SCADA system) (Mbanaso et al., 2019).
- 4 Dynamic Cyber Resilience: The notion of dynamic cyber resilience denotes handling the continuous changes over time with a self-motivated approach to maintaining the *"fundamental quality of individuals, group and organizations, and systems as a whole to respond productively to significant change that disrupts the expected pattern of events without engaging in an extended period of regressive behavior"* Horne and Orr (1997). The United Nations International Strategy for Disaster Reduction (UNISDR, 2005) stated a comprehensive explanation: *"capacity of a system, community or society potentially exposed to hazards to adapt, by resisting or changing to reach and maintain an acceptable level of functioning and structure. It is determined by the degree to which the social system can organize itself to increase this capacity to learn from past disasters for better future protection and to improve*

*risk reduction measures*” (Sansavini & Fang, 2016). Hence, it *“notices complex dynamics of infrastructure response process”* Rosato (2008), and *“the capability to cope and bounce back”* Vespignani (2010), while Dinh et al. (2010) described it as the *“ability to adapt to new situations.”* Also, Beatley et al. (2011) stated that *“the speed of systems to go towards equilibrium”* as well as Goldman et al. (2011) that *“be inherently reliable and flexible and adaptive”* and *“assess how capable the infrastructure is to absorb the cyber disruptions”* Vugrin et al. (2011). Another example, Smith et al. (2011), proposed that it is the *“ability to withstand external impacts and recover with at least outside interferences.”* Moreover, *“the ability of a system to withstand an unusual perturbation and to recover efficiently from the damage”* Agarwal et al. (2011). Furthermore, Wang et al. (2013) suggested a depiction as *“capture the importance of cyber topology and interrelationships between infrastructure constituents”* in the context of *“the interactions between infrastructure behavior and cyber disturbances”* Petit et al. (2015). In addition to *“the ability of the infrastructure to mobilize resources and deliver the intended level of cyber services”* Betz (2017), and *“identify when the infrastructure will recover to original functioning state”* He and Cha (2018).

- 5 Interdependency: The Merriam-Webster Encyclopedic Dictionary (2006) notes that the term interdependency combines two specific words linguistically, inter, and dependency (Guo, 2010). The prefix ‘inter’ means related to, between, within, and shared. On the other hand, dependency means being influenced, determined by, conditioned by, or subject to another for support (Bloomfield et al., 2017). Technically to Zimmerman (2001), interdependency is a critical bidirectional relationship between two or more entities in a system where one entity’s status is directly dependent on and controlled by another entity’s status and vice versa (Vespignani, 2010). As Rinaldi et al. (2001) state, *“it is impossible clearly to adequately analyze or understand the behavior of a given infrastructure in isolation from the environment or other infrastructures.”*

The recent definitions suggested by Dudenhoeffer et al. (2006) were *"the status of one component could influence or be influenced by the status of the other one,"* and Setola et al. (2014) attempt to identify the complicated relationships between at least two parts of a system were *"a bidirectional linkage or connections between two elements."* The interdependencies are divided into four categories, are physical, geographical, logical, and cyber. Rinaldi et al. (2001) proposed these categories, and similar ones have been investigated by Vespignani (2010). From the CII's perspective, interdependency means one CII is contingent on the operability and outcomes of another interconnected CII (Abdelgawad et al., 2019).

6 Infrastructure: This term linguistically appeared in the 1880s, but the U.S. National Research Council adopted it formally in 1987 (Beyza et al., 2019). The U.S. Presidential Decision Directive 63 in 1998 defined it as: *"the framework of interdependent networks and systems comprising identifiable industries, institutions including people and procedures, and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security, the smooth functioning of governments at all levels, and society as a whole"* (Herrera & Maennel, 2019). As a network, the infrastructure is combined with physical systems and structures with high-cost investments vital to national development and prosperity (Burla et al., 2016). Bruno (2002) differs it into three types: physical, virtual, and critical. The physical infrastructures are roads, bridges, airports, harbors, water, sewerage networks, vehicles, and aircraft that run industrialized and modern cities (Gamboa et al., 2020). In contrast, the virtual infrastructures provide particular services to country people for maintaining the economy, such as telecommunications, healthcare, educational, financial, and governmental systems (Hofreiter & Zvaková, 2017).

7 Criticality: The term refers to the state of quality or degree of importance. In the context of critical infrastructure, Lepinski and Kent (2012) defined it as a *"level of infrastructure*

*contribution to society in maintaining a minimum level of national and international law and order, public safety, economy, public health, and environment."* Further, Bush et al. (2014) turned the definition into *"Impact level to citizens or the government from the loss or disruption of the infrastructure."* Hence, infrastructure is deemed critical if a severe disruption of that *"infrastructure could lead to damage on a large scale, or its impact would be sufficiently severe"* (Panzieri et al., 2019). Usually, infrastructure is defined as critical due to its *"strategic position within the whole network of infrastructures, and especially due to interdependencies between the infrastructure and other infrastructures"* (Faramondi et al., 2020). Thus, it is acknowledged broadly; however, some infrastructures have come to be seen as critical due to *"their inherent symbolic meaning to evolve beyond the conventional sector-based focus and to look at the information, services, and the cyber flows, their role, and functionality"* for modern society, and especially the core values that are delivered by the infrastructures (Banerjee et al., 2018). The concept of critical functionality is essential to understand the purpose and outputs of the valued infrastructure and guide planning for cyber resilience to failure (Gritzalis et al., 2019).

- 8 Critical Infrastructure: In 2001, U.S. Public Law 107–56 identified critical infrastructures as *"systems and assets, whether physical or virtual, so vital to the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety"* (Karabacak et al., 2016). Moteff et al. (2003) clarify that critical infrastructures are the essential assets classified by the government as extremely important to operate the economy and society (LaRocca, 2014). While E.U. Commission (2006) defined it as: *"an asset, system or part thereof located in member states are essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of having a significant impact as a result of the*

*failure to maintain those functions"* (Pedroni et al., 2016). Also, an alternative definition of critical infrastructure provided in the E.U. international CIIP handbook version (2009) that *"infrastructures whose incorrect functioning, even for a limited period, may negatively affect the economy of individual subjects or groups, involving economic losses and/or even expose them to safety and security risk"* (Sarwat et al., 2018).

- 9 Critical Information Infrastructure: in this digital era, all critical infrastructures widely depend strongly on the assets and processes of information and communications (Theron & Bologna, 2013). These cyber assets and processes play a glue role in interconnecting infrastructures, operating as a standalone critical information infrastructure or a subset of other critical infrastructures (Viira, 2018). G8 coined the CII term in 2001, and OECD redefined it in 2008 as *"ICT systems that are critical infrastructures for themselves or that are essential for the operation of critical infrastructures that affect the achievement and continuity of state mission and the safety of society that disruption or destruction of would have a serious consequence"* (Selifanov et al., 2020). In 2014, African Union added to the OECD definition the phrase *"essential to vital services for public safety, economic stability, national security, international stability and for the sustainability and restoration of critical cyberspace. The disruption or destruction of would have a serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of the government or the economy"* (Mbanaso et al., 2019). Besides, Estonia, ranked in 2020 as a leader of the global cybersecurity index, stated the definition of CII as an *"Information and communication system whose maintenance, reliability, and safety are essential for a country's proper functioning. The critical information infrastructure is a part of the critical infrastructure"* (Martin, 2020).
- 10 Interdependent Critical Information Infrastructure is investigated as complex, interdependent adaptive networks among real-world systems based on their cyber interdependency (Zheng &

Albert, 2019). They have been clarified by Lee et al. (2007) as *"information processes supported by Information and Communication Technology (ICT) that are critical infrastructures by themselves or that are critical for the operation of other critical infrastructures"* (Anne et al., 2018). The focus is on analyzing the impacts of cascading failure through mutual interdependencies, addressing bidirectional relationships in critical information infrastructures (Gnatyuk et al., 2019).

- 11 Vulnerability: The term definition of vulnerability refers to *"three degrees: the degree of exposure to risk, the degree of loss, the degree of resilience,"* based on Kröger and Zio (2011). Besides, Aven (2011) offers a slightly different definition where *"vulnerability is defined as the manifestation of the inherent states of the system that can be subjected to a natural hazard or be exploited to affect that system adversely."* However, Wang et al. (2015) extended the vulnerability concept to include the *"changes of characteristics, scale or duration of loss, the frequency of failures or severity following hazards or attacks."* In 2018, Solicitors Regulation Authority (SRA) of the UK published its handbook version 21 and considered the vulnerability as a *"technical property that interprets the weaknesses in design, implementation, operation or management of infrastructure, or its elements when exposed to risk source, renders it susceptible to destruction or incapacitation or reduces its capacity to resume new stable conditions"* (Abdelgawad et al., 2019). The International Risk Governance Council (IRGC) stipulates that infrastructure vulnerability is a viable research area, especially for coupled infrastructures because of mutual interdependencies that exist among them (Chen, 2016).
- 12 Cyberattack: The special publication of risk assessment guidance number 800-30R1 (2012) published by the U.S. National Institute of Standards and Technology (NIST) defines a cyberattack as *"any circumstance or event with the potential to impact organizational operations adversely, functions, reputations, assets, individuals through an information system"*



*via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service*” (Schneider et al., 2015). As well as in the handbook version 2016 of information security approved by the U.S. Federal Financial Institutions Examination Council (FFIEC), defines a cyberattack as an *“event that could cause harm to the confidentiality, integrity, or availability of information or information systems, through unauthorized disclosure, misuse, alteration, or destruction of information or information systems”* (Kochedykov et al., 2020). In 2017, The U.S. Office of Financial Research (OFR) enhances the definition of cyberattack with *“deliberate efforts to disrupt, steal, alter, or destroy data stored on IT systems”* (Sinha et al., 2020). The Department of Homeland Security in the U.S. realizes the urgency and need to protect the CII networks in different critical infrastructures: *“attacks on the critical network and key resources could significantly disrupt the functioning of government and business alike and produce cascading effects far beyond the targeted sector and physical location of the incident. Direct terrorist attacks and natural, human-made, or technological hazards could produce catastrophic losses regarding human casualties, property destruction, and economic effects, as well as profound damage to public morale and confidence”* (Yong et al., 2016).

- 13 CII Cyber Failure: The increasing connectivity of today’s CII networks has meant that disruptions’ direct impacts lead to indirect multiplier effects (Jahromi et al., 2019). For considerable time US public policymakers considered CII networks *“as facilities with the common characteristics of capital intensiveness and high public investment at all government levels”* (Mosharraf et al., 2015). The Clinton Executive Order described CII networks in a cybersecurity context: *“the framework of interdependent networks and systems comprising identifiable industries, institutions, and distribution capabilities. It provides reliable products and services essential to the defense and economic security, the smooth functioning of government at all levels, and society as a whole”* (O’Halloran et al., 2017).

14 Optimization: The methodology of alternative actions to “finding the best solution from all feasible solutions” Bradley and Atkins (2015). *“Attempts to optimize (maximize or minimize) infrastructure objectives and functions without violating resource constraints”* Barron (2016). Li et al. (2018) stated it as a *“Maximum or minimum value of the objective function subject to the constraints where the input variables are restricted through identify potential areas, analyze processes, raising productivity, removing loss, and establishing controls.”* The National Institute of Standards and Technology defined it as *“maximizing effective performance by minimizing the cost factors to attain as efficient infrastructure functionality as possible under the cyber constraints”* (NIST, 2018).

## **Appendix C: Secondary Data Overview**

This research's secondary data depends on the information collected from the literature related to the thesis topic and already handled through primary sources in the past and published by the research community, and made readily available for reuse (Dibaji & Ishii, 2015).

Such secondary data's main advantages are ease of access, inexpensive, time-saving, longitudinal and comparative, and new insights (Friedman et al., 2017). Furthermore, it benefits the thesis for identifying the established research gaps, purpose, objectives, assists for formulating the research questions, and hypotheses helps for designing the research methodology and quantitative methods, supports for the developing and optimizing the proposed solution, provides evaluating metrics and testing scenarios, and facilitates the analyzing and comparing the research results (Bowker et al., 2019).

Furthermore, a systematic literature review inspired this research. It used the guidelines described by Kitchen ham and Charters (2007) and extended by Neiva and Silva (2016) to avoid the disadvantages of the secondary data like low quality, irrelevant, exaggerated, and outdated information (Sepúlveda-Estay et al., 2020). It outlines the strategy of identifying key sources of secondary data, generating terms, searching items, sourcing databases, collecting tools, evaluating criteria, documenting selected studies, analyzing the contents, and synthesizing the central debates, unique patterns, and new trends that have scientific values for articulating how to address the thesis gaps (Xiong & Lagerström, 2019).

The systematic reviewing process's sequential steps start with efficiently identifying a set of accredited publication sources, scanning the extant literature, and seeking the primary studies. Besides, extracting and analyzing the data, assessing the quality of founded information, criticizing the arguments, and finally synthesizing the inclusion based on the thesis questions as a guiding point

(Singh et al., 2016).

Identifying the research key terms comes mainly from the thesis title (Bergström et al., 2015). The central search term is ‘dynamic cyber resilience’ to focus on the solutions to meet the increasing threat of cyberattacks against CIIs. The other searches contain keywords such as ‘critical information infrastructures,’ and ‘cyber interdependency,’ and ‘coupling networks,’ and ‘scale-free topology,’ and ‘concurrent cyberattacks,’ in addition to the 31 combinations of these search terms (Wang et al., 2019). If there is more than one search box with Boolean operators, then ‘dynamic cyber resilience’ is entered in the first box, and other keywords are added to the other boxes with the AND operator selected (Caverzan & Solomos, 2014).

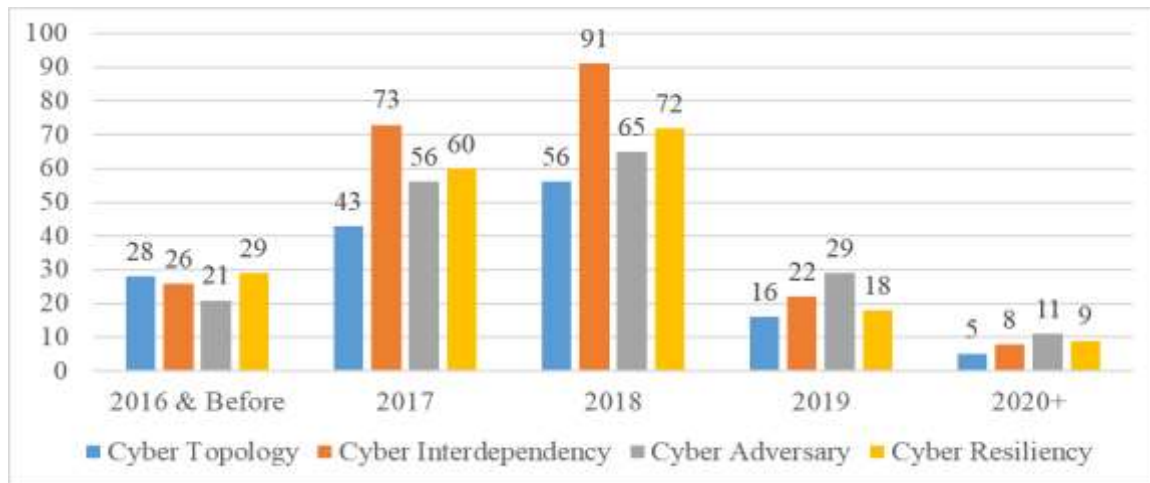


Figure 2.1: Research Items based on Publication Year by Domain

Furthermore, gathering the potential databases list derives from other systematic literature reviews and the library’s website of the British University in Dubai that suggested database repositories for computer science research (Bhamra et al., 2011). These databases include EBSCO, ProQuest, Elsevier Science Direct, Springer Link, IEEE Xplore, Google Scholar, ACM Digital Library, Compendex, SAGE, LISTA, and Computers & Applied Sciences Complete (Ani et al., 2019).

All non-refereed papers and books are excluded when databases allow for an advanced search.

Additionally, the subject of computer science restricts papers. An initial search was conducted between 2017 and 2020+. A second search was conducted between 2010 and 2016. As a result, two-thirds of publications were released in 2017 and 2018, around 16% in 2019 and 2020+ by research domains shown in Figure 2.1 (Bosetti et al., 2016).

Before the study selection process, the duplicate papers identified by different database keyword searches were removed. Then, the study data were stored in software of the Mendeley Desktop version 1.19.3 (2018), and the studies were listed in separate tables for each stage of the selection process by keeping the available information like the following: title, author, affiliation, publication source, publication year, publisher, and abstract (Caverzan & Solomos, 2014).

The selection of studies for inclusion in this research is described and documented within the three-stage process: (1) selection by title. (2) selection by an abstract. And (3) selection by paper. The initial selection of studies is based on the paper's title and the next stage upon reading the abstract and keywords (Fernando et al., 2017). Additionally, after the first two stages were completed, the selected studies moved to further select studies based upon browsing the whole paper's content with any additional information required for the selection (Gasser et al., 2019).

The start number of papers evaluated at the first stage is 16,552 different papers from the database search and selected 738, moved to the second stage of paper selection. Finally, 374 papers from the original search had relevant abstracts in the third stage and warranted further reading and searching the author's websites for additional work (Harrop & Matteson, 2015).

The second stage's selected studies categorize into three sectors: academia, government, and commercial (Ouyang, 2014). The academic contributions have been extracted from 572 journal articles, conference proceedings, and books, while the 106 white papers and official studies form the primary research items from the government sector (Liu & Song, 2020). As a final point, the total count of 82 technical reports and expert presentations cover the commercial sector's main research

inputs, as shown in Figure 2.2 (Saidi et al., 2018).

Automatically, the selection process's inclusion criteria focused at each stage on identifying peer-reviewed studies that meet the research objectives, report dynamic cyber resilience and involve the environment of the critical information infrastructures (Tatar, 2020). These criteria take in the: (1) theoretical frameworks of development solutions; (2) practical implementations using quantitative research methods; (3) empirical results from evaluation testing scenarios; and (4) optimal algorithms and models to drive improvement for existing solutions (Ullah et al., 2018).

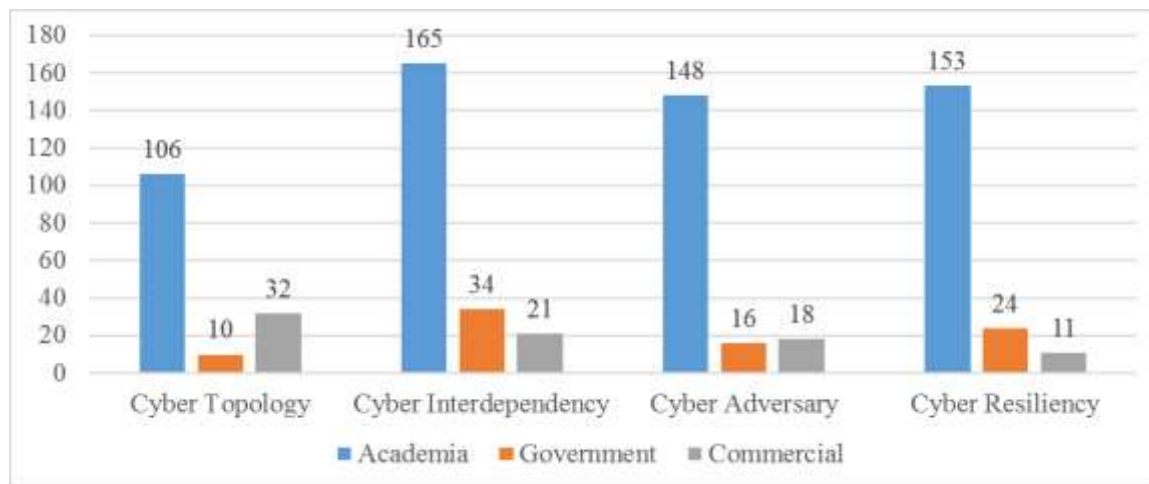


Figure 2.2: Research Items based on Sector Contributions by Domain

On the other hand, the rejected studies at each stage of the selection process met exclusion criteria that include: (1) homogeneous and physical critical information infrastructures; (2) policy frameworks of cyber resilience; (3) technical vulnerabilities; (4) cyber risk management and cybersecurity; and (5) single and multiple cyberattacks (Xiong & Lagerström, 2019).

During the first stage of selection, any titles that contained the phrases' critical information infrastructure', 'interdependent critical information infrastructure,' 'cyber resilience,' 'dynamic cyber resilience,' or any variation thereof were selected for inclusion in the next stage of the study unless they were obviously outside the scope of this research (Arghandeh et al., 2016).

In the second stage, each abstract was read while considering inclusion and exclusion criteria in addition to a paper classification. A classification of 'R' denoted papers to be read thoroughly to determine inclusion. A classification of 'S' denoted supporting papers that may be useful. At last, a classification of 'O' denoted papers that were out of scope because they did not meet the inclusion criteria. In comparison, the third stage incorporated a reading of the selected papers (Bosetti et al., 2016).

Moreover, the first and second stages are repeated on a random sample of papers for selection process verification. Details of the final inclusion or exclusion classification, quality assessment, corresponding reason, and the data extraction were recorded (Bhamra et al., 2011). After all the systematic literature review selection stages were complete, the next step measured the selected studies' quality and extracted the secondary data from each of them (Caverzan & Solomos, 2014).

Assessing the quality of each selected study conducted by answering the questions was generated based on the components of similar studies in the different topics and domains, have high citation scores widely (Harrop & Matteson, 2015), (Fernando et al., 2017), and (Liu & Song, 2020).

The assessment questions are outlined as the following:

Are the study purposes interrelated clearly to the thesis scope?

Are the study limitations enumerated, and can they be linked with the research gaps in the thesis?

Are the study methodologies well-defined and associated with the thesis purpose?

Are the research methods used in the study coming up with the thesis goal's context?

Are there contributions listed in the study appropriate to the thesis objectives?

Are the empirical results in the study evident and relevant to the thesis questions and hypotheses?

Are the testing scenarios in the study significant and can be used for comparisons in the thesis?

Are the quantitative metrics in the study suitable for evaluating the solutions in the thesis?

Are the references in the study recent and published with good impact factors?

All of the above questions have three possible answers and associated numerical values: yes (1), no (0), or somewhat (0.5). The sum of the numerical values for the quality assessment questions provides a relative measure of study quality (Gasser et al., 2019).

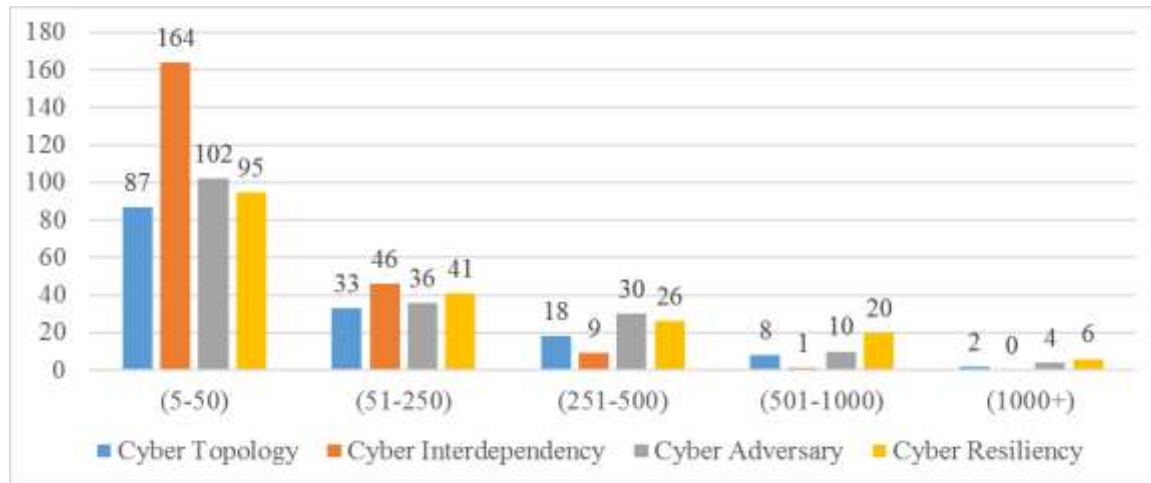


Figure 2.3: Research Items based on Number of Citations by Domain

The quality of the published research items was controlled by the number of citations based on google scholars' search engines. About 60% of the research items have 5 to 50 citations by four research domains, and 21% of them have 51 – 250 citations, while the rest of the research items have more than 251 citations, as shown in Figure 2.3 (Wang et al., 2019).

After finalizing the quality assessment, the extraction of secondary data from the selected studies includes research gaps and objectives, the definition of terminologies, official records and technical statistics, characteristics of existing solutions, limitations, and contributions, quantitative research methods, testing scenarios, evaluation metrics, analysis tools, and results, future trends, and recommendations (Sepúlveda-Estay et al., 2020). These extracted data were maintained in several locations such as internal wiki, paper notes, and excel spreadsheets, allowing for the more straightforward synthesis of secondary data (Singh et al., 2016).



## **Appendix D: Research Methodological Choices**

Research philosophy refers to how knowledge is developed, as Saunders et al. (2016) mentioned. It incorporates beliefs and assumptions into how this research development constitutes the cornerstone for the choice of research philosophy (Ferreira, 2019). As shown in Figure 4.1, the snapshot of Mark's onion of the research process, the philosophy influences the subsequent choice of methodology, research strategy, data collection techniques, and analysis procedures (Potii & Tsypinsky, 2020).

The overall research philosophy considered explicitly in this thesis is based on the epistemological position that agrees with the positivism theory (Hehenberger et al., 2016). Epistemology plus positivism uses scientific methods, observable and measurable facts, causal explanation, and prediction (Hong et al., 2012).

In this way, this research's epistemological approach is the paradigm approach, as denoted by Thomas (1962). It considers scientific knowledge as groups of ideas known as paradigms that help explain the world (Igor & Aleksandr, 2018). The use of these paradigms on the data until unexplainable differences between the current paradigm and the data seen in the world require this paradigm to change (Kochedykov et al., 2020).

Through this lens, this research's epistemological position is a concept that refers to the aspects of "What is constitutes good quality data?" Furthermore, given the nascent nature of dynamic cyber resilience in the interdependent CII networks, the paradigms approach is realized as the most appropriate to accommodate new solutions that rely exclusively on quantitative data (Nan & Sansavini, 2017).

Positivism is a philosophical theory stating that specific positive knowledge is grounded on verified data from the senses, known as empirical evidence and their properties and relations; such positivism

is constructed on empiricism (Marais & Uday, 2015). Thus, information derived from sensory experience, interpreted through reasons, forms the only source of all specific knowledge (Lukas & Hromada, 2011). Positivism holds that helpful knowledge is found only in these positive facts (Orojloo & Azgomi, 2017).

Computing scientists use several approaches to tackle the research questions within the discipline. Even the activities required to tackle a single research question may include several approaches (Pipyros, 2019). This research used a deductive inference approach. This approach adopts the logic by listing several relationships between hypotheses and conclusions (Uday, 2015). The primary data was collected and analyzed to evaluate the hypotheses of the proposed solution compared to existing ones. If the hypotheses are formulated correctly, the conclusions must also be correct (Ottenburger et al., 2020).

Moreover, the results of deductive research could be generalizable. The idea is to generalize the conclusions to the specific (Ani et al., 2019). Thus, the novel conceptual framework proposed in the thesis can be verified. The merging of theoretical with empirical by combining three research methods in this single study became quantitative multi-methods (Turskis et al., 2019).

With the consideration of possible evaluative purposes for this research, it is also essential to identify and define the methodological choices available in terms of three dimensions (Başar & Zhu, 2012): (1) Quantitative research is generally associated with positivism (Setola et al., 2017). (2) Associated with the deductive approach to conceptual framework development (Bloomfield et al., 2017). (3) Focus on the data to test the proposed solution (Senovsky et al., 2019).

As such, a quantitative approach seeks to identify and analyze the capabilities of dynamic cyber resilience between proposed solutions and standard solutions by different numerical and graphical methods (Nan & Sansavini, 2017). Accordingly, it can use the data from single or multiple techniques and data collection sources upon the time horizon chosen (Fotouhi et al., 2017).



Figure 4.1: Methodological Choices of this Research (Potii & Tsyplinsky, 2020 modified)

The benefit of a longitudinal time study is detecting the changes in dynamic cyber resilience capabilities of the same targets of interdependent critical information infrastructures at both the group of the existing solutions and the proposed solution over time during computing simulations and emulating experiments (Moraitis et al., 2020).

This study will examine research questions regarding the methodological choices of research paradigms and practical experiments. The findings work toward a final justification for an interpretation approach (Nan et al., 2014). Therefore, making appropriate methodological choices concerning information management ensures thoughtful methodology and likely research results (Häring et al., 2016).

## *Quantitative Methods*

Methodically, the research community has introduced five quantitative research methods for data collection, data validation, and data analysis, including analytical modeling, simulation, emulation, testbed, and real-world experimentations (Choras et al., 2015). These methods are used to test and evaluate dynamic cyber resilience capabilities for the proposed solution developed within this research (Senovsky et al., 2019). As well, comparing the results with the other results of the existing solutions in the same field (Johnston et al., 2014).

At a glance, the analytical models are a set of mathematical equations that simplify the data analysis and represent the technology solutions' modeling procedure (Georgiev & Nikolova, 2017). In comparison, the simulation is the most effective and frequent quantitative method for data collection and validation (Dueñas-Osorio & Ouyang, 2011).

Correspondingly, designing the cyber algorithms and protocols allows testing and improving them at any development stage (Deng et al., 2017). Simulators and various real-world scenarios can be modeled (Sansavini & Fang, 2016).

As a hybrid method, emulation is a combination of hardware and software components accompanying simulation possibilities for network modeling, data collecting, and validating (Kiss et al., 2015). Emulators use the firmware and hardware to execute simulations in laboratory conditions (Oliva et al., 2019). Since emulators can be utilized in real environments, they potentially perform precisely in comparison to simulators (Rahnamay-Naeini & Hayat, 2016).

Physical testbeds are frameworks for the real implementation of algorithms and protocols (Shevchuk, 2019) that allow remote configuration, running, and monitoring experiments and support the model, protocol, and algorithm evaluation. Thus, they have bridged the gap between simulation and real devices' deployment (Ormrod & Turnbull, 2019).

Real-world experimentation allows for feasible and actual deployment practices in production environments (Rasouli et al., 2014). All the functions are set in reality, and no incorrect or inaccurate presumption is made. It is the ultimate stage of validating algorithms and protocols (Zhu & Chen, 2020).

The quantitative methods range from purely software-based to solely hardware-based (Chowdhury et al., 2020). Figure 4.2 depicts each method's contribution regarding the proportion of cyber and physical spaces they use (Sharif & Sadeghi-Niaraki, 2017). In this regard, analytical modeling and simulation are only performed in cyberspace, and no physical deployment is implemented (Dan-Suteu & Gânsac, 2020).

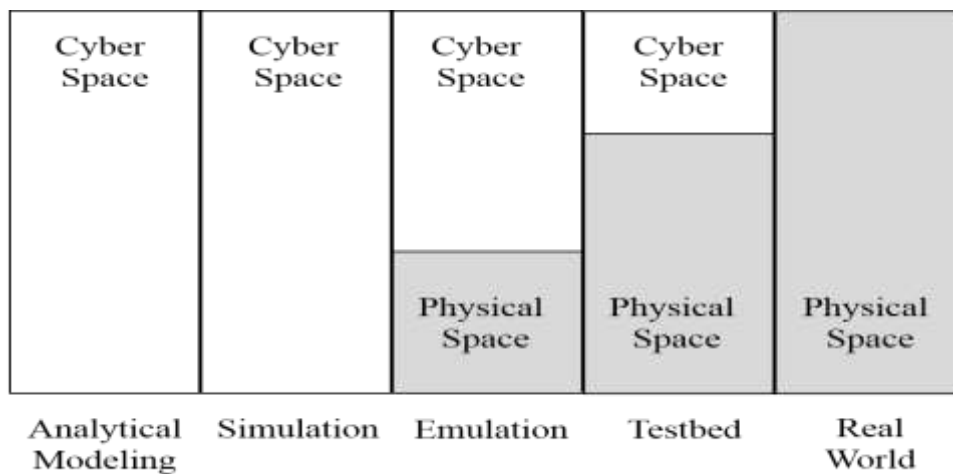


Figure 4.2: Proportion of Quantitative Research Methods from Cyber Space to Physical Space (Sharif & Sadeghi-Niaraki, 2017 modified)

For emulators and testbeds, this sounds different. These methods apportion their throughput to cyber and physical spaces, as pointed out by Halder and Ghosal (2016). In the former, cyberspace has a much generous portion, while in the latter, most of the implementation is dedicated to physical space (Grafenauer et al., 2018).

Real-world deployment, as the latest method, fully manipulation and implementation, concentrates on

the physical space usually applied in the implantation research (Sterbenz et al., 2013). In this research, three of the above quantitative methods have been adopted and used. Simulation and emulation are used for data collection and validation, while analytical modeling is used for data analysis (Leslie et al., 2018). These methods have intended to organize the research design discussion required, whereas each method has pros and cons (Ouyang, 2014).

On top of that, analytical modeling has low cost and provides quick insight and initial evaluation; in contrast, the deduced results are not precise in terms of the massive number of nodes and links, unattended processes in the complicated environments (Barker et al., 2017).

Additionally, the simulation method is fast, low cost, easy to implement, repeatable, supports tight controlling, scalable, i.e., supports many nodes, and supports dynamic and flexible modeling and heterogeneous environments (Rozorinov et al., 2017). Conversely, it considers a high degree of abstraction and may not generate accurate results as real implementation since it contains oversimplified protocols (Sethi & Hnatyshin, 2012).

The emulation is repeatable, supports tight control, and provides a certain degree of realism contrariwise; it has low speed, limited scalability, platform dependence, technical bounds, and high cost per tested node (Castillo et al., 2019).

After considering all the positive and negative aspects of the selected quantitative methods, the thesis investigates the proposed solution results compared with standard solutions under different cyberattack scenarios (Mohammad et al., 2017). It enables the assessment of dynamic cyber resilience capabilities and evaluates the proposed solution developed and implemented purely in cyberspace and a mixture of cyber and physical spaces (Welsh, 2013).

The main reasons for selecting these three methods in this research are the thesis topic, focuses exclusively on the cyber aspects of the critical information infrastructures, especially the layer-3

capabilities of technology solutions that provide the dynamic cyber resilience for interdependent CII networks (Malik & Sahu, 2019).

Furthermore, this research is a self-funded study by the author; therefore, there is a financial cost for deploying additional hardware if the testbed method is selected because it needs expensive technical requirements (Seppänen et al., 2018). In contrast, the emulation method gives the same results, although it has a physical part less cost and minimal hardware requirements, mainly when operating in virtual environments (Das et al., 2020).

Lastly, the real-world quantitative method is rarely applied in critical information infrastructures' production ecosystems except for exceptional cases (Igor & Aleksandr, 2018). This method has very high costs and anticipated risks when used, such as disrupting the CIIs' susceptible operations or interrupting their sensitive services in many sectors (Pipyros, 2019).

### ***Technical Instrumentation***

From the beginnings of the development of modern scientific methods, its emphasis on testable hypotheses required the ability to make quantitative and ever more accurate measurements (Nan & Sansavini, 2017). As a result, it revolutionized how researchers look at the world and refined and extended their senses' range (Herrera & Maennel, 2019).

Technical instrumentation is the process of constructing research instruments used to obtain, measure, and analyze data from subjects around the study topic. Therefore, the OPNET simulator and GNS3 emulator were employed in collecting data and the MAXIMA platform for analyzing data appropriately on this thesis (Marais & Uday, 2015).

The reasons beyond selecting these instruments in this research among more than 150 quantitative instruments that are available in the literature lie in its unique features that include the licenses provided free of charge for academic users, the platforms supported by numerous operating systems,

and the presence of online installation tutorials (Das et al., 2020).

These three instruments also have the open-source capability with the benefits of modifiable source code and free extension of the software (Herrera & Maennel, 2019). As well, they are the most widely used in similar researches like this study and provide powerful and graphical user interfaces to visualize the topology structures of the CII and easily drag and drop the nodes, links, and networks with different displays of the data collected in the potential failure behavior analysis (Van der Kleij & Leukfeldt, 2019).

All of them are object-oriented software designed with C/C++ embedded coding language in addition to their suitability to run the widespread networking protocols operated in the proposed solution and standard solutions of dynamic cyber resilience (Pitt-Francis & Whiteley, 2017).

The first instrument is OPNET. It is the first well-known commercial general-purpose network simulator developed in 1987. It is an object-oriented and discrete-event optimum modeler with the ability to simulate the behavior and measure the performance of any type of network (Lu & Yang, 2012).

The educational version is rugged, versatile, and available free for academic purposes. Recently OPNET, acquired by Riverbed Technology, replaced its name with Riverbed Modeler (Mohammad et al., 2017).

The OPNET riverbed modeler version 18.8.0, released in February 2019, academic edition software compatible with Microsoft Windows operating system was used to configure the testing labs and collect data in this research (Sethi & Hnatyshin, 2012).

OPNET simulator provides a virtual network environment that models entire CII networks' behavior, including routers, switches, and protocols, servers that are empowered to diagnose testing scenarios more cost-effectively by understanding the impact of changes and validating these before implementation (Dan-Suteu & Gânsac, 2020).



As illustrated in Figure 4.7, the OPNET software package runs over the architecture of four typical online servers separately hosted in the global web-hosting provider; all servers have the same technical specifications and configurations as the following:

- Processor : 4 CPUs x 2 Core @ 3.3 GHz.
- Motherboard : Super micro H8DGi.
- Storage : 500 GB (Mirrored RAID 1).
- Memory : 16 GB RAM.
- Bandwidth : 15 TB.
- Network : 10GbE × 5 with 5 IP Addresses (Traffic Metered).
- Operating System : Microsoft Windows Server 2019 (64 bit).

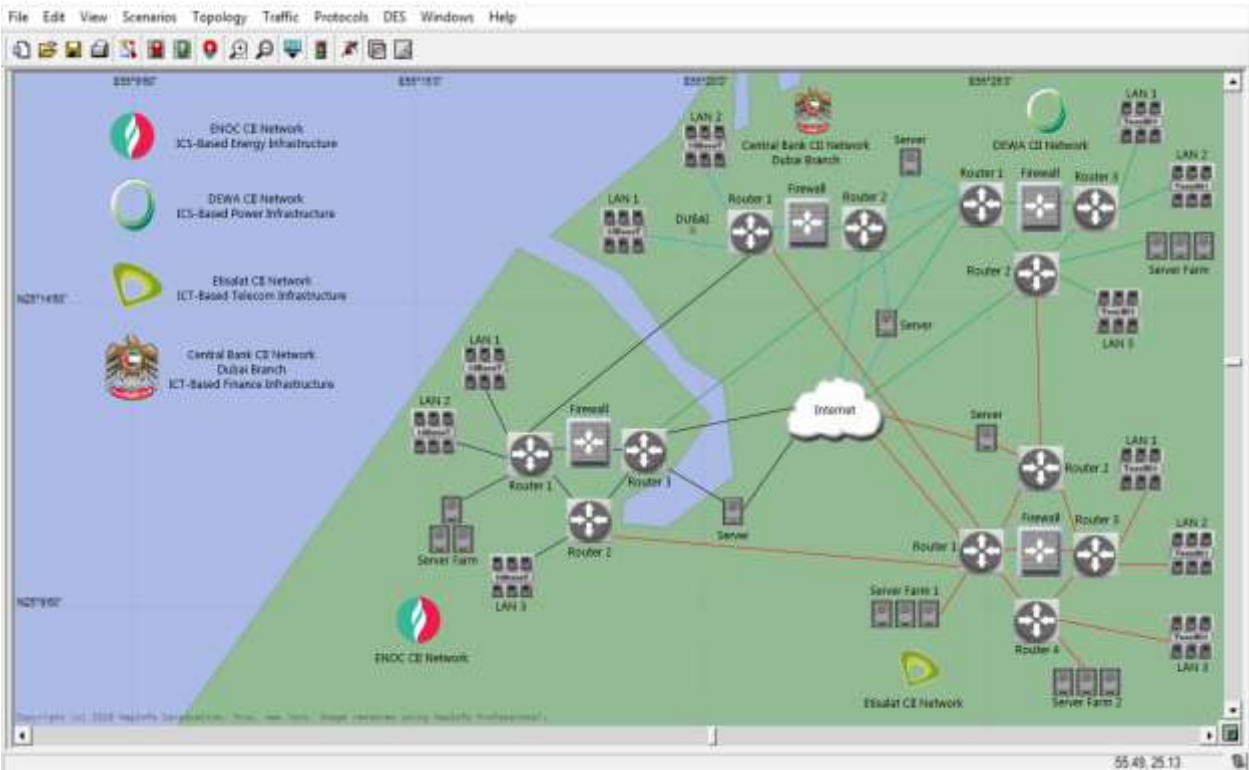


Figure 4.7: OPNET Simulator Setup Settings and Configurations

Each server is dedicated to testing just one solution parallel with standard solutions based on the same setup settings. Several simulation labs of CII networks were implemented over the OPNET simulator. They were designed upon the testing scenarios described exhaustively in section 4.3.3 of the Chapter

(Rozorinov et al., 2017).

Every OPNET server has fixed labs containing a direct link network with media control access and medium access control for wired connected stations. The set of local area networks interconnected by switches, planning CII networks with different hosts, routers, and services, and provide a reliable, connection-oriented, byte-stream service by Transmission Control Protocol (TCP) (Lu & Yang, 2012).

Moreover, it was queuing disciplines to order of the transmission of the packets and dropping over the entire CII networks as well as delivering quality of service (QoS) by reserving resources through Resource Reservation Protocol (RSVP) in addition to operating the firewalls for networking security and virtual private networks (VPN). Each server is customized by the package of the mechanisms and protocols specialized in the four technology solutions individually (Sethi & Hnatyshin, 2012).

The second instrument is GNS3. It is a free and open-source network emulator created and initially released in 2008 under the GNU GPL license. GNS3 allows the combination of virtual and real network deployments, used worldwide to emulate, configure, virtualize, test, and troubleshoot the broad range of networks from small and regular topologies with few nodes to complex and large-scale ones that have many devices hosted on multiple servers (Neumann, 2015).

The GNS3 version 2.2.3 was released in January 2019. GUI all-in-one software compatible with Microsoft Windows operating system was used to collect data in this research alongside integrating the virtualization extensions supported by local Microsoft Hyper-V version 2.2.12 and remote GNS3 VM virtual machine (Castillo et al., 2019).

As illustrated in Figure 4.8, the GNS3 software package run over the architecture of five typical online servers separately hosted in the global web-hosting provider; all servers have the same technical specifications and configurations as the following:

- Processor : 4 CPUs x 2 Core @ 3.3 GHz.
- Motherboard : Super micro H8DGi.
- Storage : 500 GB (Mirrored RAID 1).
- Memory : 16 GB RAM.
- Bandwidth : 15 TB.
- Network : 10GbE × 5 with 5 IP Addresses (Traffic Metered).
- Operating System : Microsoft Windows Server 2019 (64 bit).
- SCSI Controller : Microsoft Hyper-V & GNS3 VM.

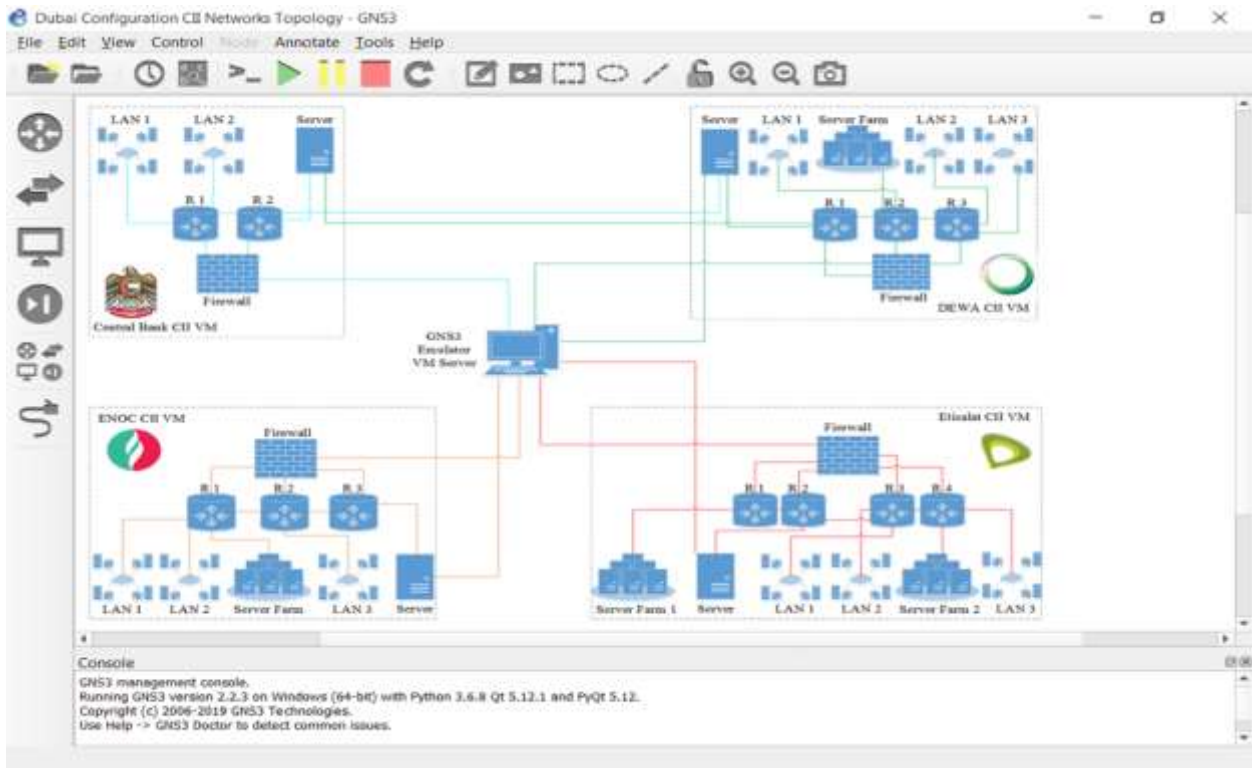


Figure 4.8: GNS3 Emulator Setup Settings and Configurations

Four servers are dedicated to configuring one virtual CII network parallel with other virtual CII networks. The fifth server operates the GNS3 mimics to emulate the devices' hardware and as actual images on the virtual machine to connect the other four servers to each other virtually. Thus, the virtual networked servers for each testing CII network are configured physically within the real server and emulated across a virtual GNS3 server (Welsh, 2013).

The virtual servers are divided into three configurations. The first configuration involves using

heterogeneous virtual machines running the same operating system and different implementations of the same specifications for network protocols that provide cyber resilience against cyber-attacks, as not all implementations are affected by the same vulnerability (Emiliano & Antunes, 2015).

The second configuration used shared two or more redundant servers but did not include common to all network protocols that provide cyber resilience on physical machines against failures (Neumann, 2015). Lastly, the third configuration involves a physical disaster recovery server consisting of two or more virtual servers for redundant fault-tolerant that provide cyber resilience on the mirrored virtual servers against applications (Emiliano & Antunes, 2015).

The virtual servers maintain their services by combining two different CII network specifications and two different implementations of the same network protocols (Welsh, 2013). Therefore, not all implementations are affected by the same vulnerability, except for vulnerabilities in specifications, and two different vulnerabilities have not been found in two different implementations simultaneously (Sharif & Sadeghi-Niaraki, 2017).

The third instrument is the MAXIMA. It is a free mathematical computing platform derived from the DOE Macsyma system developed at MIT Institute between 1968-1982 and written in the Common Lisp programming language. The source code of this computer software was released in 1998 under the GNU GPL terms to run on all popular operating systems. Since 2000, it has been maintained by the Source Forge enterprise.

The MAXIMA version 5.43.0, with stable graphical capabilities released in May 2019 compatible with Microsoft Windows operating system, was used to analyze this research data. A full-featured general-purpose computer algebraic system specializes in symbolic operations entirely and accesses programmatically. In addition, MAXIMA offers numerical capacities such as arbitrary-precision arithmetic integers and rational numbers and floating-point numbers and arrays heavily (Maxima, 2019).

For numeric calculations, using the possibility of generating code in the extended programming language might execute more efficiently with special-case calculations to factorize large numbers and manipulate extremely large polynomials. Screenshot of the wxMaxima is a graphical front-end using wxWidgets Gnuplot drawing for various graphical user interfaces (GUIs), is implemented in Python (Karjanto & Husain, 2017).

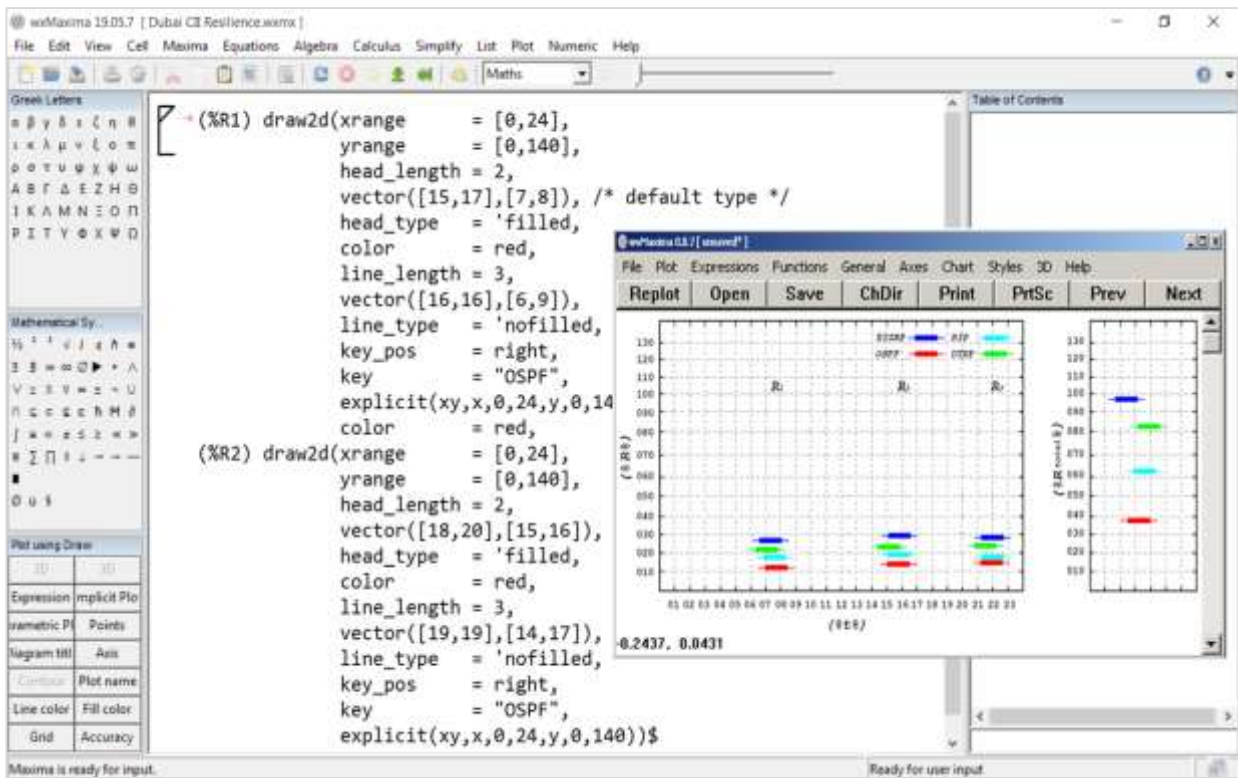


Figure 4.9: MAXIMA Platform Setup Settings and Configurations

As illustrated in Figure 4.9, the MAXIMA software package run over the architecture of one typical online server hosted in a global web-hosting provider; the server has the technical specifications and configurations as the following:

- Processor : 4 CPUs x 2 Core @ 3.3 GHz.
- Motherboard : Super micro H8DGi.
- Storage : 500 GB (Mirrored RAID 1).
- Memory : 16 GB RAM.

- Bandwidth : 15 TB.
- Network : 10GbE × 5 with 5 IP Addresses (Traffic Metered).
- Operating System : Microsoft Windows Server 2019 (64 bit).

The mathematical editor, along with MAXIMA, provides an interactive GUI interface for entering the coding of the Tran (2015) mathematical model to calculate the cyber resilience metrics, whether for the single dynamic cyber resilience or total dynamic cyber resilience of the tested CII networks under different scenarios using the proposed solution and standard solutions (Villate, 2014).

During the primary and optimized phases in this research, the collected data through the quantitative instruments of the OPNET simulator and GNS3 emulator was analyzed mathematically with the MAXIMA platform to obtain the concluding results of the dynamic cyber resilience metrics for each technology solution (Karjanto & Husain, 2017).

The separate Gnuplot console program in MAXIMA Graphics automatically produces these graphical charts in screen resolution. Final measurements were performed in 2d-plots when calling the standard plotting routines to display the popping up containing the output PNG graphics (Maxima, 2019).

## **Appendix E: Primary Proposed Solution**

The primary phase focuses on developing a primary conceptual framework theoretically and a primary technology stack empirically based on cyber zero-trust engineering (Mbanaso et al., 2019). Besides, prototyping the novel proposed solution enhances dynamic cyber resilience capabilities for interdependent CIIs to continuously deliver their missions and core services against concurrent and consecutive cyberattacks within acceptable timelines and performance levels (Schaub et al., 2016).

### ***Primary Conceptual Framework***

The primary conceptual framework is applied to understand the overall picture of the deductive research problem and investigate the multimethod quantitative study (Lazari, 2014). It organizes theoretical ideas as proposed concepts and shows the scientific relationships (Spirin et al., 2020). Moreover, clarifying how these concepts relate to the empirical findings obtained from the literature review also makes conceptual distinctions to standard solutions (Wang et al., 2019).

Furthermore, guiding the technical requirements of the proposed solution development and designing the instrumental context that crosses both primary data collection and analytical methods (Haque et al., 2018). With no going back, it directs the questions associated with their hypotheses and abstracts finally the representations connected to achieve this research purpose (Linkov & Kott, 2019).

The primary conceptual framework of the proposed solution initially identified four primary fundamental concepts that lined up with the research goal. These concepts include decentralized registry, delegated peers, consensus rules, and dynamic routing.

Each fundamental concept employed specific technology in the primary technology stack implemented in the proposed solution, as shown in Figure 3.3. Therefore, this section discusses the primary fundamental concepts and algorithms, while the primary technology stack and protocols are deliberated in section 3.2.2.



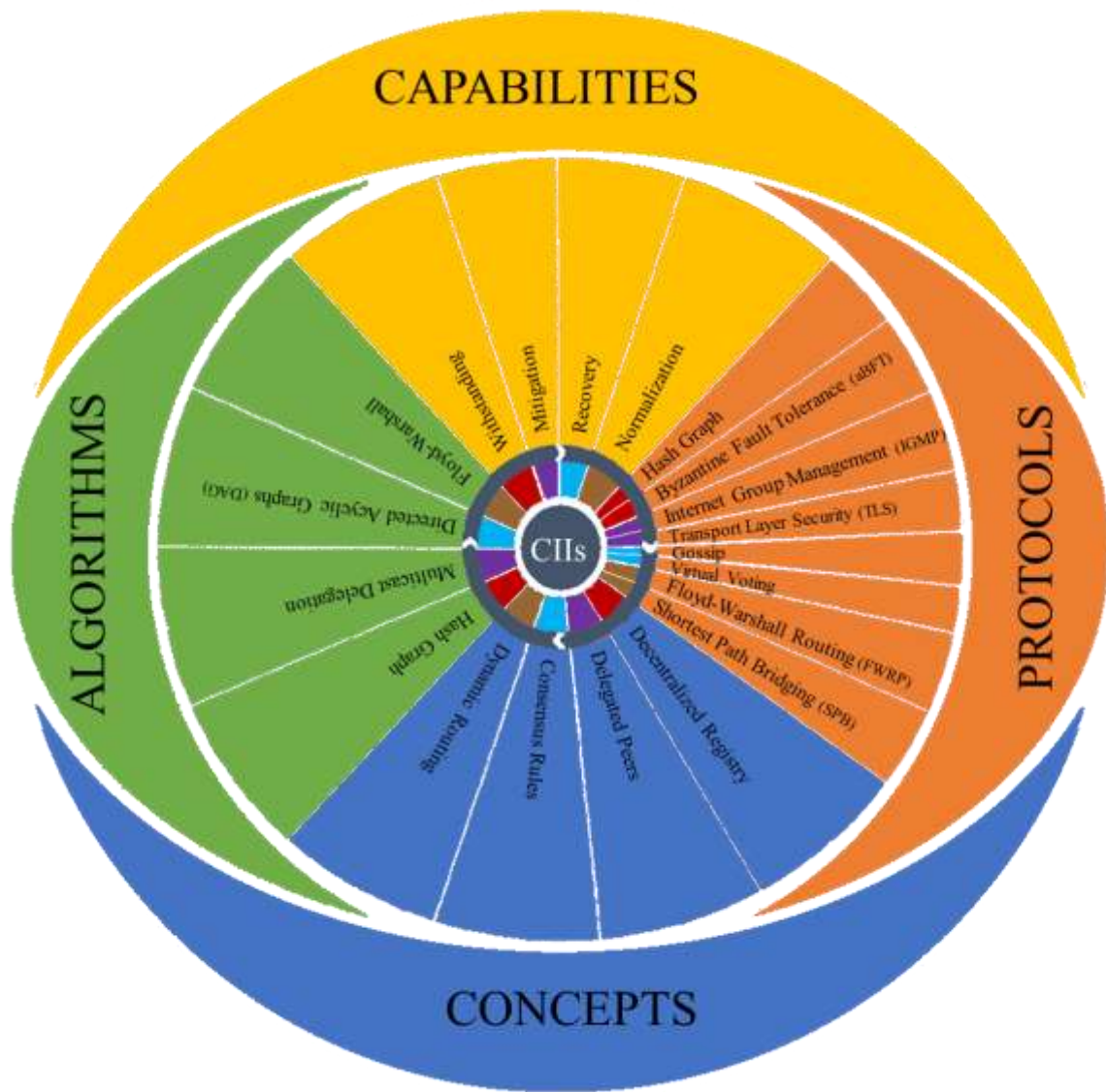


Figure 3.3: Primary Conceptual Framework of Proposed Solution

***Development of Evolutionary Prototyping Model***

The evolutionary prototyping model helps develop the proposed solution in this research by understanding the novel ideas, building the new technologies, checking the additional functionalities, and saving time and costs (Bimonte et al., 2017).

The prototype development is an initial process that uses the Software Development Life Cycle (SDLC) to create and validate the technological production-suite of the conceptual framework, can



be tested in the primary phase with experimental evaluation and addressed the crucial changes and improved later on thru the optimization phase (Bhuvaneswari & Prabakaran, 2013).

The SDLC developmental process involved several essential steps from early identifying core requirements, gathering technical specifications, compiling the algorithms and protocols coded by Microsoft Visual Studio C++ editor version 2019, and structured with the Object-Oriented concepts Programming (OOP) (Pitt-Francis & Whiteley, 2017).

In addition, monolithic fashioned framework and library are organizing protocols suite based on modern Morpheus 2010 network protocol software. It orchestrated all algorithms and protocols of the proposed solution in the same technology stack and layered them on top of one another with complete integration (Voros et al., 2013).

Moreover, preliminary designing assembly and setting up required instrumentation, dealing with trials, and errors, figuring out the iterations and refining the prototype incrementally according to them until the high-fi prototype model is accepted (Madni et al., 2019). Lastly, releasing the functional scaled-down version of the proposed solution, undergoing routine upkeep to prevent breakdowns and minimize downtime during implementation (Salve et al., 2018).

The technology stack of the prototype is a set of four modules organized on top of each other; each module is a combination of one algorithm and a group of associated protocols used cyber zero-trust engineering in line with the related fundamental concepts of the primary conceptual framework, as shown in Figure 3.4.

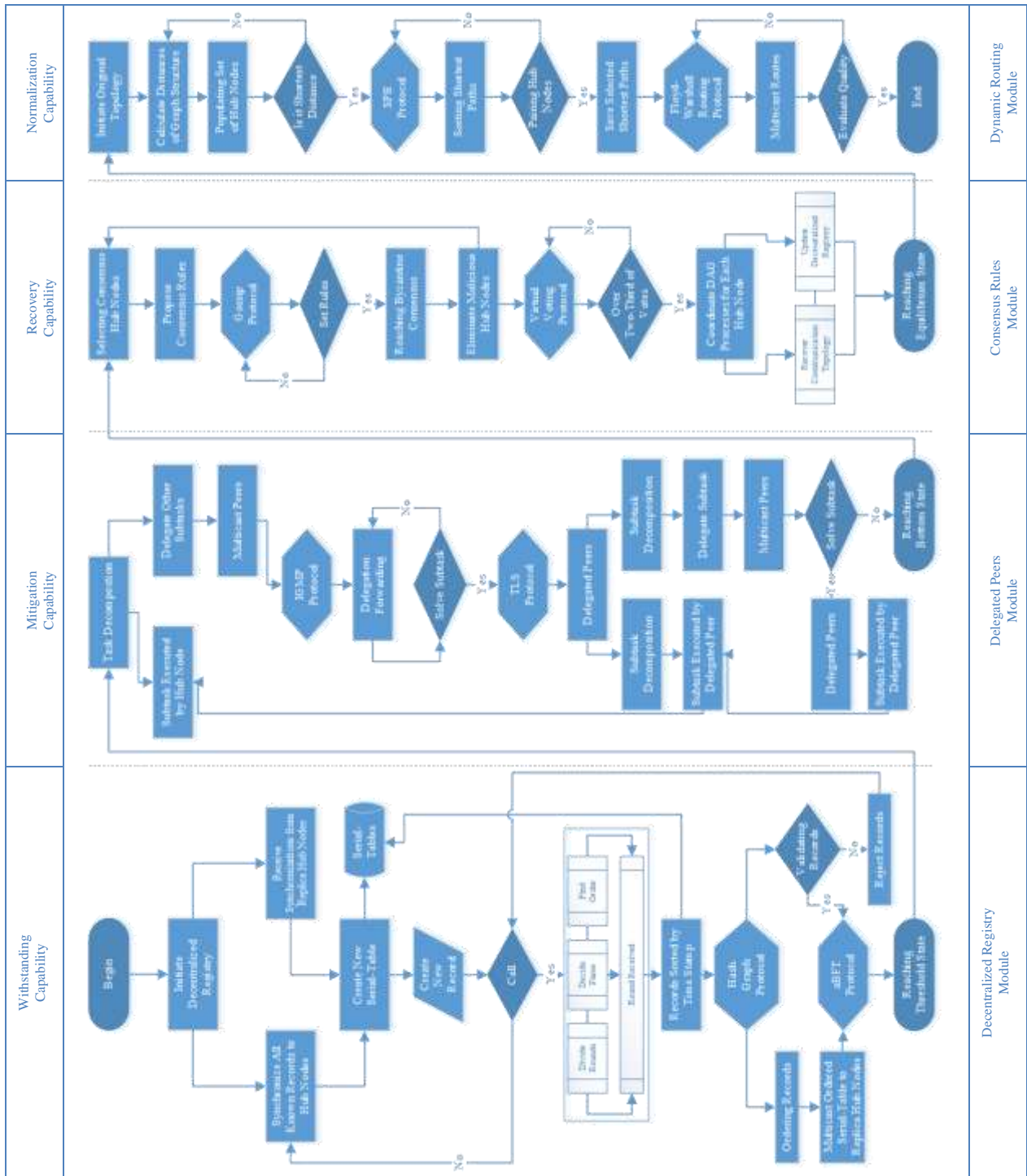


Figure 3.4: Flowchart Diagram of Technology stack for Primary Proposed Solution

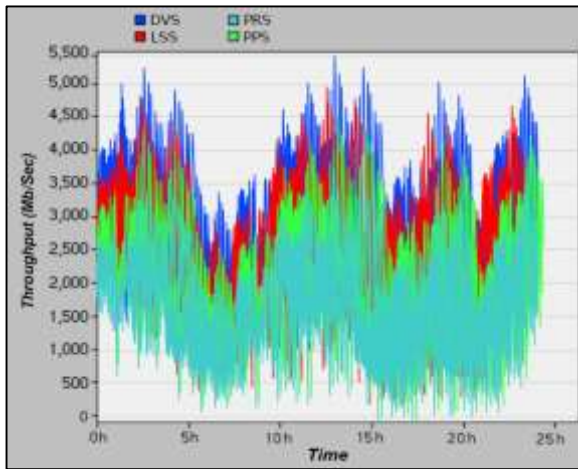
## **Appendix F: Primary Results Analysis and Discussion**

This section incorporates three subsections; the first two subsections display the collected outputs of computing simulations using OPNET and emulated experiments using GNS3; moreover, the third subsection presents the primary results' analysis by analytical modeling using MAXIMA.

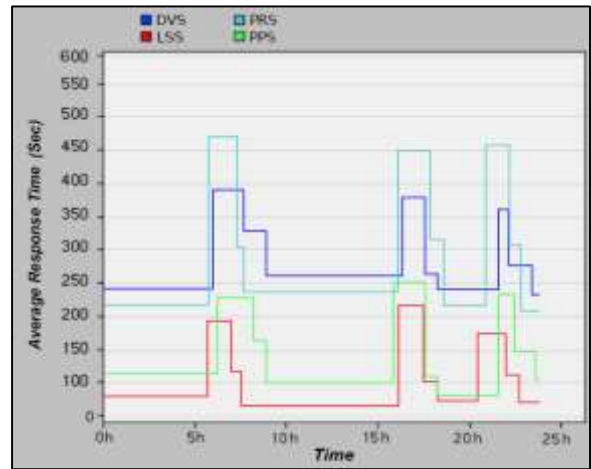
### ***Primary Results Analysis of Computing Simulations***

The computing simulations were conducted throughout three repeated scenarios. These scenarios include core-core scenario, core-edge scenario, and edge-edge scenario. Besides, five networking metrics consist of throughput, average response time, network traffic dropped, average delay variation, and average convergence duration.

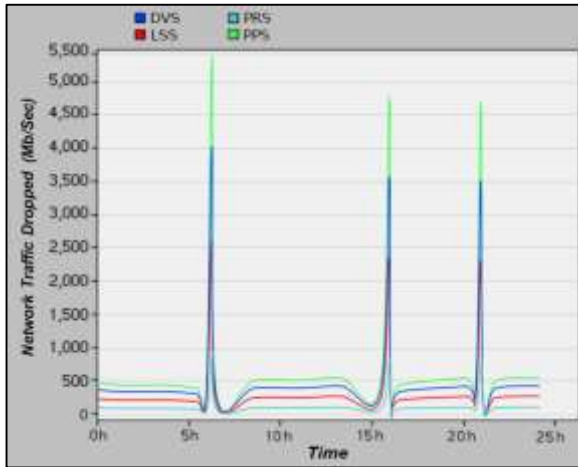
In essence, these metrics are used to measure the definable computations of dynamic cyber resilience capabilities of the primary proposed solution (PPS), and the standard solutions involve distance-vector solution (DVS), link-state solution (LSS), and path-rule solution (PRS). Further analysis augmented results regarding sources and consequences of failure events on timelines.



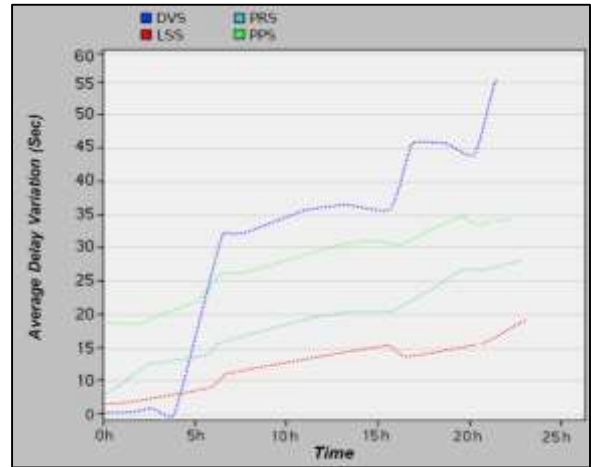
(a)



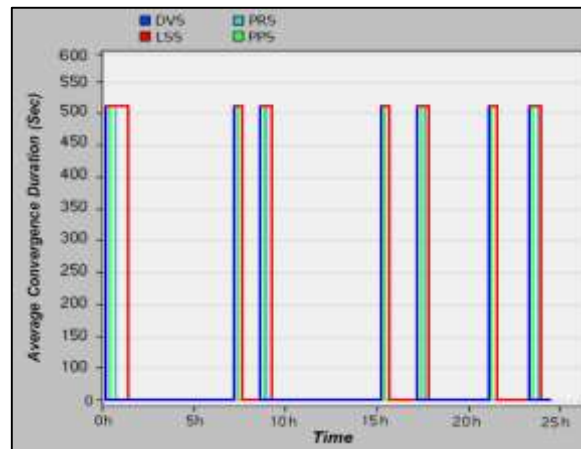
(b)



(c)



(d)



(e)

Figure 5.1: Primary Results of OPNET Simulation for the Core-Core Scenario

(a) Throughput (b) Average Response Time (c) Network Traffic Dropped

(d) Average Delay Variation (e) Average Convergence Duration

Table 5.1: Primary Results of OPNET Simulation for the Core-Core Scenario

Networking Metrics	OPNET Simulation			Dynamic Cyber Resilience Solutions			
	Event	Time (min)		PPS	PRS	LSS	DVS
Throughput (Mb/Sec)	No Cyber Attack						
	No Failure	$t_0$	0421	2646	2151	3233	3698
	First Cyber Attack						
	First Failure	$t_1$	0422	1466	1102	1892	2232
	First Recovery	$t_2$	0496	2641	2129	3225	3681
	Second Cyber Attack						
	Second Failure	$t_3$	0936	1771	1272	2357	2711
	Second Recovery	$t_4$	1025	2597	2140	3231	3692
	Third Cyber Attack						
	Third Failure	$t_5$	1284	1607	1313	2649	2808
Third Recovery	$t_6$	1398	2644	2150	3232	3691	
Average Response Time (Sec)	No Cyber Attack						
	No Failure	$t_0$	0422	0116	0226	0072	0244
	First Cyber Attack						
	First Failure	$t_1$	0423	0233	0471	0196	0391
	First Recovery	$t_2$	0498	0162	0303	0116	0326
	Second Cyber Attack						
	Second Failure	$t_3$	0941	0258	0450	0218	0375
	Second Recovery	$t_4$	1020	0104	0311	0100	0261
	Third Cyber Attack						
	Third Failure	$t_5$	1283	0238	0462	0173	0360
Third Recovery	$t_6$	1391	0150	0306	0114	0277	
Network Traffic Dropped (Mb/Sec)	No Cyber Attack						
	No Failure	$t_0$	0426	0498	0158	0253	0412
	First Cyber Attack						
	First Failure	$t_1$	0427	5492	0986	2576	4013
	First Recovery	$t_2$	0489	0495	0156	0257	0411
	Second Cyber Attack						
	Second Failure	$t_3$	0940	4827	0795	2339	3507
	Second Recovery	$t_4$	1026	0495	0160	0251	0416
	Third Cyber Attack						
	Third Failure	$t_5$	1287	4788	0780	2304	3500
Third Recovery	$t_6$	1399	0499	0153	0254	0414	
Average Delay Variation (Sec)	No Cyber Attack						
	No Failure	$t_0$	0424	0018	0006	0004	0002
	First Cyber Attack						
	First Failure	$t_1$	0425	0030	0014	0011	0037
	First Recovery	$t_2$	0497	0026	0013	0008	0032
	Second Cyber Attack						
	Second Failure	$t_3$	0938	0035	0021	0014	0046
	Second Recovery	$t_4$	1022	0029	0020	0013	0036
	Third Cyber Attack						
	Third Failure	$t_5$	1286	0035	0028	0019	0055
Third Recovery	$t_6$	1401	0034	0027	0016	0044	
Average Convergence Duration (Sec)	No Cyber Attack						
	No Failure	$t_0$	0430	0328	0386	0430	0301
	First Cyber Attack						
	First Failure	$t_1$	0431	0462	0434	0488	0454
	First Recovery	$t_2$	0503	0354	0390	0441	0340
	Second Cyber Attack						
	Second Failure	$t_3$	0944	0449	0428	0492	0475
	Second Recovery	$t_4$	1023	0360	0386	0438	0362
	Third Cyber Attack						
	Third Failure	$t_5$	1287	0431	0438	0479	0471
Third Recovery	$t_6$	1399	0333	0382	0433	0319	

In Table 5.1, at simulation time  $t_0$  421 min, the throughput of DVS with no failure event was the highest level by 3698 Mb/sec compared to the rest of the solutions, LSS by 3233 Mb/sec, PPS by 2646 Mb/sec, and PRS by 2151 Mb/sec. Also, DVS keeps the same highest throughput trend despite three failure events at 422 min, 936 min, 1284 min with 2232 Mb/sec, 2711 Mb/sec, and 2808 Mb/sec, accordingly. That means the PPS has a lower performance level next to PRS, but the DVS has the highest one, as shown in Figure 5.1 (a).

In contrast, LSS has the lowest response time over three recovery events, followed by PPS, DVS, and PRS. The average response time of LSS was 116 sec, 100 sec, 114 sec at the simulation time  $t_2$  498 min,  $t_4$  1020 min, and  $t_6$  1391 min compared to the average response time of PPS was 162 sec, 104 sec, and 150 sec, respectively. These outputs indicate that the PPS is the second higher after LSS in the recovery factor along the irregular hexagon lines illustrated in Figure 5.1 (b).

On the other hand, all PRS measurements of the network traffic dropped metric via concurrent and consecutive cyberattacks were the lowest, followed by the LSS and DVS solutions. The PSS came last by 5492 Mb/sec at  $t_1$  427 min, 4827 Mb/sec at  $t_3$  940 min, and 4788 Mb/sec at  $t_5$  1287 min. These results were clear in Figure 5.1 (c) that showed the peak light-green curve of the PPS solution, which means it has the highest amount of network traffic packets dropped through three failure events.

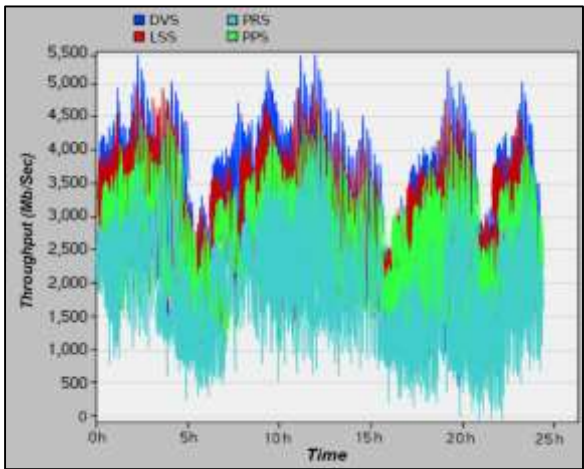
Similarly, the PPS results were placed before the final solution of dynamic cyber resilience in the average delay variation metric even with its no failure event was 18 sec at  $t_0$  424 min. The PPS has a higher average delay on the first recovery event with 26 sec at  $t_2$  497 min, 29 sec at  $t_4$  1022 min, and 34 sec at  $t_6$  1401 min on both second and third recovery events. However, the LSS solution has the lowest average delay variation, with 8 sec, 13 sec, and 16 sec in the same events above that plotted in Figure 5.1 (d).

Table 5.2: Solutions Ranking of Primary Simulation Results for the Core-Core Scenario

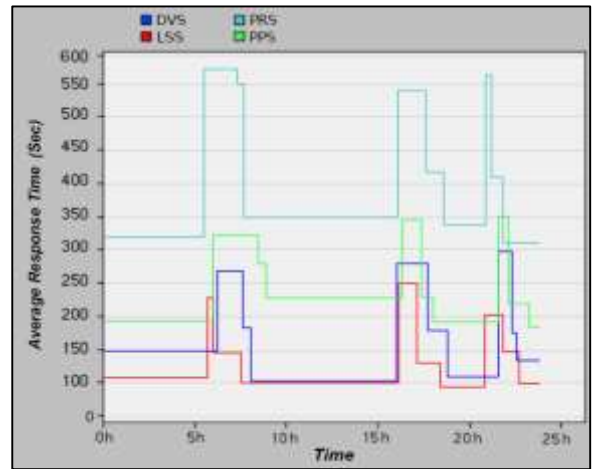
<i>Standard Simulation Networking Metrics</i>	<i>Dynamic Cyber Resilience Factors</i>	<i>Ranking of Dynamic Cyber Resilience Solutions</i>			
		<i>PPS</i>	<i>PRS</i>	<i>LSS</i>	<i>DVS</i>
<i>Throughput</i>	<i>Performance</i>	3	4	2	1
<i>Average Response Time</i>	<i>Recovery</i>	2	4	1	3
<i>Network Traffic Dropped</i>	<i>Absorption</i>	4	1	2	3
<i>Average Delay Variation</i>	<i>Volatility</i>	3	2	1	4
<i>Average Convergence Duration</i>	<i>Recovery Time</i>	2	3	4	1

Nevertheless, the average convergence duration results showed that the DVS and the PPS are the highest solutions corresponding to the PRS and LSS solutions. The PPS attained the appropriate convergence durations during three recovery events near the starting point before the wave of failures. At  $t_2$  503 min in the first recovery event, its average convergence duration was 354 sec and 360 sec in the second recovery event at  $t_4$  1023 min, while the convergence duration of the third recovery event at  $t_6$  1399 min was 333 sec, the closest one to the convergence duration of the initial event with no failure at 328 sec in the time  $t_0$  430 min. Figure 5.1 (e) introduces a shred of evidence that the DVS with the blue lines and PPS with light-green lines have the top average convergence durations compared to their results in average delay variation evaluated to the LSS PRS solutions. As a reminder, each standard simulation networking metric used in the testing scenarios considers a particular measure to assess one of the dynamic cyber resilience factors, in turn, evaluate associated dynamic cyber resilience capabilities. The conclusion of the primary simulation results above reflected the ranking of dynamic cyber resilience solutions over the core-core scenario.

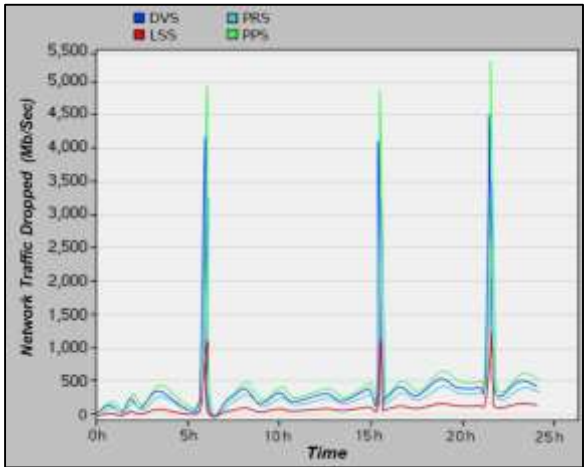
As revealed in Table 5.2, the PPS solution results were not achieved the first rank in any dynamic cyber resilience factor; however, the PPS ranked second in recovery and recovery time factors. The third grade in performance and volatility factors and the last position for the absorption factor. The LSS and the DVS solutions were achieved the best rankings than others.



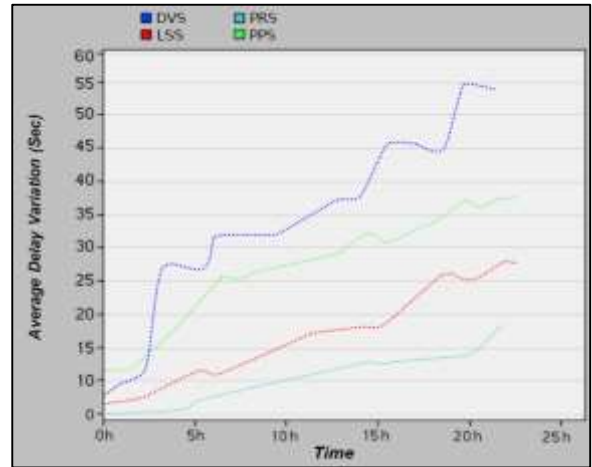
(a)



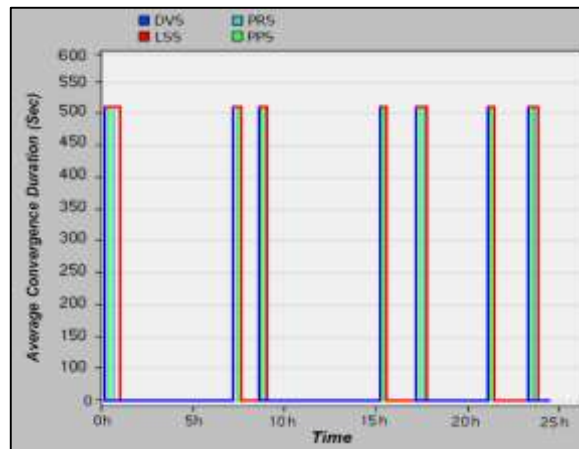
(b)



(c)



(d)



(e)

Figure 5.2: Primary Results of OPNET Simulation for the Core-Edge Scenario  
 (a) Throughput (b) Average Response Time (c) Network Traffic Dropped  
 (d) Average Delay Variation (e) Average Convergence Duration



Table 5.3: Primary Results of OPNET Simulation for the Core-Edge Scenario

Networking Metrics	OPNET Simulation			Dynamic Cyber Resilience Solutions			
	Event	Time (min)		PPS	PRS	LSS	DVS
Throughput (Mb/Sec)	No Cyber Attack						
	No Failure	$t_0$	0422	3225	2335	3701	4121
	First Cyber Attack						
	First Failure	$t_1$	0423	1678	1275	2583	2590
	First Recovery	$t_2$	0494	2896	2504	3554	3718
	Second Cyber Attack						
	Second Failure	$t_3$	0939	2004	1190	2225	2449
	Second Recovery	$t_4$	1028	2951	2318	3480	3663
	Third Cyber Attack						
	Third Failure	$t_5$	1288	2181	1821	2872	2716
Third Recovery	$t_6$	1393	3183	2328	3686	4028	
Average Response Time (Sec)	No Cyber Attack						
	No Failure	$t_0$	0424	0195	0322	0105	0149
	First Cyber Attack						
	First Failure	$t_1$	0425	0322	0577	0227	0265
	First Recovery	$t_2$	0495	0271	0550	0148	0187
	Second Cyber Attack						
	Second Failure	$t_3$	0943	0348	0542	0250	0274
	Second Recovery	$t_4$	1023	0232	0428	0138	0171
	Third Cyber Attack						
	Third Failure	$t_5$	1284	0350	0565	0200	0293
Third Recovery	$t_6$	1393	0229	0426	0150	0182	
Network Traffic Dropped (Mb/Sec)	No Cyber Attack						
	No Failure	$t_0$	0425	0111	0125	0088	0143
	First Cyber Attack						
	First Failure	$t_1$	0426	4991	3281	1117	4121
	First Recovery	$t_2$	0485	0491	0225	0053	0370
	Second Cyber Attack						
	Second Failure	$t_3$	0941	4902	3105	1231	4030
	Second Recovery	$t_4$	1023	0508	0310	0066	0448
	Third Cyber Attack						
	Third Failure	$t_5$	1286	5454	3502	1295	4502
Third Recovery	$t_6$	1402	0530	0312	0108	0461	
Average Delay Variation (Sec)	No Cyber Attack						
	No Failure	$t_0$	0428	0012	0002	0005	0008
	First Cyber Attack						
	First Failure	$t_1$	0429	0026	0008	0017	0027
	First Recovery	$t_2$	0493	0025	0004	0012	0026
	Second Cyber Attack						
	Second Failure	$t_3$	0934	0032	0014	0026	0037
	Second Recovery	$t_4$	1026	0030	0012	0016	0036
	Third Cyber Attack						
	Third Failure	$t_5$	1289	0037	0018	0028	0046
Third Recovery	$t_6$	1396	0036	0013	0025	0044	
Average Convergence Duration (Sec)	No Cyber Attack						
	No Failure	$t_0$	0429	0316	0374	0428	0310
	First Cyber Attack						
	First Failure	$t_1$	0430	0445	0425	0483	0449
	First Recovery	$t_2$	0500	0351	0388	0436	0343
	Second Cyber Attack						
	Second Failure	$t_3$	0942	0432	0417	0488	0471
	Second Recovery	$t_4$	1021	0348	0373	0432	0360
	Third Cyber Attack						
	Third Failure	$t_5$	1285	0427	0422	0472	0467
Third Recovery	$t_6$	1395	0329	0369	0432	0309	

The primary results of the four competing solutions during the OPNET simulations in the core-edge scenario were demonstrated entirely in Figure 5.2 and Table 5.3. Consequently, throughput results of the DVS and the LSS solution were the highest ones, followed by the PPS solution by 1678 Mb/sec in the first failure event at  $t_1$  423 min, 2004 Mb/sec in the second failure event at  $t_3$  939 min, and 2181 Mb/sec in the third failure event at  $t_5$  1288 min. The light-green zigzag curve in Figure 5.2 (a) depicted the measured performance factor of the PPS along with other solutions.

Moreover, the LSS solution has the highest results in the standard metrics of average response time, and network traffic dropped, while the results of the PPS solution were modest in both metrics.

In Figure 5.2 (b), the illustrated LSS red irregular hexagon line was reached 148 sec as a response time in the first recovery event at  $t_2$  495 min, at the same time as the PPS solution touched 271 sec. Likewise, for the next two recovery events, the LSS solution gets hold of 138 sec and 150 sec at  $t_4$  1023 min and  $t_6$  1393 min respectively in opposite the PPS solution was moved between 232 sec and 229 sec for both recovery events above.

Furthermore, the LSS solution dropped the lowest network traffic packets in three failure events counter to the PPS solution and dropped the highest network traffic than other solutions. For example, the red curve of the LSS solution in Figure 5.2 (c) was dropped by 1117 Mb/sec in the first failure event at  $t_1$  426 min, but then again, the PPS solution was dropped by 4991 Mb/sec in the same circumstances.

Similarly, in the second and third failure events at  $t_3$  941 min and  $t_5$  1286 min, the LSS solution was dropped by 1231 Mb/sec and by 1295 Mb/sec of the network traffic, on the contrary of the PPS solution that dropped the number of packets stretched to 4902 Mb/sec and 5454 Mb/sec.

As per the light-green plots in Figure 5.2 (d), the situation of the PPS solution was slightly different regarding its measurements of the average delay variation compared to others, where it was carried out 26 sec at  $t_1$  429 min, 32 sec at  $t_3$  934 min, 37 sec at  $t_5$  1289 min across the first, second and third

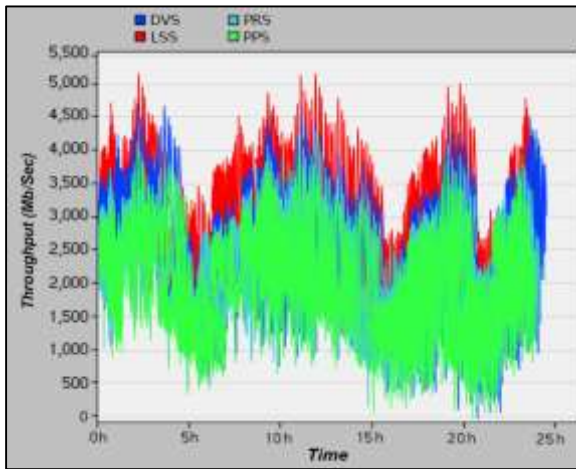
failure events consistently. Thus, the PRS solution has the lowest delay variation, and the DVS has the highest delay than other solutions.

Table 5.4: Solutions Ranking of Primary Simulation Results for the Core-Edge Scenario

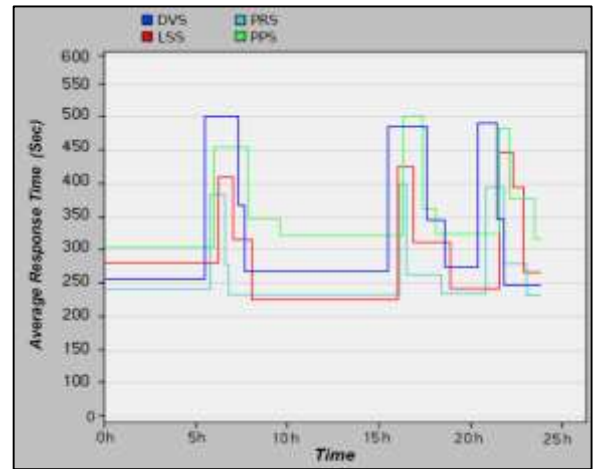
<i>Standard Simulation Networking Metrics</i>	<i>Dynamic Cyber Resilience Factors</i>	<i>Ranking of Dynamic Cyber Resilience Solutions</i>			
		<i>PPS</i>	<i>PRS</i>	<i>LSS</i>	<i>DVS</i>
<i>Throughput</i>	<i>Performance</i>	3	4	2	1
<i>Average Response Time</i>	<i>Recovery</i>	3	4	1	2
<i>Network Traffic Dropped</i>	<i>Absorption</i>	4	2	1	3
<i>Average Delay Variation</i>	<i>Volatility</i>	3	1	2	4
<i>Average Convergence Duration</i>	<i>Recovery Time</i>	2	3	4	1

The results of the PPS solution improved dramatically in the average convergence duration metric starting from 316 sec at  $t_0$  429 min with no cyberattack occurred to become 351 sec at  $t_2$  500 min over the first recovery event, 348 sec at  $t_4$  1021 min after the second one, and lastly 329 sec at  $t_6$  1395 min. Figure 5.2 (e) shows that only the DVS solution results were higher than the PPS solution results in this metric.

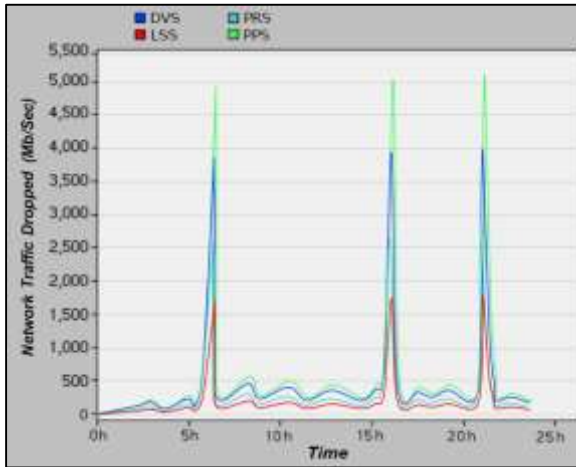
The obtainable rankings from Table 5.4 presented that the LSS solution also has the best overall ranks in the primary simulation results for the core-edge scenario followed by the DVS solution. These concluded results were comparable to their previous results in the core-core scenario above. At variance of the PRS solution, its orders in the core-core scenario were better than the core-edge scenario. On the PPS solution rankings, the best one was the second status in the recovery time factor, the third class in three factors of performance, recovery, and volatility, while it was graded fourth in the absorption factor like in the previous core-core scenario. In general, most of the PPS solution ranks in the core-core scenario were better than its sorts in the core-edge scenario, as detailed in Table 5.3 and Table 5.4.



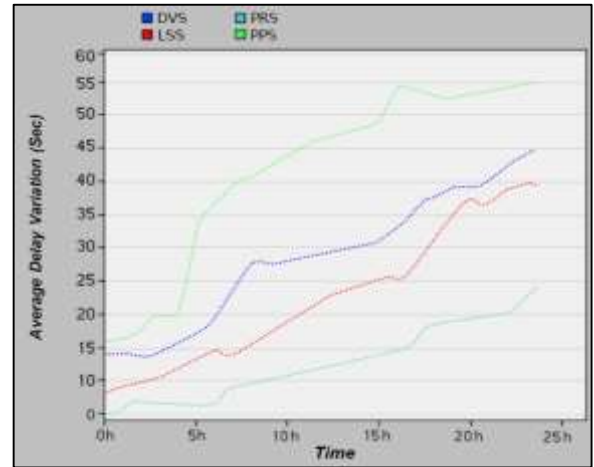
(a)



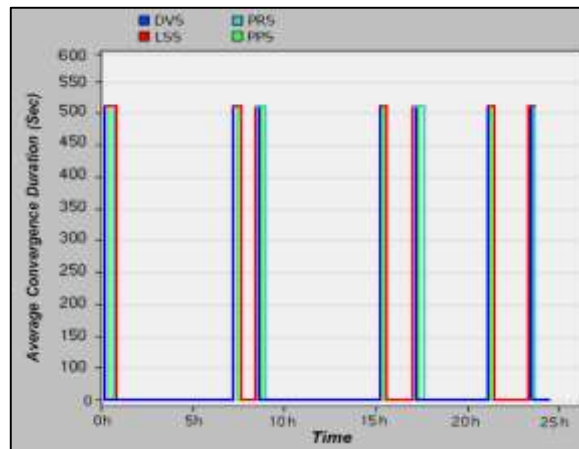
(b)



(c)



(d)



(e)

Figure 5.3: Primary Results of OPNET Simulation for the Edge-Edge Scenario

(a) Throughput (b) Average Response Time (c) Network Traffic Dropped

(d) Average Delay Variation (e) Average Convergence Duration

Table 5.5: Primary Results of OPNET Simulation for the Edge-Edge Scenario

Networking Metrics	OPNET Simulation			Dynamic Cyber Resilience Solutions			
	Event	Time (min)		PPS	PRS	LSS	DVS
Throughput (Mb/Sec)	No Cyber Attack						
	No Failure	$t_0$	0423	2338	2515	3766	3349
	First Cyber Attack						
	First Failure	$t_1$	0424	1454	1686	2613	1575
	First Recovery	$t_2$	0497	2112	2348	3193	2792
	Second Cyber Attack						
	Second Failure	$t_3$	0934	1235	1466	2253	1480
	Second Recovery	$t_4$	1028	1997	2201	3006	2663
	Third Cyber Attack						
	Third Failure	$t_5$	1289	1150	1373	2332	1673
Third Recovery	$t_6$	1394	2088	2229	3448	3192	
Average Response Time (Sec)	No Cyber Attack						
	No Failure	$t_0$	0423	0304	0243	0282	0255
	First Cyber Attack						
	First Failure	$t_1$	0425	0456	0381	0411	0500
	First Recovery	$t_2$	0493	0350	0280	0317	0373
	Second Cyber Attack						
	Second Failure	$t_3$	0942	0500	0400	0422	0484
	Second Recovery	$t_4$	1019	0366	0255	0309	0348
	Third Cyber Attack						
	Third Failure	$t_5$	1288	0481	0393	0446	0493
Third Recovery	$t_6$	1392	0378	0284	0391	0347	
Network Traffic Dropped (Mb/Sec)	No Cyber Attack						
	No Failure	$t_0$	0427	0211	0145	0116	0181
	First Cyber Attack						
	First Failure	$t_1$	0428	4917	2512	1712	3888
	First Recovery	$t_2$	0488	0413	0240	0186	0376
	Second Cyber Attack						
	Second Failure	$t_3$	0942	5045	2545	1779	3909
	Second Recovery	$t_4$	1023	0407	0232	0176	0353
	Third Cyber Attack						
	Third Failure	$t_5$	1283	5119	2576	1767	4000
Third Recovery	$t_6$	1392	0232	0172	0135	0208	
Average Delay Variation (Sec)	No Cyber Attack						
	No Failure	$t_0$	0423	0016	0005	0007	0014
	First Cyber Attack						
	First Failure	$t_1$	0424	0040	0008	0015	0027
	First Recovery	$t_2$	0493	0035	0006	0014	0025
	Second Cyber Attack						
	Second Failure	$t_3$	0935	0054	0018	0025	0039
	Second Recovery	$t_4$	1021	0048	0015	0023	0036
	Third Cyber Attack						
	Third Failure	$t_5$	1283	0055	0024	0037	0043
Third Recovery	$t_6$	1397	0053	0020	0036	0040	
Average Convergence Duration (Sec)	No Cyber Attack						
	No Failure	$t_0$	0428	0297	0308	0341	0289
	First Cyber Attack						
	First Failure	$t_1$	0429	0332	0368	0398	0314
	First Recovery	$t_2$	0499	0356	0377	0326	0333
	Second Cyber Attack						
	Second Failure	$t_3$	0940	0341	0399	0369	0326
	Second Recovery	$t_4$	1021	0337	0352	0313	0322
	Third Cyber Attack						
	Third Failure	$t_5$	1282	0349	0384	0355	0341
Third Recovery	$t_6$	1396	0338	0356	0327	0332	

A continuation of the analysis of the primary simulation results for the dynamic cyber resilience solutions through the edge-edge scenario, Table 5.5, is established that the optimal results in this scenario were achieved by two solutions only, the LSS and the PRS solutions. The LSS has the optimal results in three standard networking metrics lump sum: throughput, network traffic dropped, and average convergence duration. Correspondingly, the PRS solution has the best metrics in the other two metrics, which comprise average response time and average delay variation.

In contrast, the PPS solution during this scenario did not succeed in delivering competitive results in overall standard networking metrics competed with the LSS and the PRS solutions. In detail, the LSS ascertained an increase of one-third in the primary results of the throughput metric rather than PSS across both failure and recovery events; LSS has throughput results by 2613 Mb/sec, 2253 Mb/sec, and 2332 Mb/sec at  $t_1$  424 min,  $t_3$  934 min, and  $t_5$  1289 min respectively in differing of PPS throughput results were by 1454 Mb/sec, 1235 Mb/sec, and 1150 Mb/sec with the same time frames for the period of three failure events, as displayed in Figure 5.3 (a).

Alike in Figure 5.3 (c), the light-green peaks of the PPS solution were dropped nearly three times of network traffic more than the red peaks of the LSS solution thru the cyberattacks events at  $t_1$  428 min,  $t_3$  942 min, and  $t_5$  1283 min. The rate of the packets number dropped through these failure events was 1712 Mb/sec, 1779 Mb/sec, and 1767 Mb/sec for the LSS, while in the case of the PSS, this rate was increased highly to reach 4917 Mb/sec, 5045 Mb/sec, and 5119 Mb/sec.

In order to complete the comparison between these two solutions, the LSS and the PPS. The red straight lines in Figure 5.3 (e) were clarified that the LSS has the highest time results in the average convergence duration metric comparable with all other solutions, including the PSS solution. For example, in three recovery events after the cyberattacks, the LSS was achieved 326 sec in the first recovery event at  $t_2$  499 min, 313 sec in the second recovery event at  $t_4$  1021 min, and 327 sec in the third recovery event at  $t_6$  1396 min. However, the PPS solution was realized 356 sec, 337 sec, and

338 sec during the related recovery events.

Table 5.6: Solutions Ranking of Primary Simulation Results for the Edge-Edge Scenario

<i>Standard Simulation Networking Metrics</i>	<i>Dynamic Cyber Resilience Factors</i>	<i>Ranking of Dynamic Cyber Resilience Solutions</i>			
		<i>PPS</i>	<i>PRS</i>	<i>LSS</i>	<i>DVS</i>
<i>Throughput</i>	<i>Performance</i>	4	3	1	2
<i>Average Response Time</i>	<i>Recovery</i>	3	1	2	4
<i>Network Traffic Dropped</i>	<i>Absorption</i>	4	2	1	3
<i>Average Delay Variation</i>	<i>Volatility</i>	4	1	2	3
<i>Average Convergence Duration</i>	<i>Recovery Time</i>	3	4	1	2

On the other hand, the PRS and the PPS comparison are confined to two standard simulation networking metrics: the average response time and the average delay variation. The average response time as illuminated in Figure 5.3 (b), the dark green lines of irregular hexagon shapes of the PRS solution make clear that it has the highest response time competing with other solutions.

The average response times over the recovery events for the PRS were 280 sec, 255 sec, and 284 sec according to the PPS, were 350 sec, 366 sec, and 378 sec upon the recovery time at  $t_2$  493 min,  $t_4$  1019 min, and finally  $t_6$  1392 min. In the same way, giving the dark and light green plots in Figure 5.3 (d) showed that the average delay variation of the PPS solution, but over the failure events this time, was 40 sec after the first cyberattack, then 54 sec in the second one, and 55 sec in the third failure event. The PRS results were the best ones rather than others by 8 sec, 18 sec, and 24 sec through  $t_1$  424 min,  $t_3$  935 min, and  $t_5$  1283 min.

Table 5.6 concluded the rankings of the dynamic cyber resilience solutions on the basis of the primary simulation results across the edge-edge scenario, indicating that the PPS solution has the poorest positioning in this scenario absolutely compared to its grading in the other scenarios as well as to other standard solutions in this scenario especially LSS and PRS solutions.

### ***Primary Results Analysis of Emulated Experiments***

The emulated experiments were performed through three repeated scenarios to validate the collected data and results analyzed by the computing simulations. These testing scenarios were the same that applied in the simulating scenarios comprise core-core scenario, core-edge scenario, and edge-edge scenario.

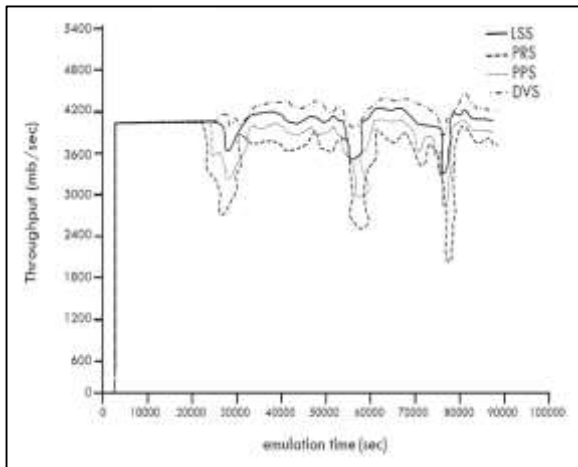
Besides, using a set of emulation networking metrics that lookalike used in the simulation testing to measure and collect the experimental results consisting of five standard metrics discussed in Chapter 4 involve: throughput, average reachable time, network traffic lost, average end-to-end delay, and average convergence duration.

Typically, every standard networking metric used in the testing emulation scenarios covered the specific measurements to assess one factor related to the dynamic cyber resilience for evaluating its associated capability of the primary proposed solution (PPS), and standard solutions include (DVS), (LSS), and (PRS) solutions across several failures and recovery events over time frames.

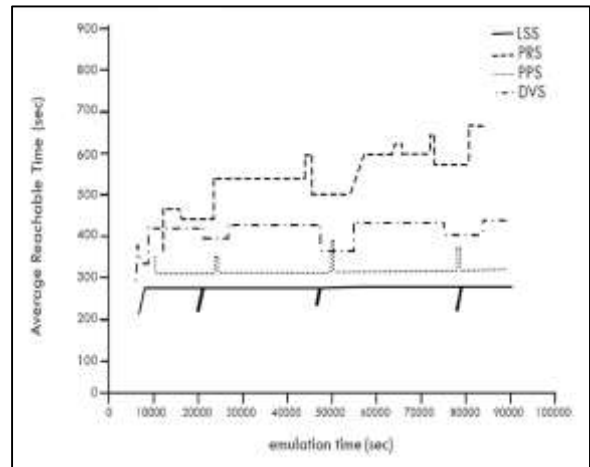
In Table 5.7 below, the primary results emulations for the core-core scenario implemented by the GNS3 platform presented that the throughput results of the PPS solution were 4085 Mb/sec at  $t_0$  426 min by initial event with no failure before the wave of the concurrent and consecutive cyberattacks have been started.

After the first failure event by the first cyberattack, the PPS throughput was 3294 Mb/sec at  $t_1$  427 min; this throughput also decreased in the second failure event by 934 Mb/sec at  $t_3$  934 min to reach lastly by 2830 Mb/sec at  $t_5$  1283 min with the third failure event. Thus, these throughput results of the PPS solution were lower than the best throughput results of the DVS solution over the equivalent events, as illustrated by the diagram chart of the light-dotted and loosely dash-dotted downward curves in Figure 5.4 (a).

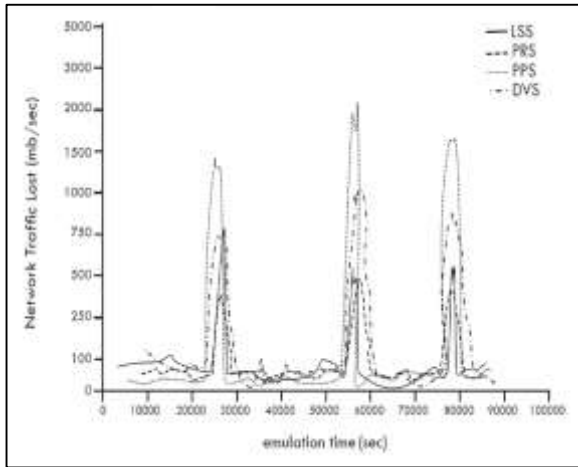




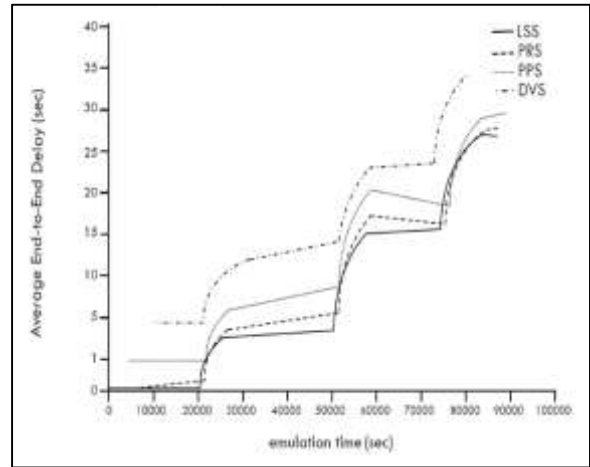
(a)



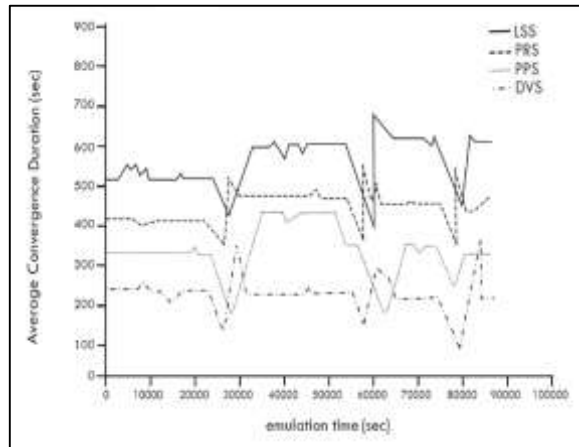
(b)



(c)



(d)



(e)

Figure 5.4: Primary Results of GNS3 Emulation for the Core-Core Scenario

(a) Throughput (b) Average Reachable Time (c) Network Traffic Lost

(d) Average End-to-End Delay (e) Average Convergence Duration

Table 5.7: Primary Results of GNS3 Emulation for the Core-Core Scenario

Networking Metrics	GNS3 Emulation			Dynamic Cyber Resilience Solutions			
	Event	Time (min)		PPS	PRS	LSS	DVS
Throughput (Mb/sec)	No Cyber Attack						
	No Failure	$t_0$	0426	4085	4034	4113	4178
	First Cyber Attack						
	First Failure	$t_1$	0427	3294	2618	3658	4083
	First Recovery	$t_2$	0493	3884	3535	3911	4213
	Second Cyber Attack						
	Second Failure	$t_3$	0934	2993	2383	3534	3915
	Second Recovery	$t_4$	1021	3741	3426	3980	4282
	Third Cyber Attack						
	Third Failure	$t_5$	1283	2830	1946	3306	3976
Third Recovery	$t_6$	1396	3917	3669	4014	4322	
Average Reachable Time (sec)	No Cyber Attack						
	No Failure	$t_0$	0423	0305	0455	0420	0283
	First Cyber Attack						
	First Failure	$t_1$	0424	0285	0433	0391	0223
	First Recovery	$t_2$	0495	0303	0554	0431	0282
	Second Cyber Attack						
	Second Failure	$t_3$	0943	0254	0503	0377	0241
	Second Recovery	$t_4$	1023	0308	0592	0429	0282
	Third Cyber Attack						
	Third Failure	$t_5$	1285	0264	0581	0401	0217
Third Recovery	$t_6$	1393	0306	0692	0431	0223	
Network Traffic Lost (Mb/sec)	No Cyber Attack						
	No Failure	$t_0$	0425	0034	0053	0081	0093
	First Cyber Attack						
	First Failure	$t_1$	0426	1421	0402	0755	0753
	First Recovery	$t_2$	0485	0028	0058	0046	0059
	Second Cyber Attack						
	Second Failure	$t_3$	0939	2012	0453	0503	1033
	Second Recovery	$t_4$	1023	0042	0068	0027	0062
	Third Cyber Attack						
	Third Failure	$t_5$	1284	1758	0412	0556	0856
Third Recovery	$t_6$	1395	0035	0064	0088	0071	
Average End-to-End Delay (sec)	No Cyber Attack						
	No Failure	$t_0$	0422	0003	0002	0001	0004
	First Cyber Attack						
	First Failure	$t_1$	0423	0006	0004	0002	0012
	First Recovery	$t_2$	0498	0003	0002	0001	0004
	Second Cyber Attack						
	Second Failure	$t_3$	0934	0021	0017	0015	0023
	Second Recovery	$t_4$	1024	0008	0006	0003	0014
	Third Cyber Attack						
	Third Failure	$t_5$	1282	0028	0027	0027	0034
Third Recovery	$t_6$	1399	0017	0015	0016	0023	
Average Convergence Duration (sec)	No Cyber Attack						
	No Failure	$t_0$	0429	0335	0423	0521	0241
	First Cyber Attack						
	First Failure	$t_1$	0430	0191	0363	0438	0157
	First Recovery	$t_2$	0499	0447	0525	0617	0345
	Second Cyber Attack						
	Second Failure	$t_3$	0941	0188	0352	0400	0171
	Second Recovery	$t_4$	1020	0376	0543	0654	0282
	Third Cyber Attack						
	Third Failure	$t_5$	1288	0273	0376	0463	0094
Third Recovery	$t_6$	1400	0329	0436	0620	0386	

Moreover, the staircase curves in Figure 5.4 (b) demonstrated the average reachable time results of the PPS solution summarized in three recovery events at  $t_2$  495 min,  $t_4$  1023 min, and  $t_6$  1393 min to become 303 sec, 308 sec, and 306 sec. These results were the second-best ones afterward; the LSS results in the same metric and over the same time frames were 431 sec, 429 sec, and 431 sec, followed by the results of the DVS solution and the PRS solution.

Furthermore, the PPS has the highest loss rate of network traffic compared to other standard solutions. For example, the PPS solution was lost 1421 Mb/sec in the first failure event at  $t_1$  426 min, while the PRS solution was lost 753 Mb/sec only, i.e., the half network traffic lost by the PPS solution. Alike in the remaining two failure events at  $t_3$  939 min and  $t_5$  1284 min by 2012 Mb/sec and 1758 Mb/sec loss rate of the PPS solution opposite the loss rate of the PRS by 453 Mb/sec and 412 Mb/sec, as shown in the dotted and dashed peaks of Figure 5.4 (c) above.

On the other hand, the measurements of the average end-to-end delay metric of the LSS solution indicated that it has the lowest delay than other solutions, followed by the PRS solution across three concurrent and consecutive cyberattacks against the core-core CIIs to turn 2 sec only for the LSS delay in the first failure event, 15 sec and 27 sec in the second and third failure events respectively.

Figure 5.4 (d) showed that the dotted gradient curve of the PPS solution pointed to end-to-end delay higher than the LSS and the PRS solutions. For instance, at  $t_1$  423 min of the first failure event, the delay result of the PPS solution was 6 sec, but at  $t_3$  934 min was 21 sec in the second failure and 28 sec at  $t_5$  1282 min of the final failure event.

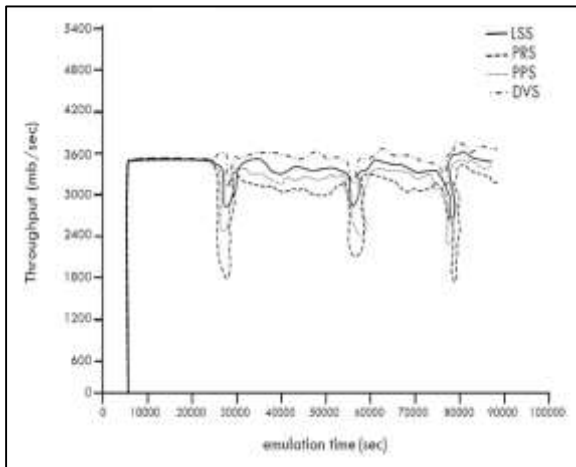
Nevertheless, the results of the PPS solution were upgraded considerably when measuring the standard metric of the average convergence duration during the core-core scenario. It succeeded in attaining its average convergence duration of around 447 sec in the first recovery event at  $t_2$  499 min, bypassing that with 376 sec in the second recovery event at  $t_4$  1020 min, to touch the 329 sec in the third recovery event at  $t_6$  1400 min.

These results have been proven in Figure 5.4 (e) that depicted the dotted zigzag curve of the PPS solution competed with the dash-dotted zigzag curve of the DVS solution, has the best convergence results tracked by the PPS solution. Upon that, the DVS solution results were 345 sec, 282 sec, and 386 sec through the recovery events previously mentioned.

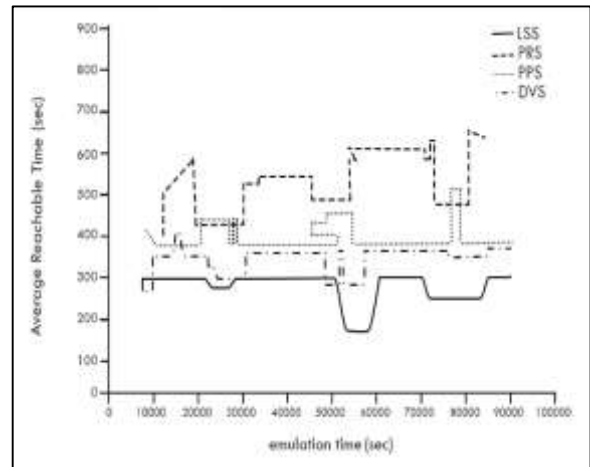
Table 5.8: Solutions Ranking of Primary Emulation Results for the Core-Core Scenario

<i>Standard Emulation Networking Metrics</i>	<i>Dynamic Cyber Resilience Factors</i>	<i>Ranking of Dynamic Cyber Resilience Solutions</i>			
		<i>PPS</i>	<i>PRS</i>	<i>LSS</i>	<i>DVS</i>
<i>Throughput</i>	<i>Performance</i>	3	4	2	1
<i>Average Reachable Time</i>	<i>Recovery</i>	2	4	1	3
<i>Network Traffic Lost</i>	<i>Absorption</i>	4	1	2	3
<i>Average End-to-End Delay</i>	<i>Volatility</i>	3	2	1	4
<i>Average Convergence Duration</i>	<i>Recovery Time</i>	2	3	4	1

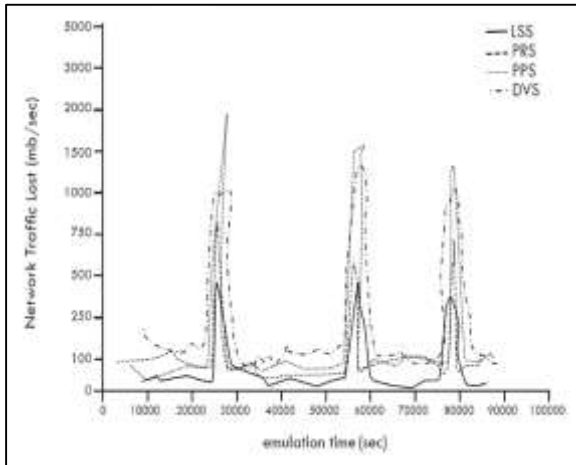
The competing rankings of the dynamic cyber resilience solutions in this research are displayed in Table 5.8 based on the primary emulation results once completing the testing core-core scenario. First, the LSS solution has the best ranking in the recovery and volatility factors, and second classifies in performance and absorption factors; then, the recovery time factor was in the latest class. Contrary, the DVS solution has a first place for the recovery time factor besides the performance factor. Additionally, it has not second ranks in any factors, but its recovery and absorption factors have third grades; however, the volatility factor was the latest. Generally, the third ranking was gone to the PRS solution in overall results with the first order for the absorption factor, the second position for the volatility factor, the third place for the recovery time factor, and the fourth level for performance and recovery factors. Finally, the PPS solution has no factor in the first title, but it has two factors in the second class: recovery and recovery time. Also, its performance and volatility factors were in third status; absorption factor came last.



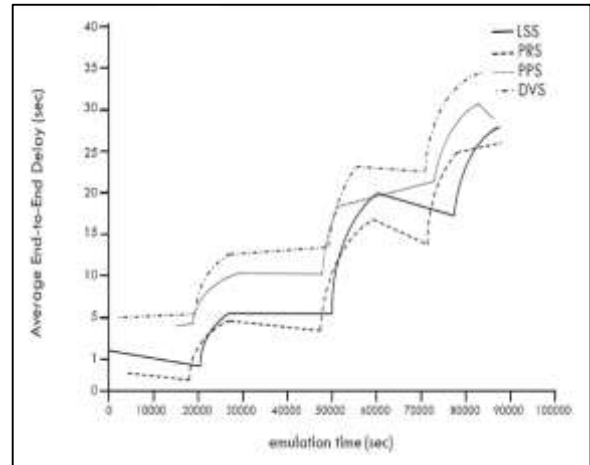
(a)



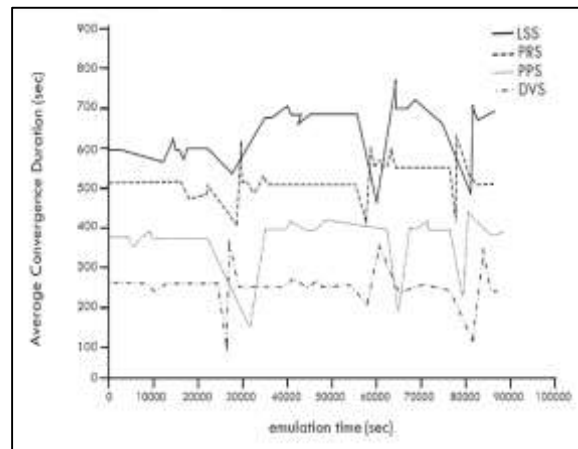
(b)



(c)



(d)



(e)

Figure 5.5: Primary Results of GNS3 Emulation for the Core-Edge Scenario

(a) Throughput (b) Average Reachable Time (c) Network Traffic Lost

(d) Average End-to-End Delay (e) Average Convergence Duration

Table 5.9: Primary Results of GNS3 Emulation for the Core-Edge Scenario

Networking Metrics	GNS3 Emulation			Dynamic Cyber Resilience Solutions			
	Event	Time (min)		PPS	PRS	LSS	DVS
Throughput (Mb/sec)	No Cyber Attack						
	No Failure	$t_0$	0424	3473	3418	3515	3526
	First Cyber Attack						
	First Failure	$t_1$	0425	2475	1803	2955	3110
	First Recovery	$t_2$	0499	3357	3014	3485	3604
	Second Cyber Attack						
	Second Failure	$t_3$	0939	2483	2144	2976	3077
	Second Recovery	$t_4$	1028	3399	3122	3515	3618
	Third Cyber Attack						
	Third Failure	$t_5$	1287	2336	1717	2766	3156
Third Recovery	$t_6$	1401	3522	3295	3607	3722	
Average Reachable Time (sec)	No Cyber Attack						
	No Failure	$t_0$	0420	0381	0406	0302	0336
	First Cyber Attack						
	First Failure	$t_1$	0421	0343	0415	0181	0300
	First Recovery	$t_2$	0496	0384	0535	0307	0346
	Second Cyber Attack						
	Second Failure	$t_3$	0939	0330	0490	0073	0288
	Second Recovery	$t_4$	1018	0387	0611	0308	0352
	Third Cyber Attack						
	Third Failure	$t_5$	1281	0303	0477	0247	0326
Third Recovery	$t_6$	1389	0383	0655	0305	0361	
Network Traffic Lost (Mb/sec)	No Cyber Attack						
	No Failure	$t_0$	0426	0076	0112	0034	0147
	First Cyber Attack						
	First Failure	$t_1$	0427	1982	0784	0453	1011
	First Recovery	$t_2$	0490	0081	0047	0033	0123
	Second Cyber Attack						
	Second Failure	$t_3$	0941	1536	0551	0479	1420
	Second Recovery	$t_4$	1027	0092	0092	0024	0101
	Third Cyber Attack						
	Third Failure	$t_5$	1288	1302	0729	0368	0989
Third Recovery	$t_6$	1398	0103	0095	0029	0096	
Average End-to-End Delay (sec)	No Cyber Attack						
	No Failure	$t_0$	0422	0004	0001	0002	0005
	First Cyber Attack						
	First Failure	$t_1$	0423	0010	0004	0005	0013
	First Recovery	$t_2$	0495	0004	0001	0001	0005
	Second Cyber Attack						
	Second Failure	$t_3$	0936	0018	0016	0020	0024
	Second Recovery	$t_4$	1020	0010	0003	0005	0014
	Third Cyber Attack						
	Third Failure	$t_5$	1284	0030	0025	0028	0034
Third Recovery	$t_6$	1395	0021	0014	0017	0023	
Average Convergence Duration (sec)	No Cyber Attack						
	No Failure	$t_0$	0431	0388	0510	0595	0275
	First Cyber Attack						
	First Failure	$t_1$	0432	0163	0412	0531	0094
	First Recovery	$t_2$	0499	0417	0637	0685	0382
	Second Cyber Attack						
	Second Failure	$t_3$	0940	0202	0425	0462	0213
	Second Recovery	$t_4$	1019	0396	0616	0778	0368
	Third Cyber Attack						
	Third Failure	$t_5$	1283	0224	0416	0506	0325
Third Recovery	$t_6$	1395	0406	0634	0713	0359	

Figure 5.5 (b) and Figure (c) introduce a shred of evidence that the LSS solution has the optimal results in two standard metrics through the core-edge scenario involving average reachable time and network traffic lost. While Figure 5.5 (a) and Figure 5.5 (e) present that the DVS solution has optimal throughput and average convergence duration metrics. However, the PRS solution has the lowest results in the metric of average end-to-end delay rather than other solutions, as shown in Figure 5.5 (d).

Regarding the PPS solution results in the above five standard metrics: in the first failure event, the PPS throughput was 2475 Mb/sec at  $t_1$  425 min, and it lost network traffic by the rate of 1982 Mb/sec at  $t_1$  427 min. Even though, in the second failure event, the PPS throughput was 2483 Mb/sec at  $t_3$  939 min with network traffic lost by 1536 Mb/sec at  $t_3$  941 min. It also has 2336 Mb/sec throughput at  $t_5$  1287 min, and 1302 Mb/sec network traffic lost at  $t_5$  1288 min in the third failure event.

Correspondingly, when comparing the PPS solution results with other solutions that optimal result in the average reachable time, average end-to-end delay, and average convergence duration, the PPS solution also attained acceptable results in these metrics. In detail, the average reachable time of the LSS solution reached 181 sec, 73 sec, and 247 sec in the failure events as opposed to in that order 343 sec, 330 sec, and 303 sec for the PPS solution of the same failure periods at  $t_1$  421 min,  $t_3$  939 min, and  $t_5$  1281 min.

Likewise, the results of the PRS solution in the average end-to-end delay metric were 4 sec in the first failure event at  $t_1$  423 min, increased to 16 sec in the second failure event at  $t_3$  936 min, and increased again to 25 sec in the third failure event at  $t_5$  1284 min. Thus, the results of the PPS solution in these failure events were wavering between 10 sec after the first cyberattack to 30 sec to the rear of the last cyberattack, passing by 18 sec once the second cyber attack occurred.

Table 5.10: Solutions Ranking of Primary Emulation Results for the Core-Edge Scenario

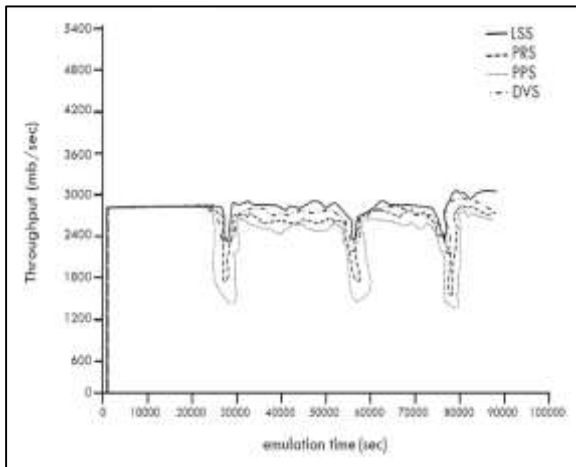
<i>Standard Emulation Networking Metrics</i>	<i>Dynamic Cyber Resilience Factors</i>	<i>Ranking of Dynamic Cyber Resilience Solutions</i>			
		<i>PPS</i>	<i>PRS</i>	<i>LSS</i>	<i>DVS</i>
<i>Throughput</i>	<i>Performance</i>	3	4	2	1
<i>Average Reachable Time</i>	<i>Recovery</i>	3	4	1	2
<i>Network Traffic Lost</i>	<i>Absorption</i>	4	2	1	3
<i>Average End-to-End Delay</i>	<i>Volatility</i>	3	1	2	4
<i>Average Convergence Duration</i>	<i>Recovery Time</i>	2	3	4	1

The standard metric result of the average convergence duration in the first recovery event for the DVS solution was 382 sec at  $t_2$  499 min; the result of the PPS solution was 417 sec. In the second recovery event at  $t_4$  1019 min, the convergence duration of the DVS solution was 368 sec, while this duration of the PPS solution was close to 396 sec. Finally, at  $t_6$  1395 min in the final recovery event next to the third cyberattack, the average convergence of the DVS solution and the PPS solution touched 359 sec and 406 sec, singly.

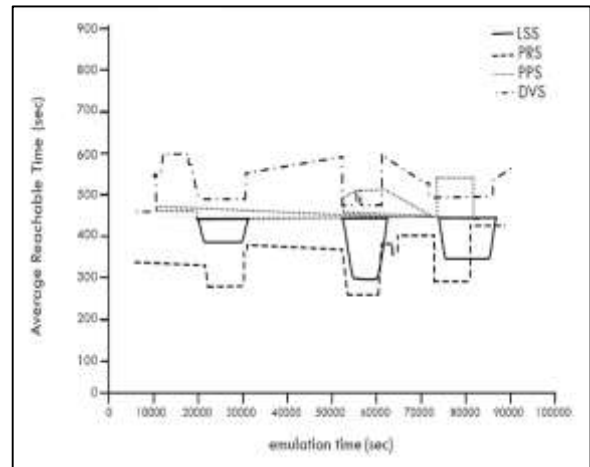
In conclusion, based on the primary emulated results for the four solutions of the dynamic cyber resilience through the core-edge scenario, the ending rankings for these solutions are established in Table 5.10. Note that the DVS solution has the optimal results in the throughput metric and average convergence duration, i.e., it was tiered first in the performance factor, and the recovery time factor competed with other solutions.

As well, the optimal results in the standard emulation networking metrics of the average reachable time and network traffic lost accomplished by the LSS solution; therefore, it has the first grade in the dynamic cyber resilience factors of the recovery and absorption. Completing the optimal results also applies in the same way to the PRS solution regarding the average end-to-end delay metric for fulfilling the first positioning in the volatility factor. Finally, PPS has no first-order in any dynamic cyber resilience factor mentioned atop; It has identical rankings between these emulated experiments and previous computing simulations thru the core-edge scenario.

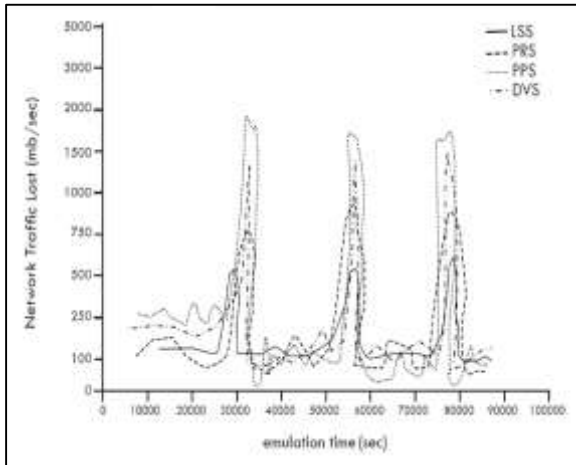




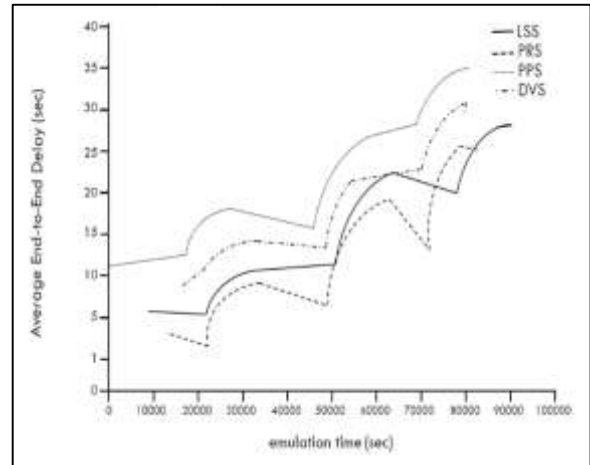
(a)



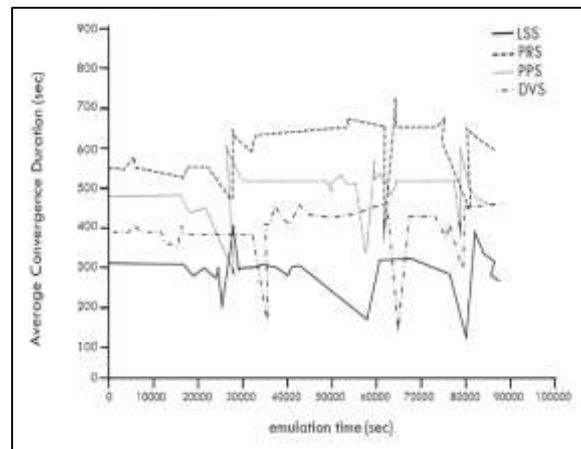
(b)



(c)



(d)



(e)

Figure 5.6: Primary Results of GNS3 Emulation for the Edge-Edge Scenario

(a) Throughput (b) Average Reachable Time (c) Network Traffic Lost

(d) Average End-to-End Delay (e) Average Convergence Duration

Table 5.11: Primary Results of GNS3 Emulation for the Edge-Edge Scenario

Networking Metrics	GNS3 Emulation			Dynamic Cyber Resilience Solutions			
	Event	Time (min)		PPS	PRS	LSS	DVS
Throughput (Mb/sec)	No Cyber Attack						
	No Failure	$t_0$	0423	2783	2812	2856	2834
	First Cyber Attack						
	First Failure	$t_1$	0424	1459	1793	2387	2400
	First Recovery	$t_2$	0498	2451	2589	2671	2888
	Second Cyber Attack						
	Second Failure	$t_3$	0938	1468	1808	2226	2413
	Second Recovery	$t_4$	1027	2565	2640	2723	2915
	Third Cyber Attack						
	Third Failure	$t_5$	1286	1387	1665	2318	2430
Third Recovery	$t_6$	1400	2643	2790	2902	2972	
Average Reachable Time (sec)	No Cyber Attack						
	No Failure	$t_0$	0422	0475	0335	0448	0600
	First Cyber Attack						
	First Failure	$t_1$	0423	0422	0283	0382	0497
	First Recovery	$t_2$	0500	0464	0387	0435	0581
	Second Cyber Attack						
	Second Failure	$t_3$	0943	0505	0276	0312	0489
	Second Recovery	$t_4$	1022	0452	0400	0457	0596
	Third Cyber Attack						
	Third Failure	$t_5$	1285	0543	0319	0348	0495
Third Recovery	$t_6$	1393	0459	0425	0434	0573	
Network Traffic Lost (Mb/sec)	No Cyber Attack						
	No Failure	$t_0$	0426	0258	0166	0135	0219
	First Cyber Attack						
	First Failure	$t_1$	0427	1892	0750	0502	1354
	First Recovery	$t_2$	0487	0136	0174	0128	0189
	Second Cyber Attack						
	Second Failure	$t_3$	0938	1666	0908	0500	1362
	Second Recovery	$t_4$	1024	0074	0158	0123	0174
	Third Cyber Attack						
	Third Failure	$t_5$	1285	1795	0827	0522	1481
Third Recovery	$t_6$	1393	0123	0067	0111	0116	
Average End-to-End Delay (sec)	No Cyber Attack						
	No Failure	$t_0$	0425	0011	0003	0005	0009
	First Cyber Attack						
	First Failure	$t_1$	0426	0017	0009	0011	0014
	First Recovery	$t_2$	0498	0013	0002	0005	0010
	Second Cyber Attack						
	Second Failure	$t_3$	0939	0027	0019	0023	0022
	Second Recovery	$t_4$	1023	0015	0006	0012	0014
	Third Cyber Attack						
	Third Failure	$t_5$	1287	0035	0025	0027	0031
Third Recovery	$t_6$	1402	0028	0013	0020	0024	
Average Convergence Duration (sec)	No Cyber Attack						
	No Failure	$t_0$	0430	0490	0555	0313	0383
	First Cyber Attack						
	First Failure	$t_1$	0431	0291	0490	0200	0176
	First Recovery	$t_2$	0498	0600	0651	0400	0423
	Second Cyber Attack						
	Second Failure	$t_3$	0939	0346	0384	0185	0155
	Second Recovery	$t_4$	1018	0578	0734	0331	0407
	Third Cyber Attack						
	Third Failure	$t_5$	1287	0362	0433	0127	0314
Third Recovery	$t_6$	1394	0594	0675	0392	0477	

The best primary results for the duration of the edge-edge scenario were acquired by the LSS solution and the PRS solution, whereas the DVS and the PPS solutions have modest results in this context. The solid line of the LSS solution pointed up in Figure 5.6 (a) its throughput outputs after first failure event started from 2387 Mb/sec at  $t_1$  424 min continued to second failure event by 2226 Mb/sec at  $t_3$  938 min ended by 2318 Mb/sec at  $t_5$  1286 min in a third failure event. The PPS results in this metric were one-to-one by 1459 Mb/sec, 1468 Mb/sec, and 1387 Mb/sec.

Moreover, the LSS solution results in the standard metric of the network traffic lost were 502 Mb/sec, 500 Mb/sec, and 522 Mb/sec as per solid peaks shown in Figure 5.6 (c) at the time of the first failure event  $t_1$  427 min, and at  $t_3$  938 min and  $t_5$  1285 min in the second and third failure events. However, the PPS solution has traffic loss rates of CII networks by 1892 Mb/sec, 1666 Mb/sec, and 1795 Mb/sec, respectively, for each failure event above in testing emulations.

Furthermore, the solid zigzag outputs illustrated in Figure 5.6 (e) presented that the average convergence duration of the LSS solution with no failure event was 313 sec at  $t_0$  430 min. Then, it decreased gradually from 200 sec in the first failure event at  $t_1$  431 min to 185 sec in the second one at  $t_3$  939 min reached to 127 sec lastly at  $t_5$  1287 min vis-a-vis its recovery events that ranged between 400 sec in the first recovery event at  $t_2$  498 min to 331 sec at  $t_4$  1018 min to 392 sec at  $t_6$  1394 min through the two rest recovery events. Nevertheless, the PPS solution results were 600 sec, 578 sec, and 594 sec in the recovery events versus 291 sec, 346 sec, and 362 sec in the failure events mentioned overhead.

On the other hand, the PRS solution optimal results in the standard emulation networking metrics of the average reachable time and average end-to-end delay through three failure events depending on the concurrent and consecutive cyberattacks wave against the edge-edge CII networks during the emulation scenario.

Table 5.12: Solutions Ranking of Primary Emulation Results for the Edge-Edge Scenario

<i>Standard Emulation Networking Metrics</i>	<i>Dynamic Cyber Resilience Factors</i>	<i>Ranking of Dynamic Cyber Resilience Solutions</i>			
		<i>PPS</i>	<i>PRS</i>	<i>LSS</i>	<i>DVS</i>
<i>Throughput</i>	<i>Performance</i>	4	3	1	2
<i>Average Reachable Time</i>	<i>Recovery</i>	3	1	2	4
<i>Network Traffic Lost</i>	<i>Absorption</i>	4	2	1	3
<i>Average End-to-End Delay</i>	<i>Volatility</i>	4	1	2	3
<i>Average Convergence Duration</i>	<i>Recovery Time</i>	3	4	1	2

The dashed irregular line of the PRS solution in Figure 5.6 (b) displayed that its average reachable time later the first failure event was 283 sec at  $t_1$  423 min, then the average time was decreased to 276 sec at  $t_3$  943 min in the second failure event, and suddenly it jumped to 319 sec at  $t_5$  1285 min when the last failure event has happened. However, PPS solution results measured by this metric were 422 sec, 505 sec, and 543 sec in parallel with the atop failure time frames.

Additionally, Figure 5.6 (d) showed the primary results through a dashed chaired curve clarified the average end-to-end delay of the PRS solution that excels the PPS solution. The delay time of the PRS solution was 9 sec versus 17 sec for the PPS solution in the first failure event at  $t_1$  426 min. Also, it was 19 sec for the PRS solution and 27 sec for the PPS solution at  $t_3$  939 min during the second failure event, as well as the results obtained after the third failure event at  $t_5$  1287 min, was 25 sec for the PRS solution and 35 sec for the PPS solution.

As evidenced by the primary results standard emulation networking metrics represented in Table 5.12, the rankings of the competing solutions of the dynamic cyber resilience in the emulated edge-edge scenario well deservedly went to the LSS solution with first classes in three dynamic cyber resilience factors and the PRS solution with first grades in two of these factors.

Whatever the case, the PPS solution has the third ordering in both recovery and recovery time factors. Also, the fourth categorizing among the standard solutions in three dynamic cyber resilience factors includes the performance factor, the absorption factor, and the volatility factor.

### ***Primary Results Analysis of Analytical Modeling***

Applying the adopted types of data analysis in this research, the analytical modeling was used as a quantitative research method besides the computing simulations and experimental emulations. The simulated and emulated data was collected and fed into the analytical modeling and then executed using the computerized mathematical platform (MAXIMA) based on quantification equations of dynamic cyber resilience by Tran (2015) coded in section 4.3.1 Chapter 4.

Analytical modeling was constructed primarily for computational processing to understand the various coupling behaviors of interdependent CII networks under single or multiple concurrent and consecutive cyber-attacks in different scenarios. Measuring  $R$  the single dynamic cyber resilience and  $R_{total}$  the total dynamic cyber resilience metrics when implementing the testing scenarios through simulations and emulations using proposed solution and each standard solution.

The  $R$  and  $R_{total}$  metrics were calculated on the integration basis of five dynamic cyber resilience factors modeled mathematically to evaluate the dynamic cyber resilience capabilities for interdependent CII networks to study their cyber failure effects.

Each MAXIMA Figure in this subsection consists of two exemplary diagrams; the left-side diagram described the single resilience  $R_1$ ,  $R_2$ ,  $R_3$  measurements for the four solutions of dynamic cyber resilience solutions over three cyber failure events. The right-side diagram showed the total resilience  $R_{total}$  measurements of these failure events for every dynamic cyber resilience solution.

Each MAXIMA Table also presents the single resilience and total resilience results for every dynamic cyber resilience used in testing scenarios. The higher results of the single resilience and total resilience mean that the dynamic cyber resilience solution is used to enhance the dynamic cyber resilience capabilities of interdependent CII networks and become cyber resilient against cyberattacks compared to other technology solutions.

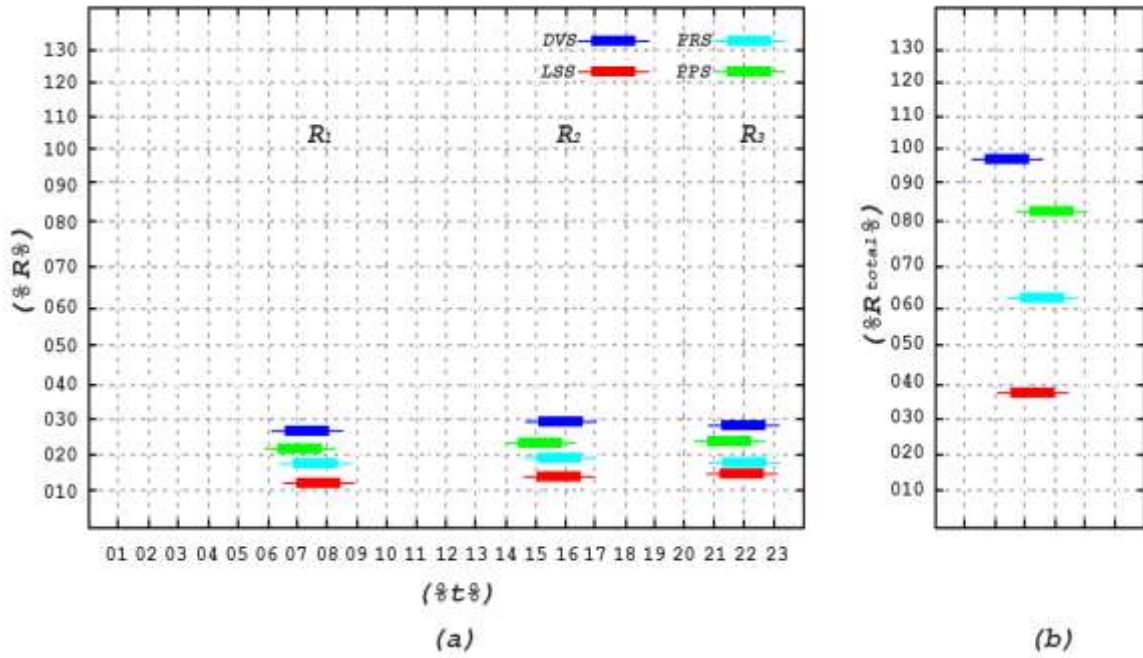


Figure 5.7: MAXIMA Analytical Modeling for Primary Simulated Core-Core Scenario  
 (a) Single Resilience ( $R_1, R_2, R_3$ ) (b) Total Resilience ( $R_{total}$ )

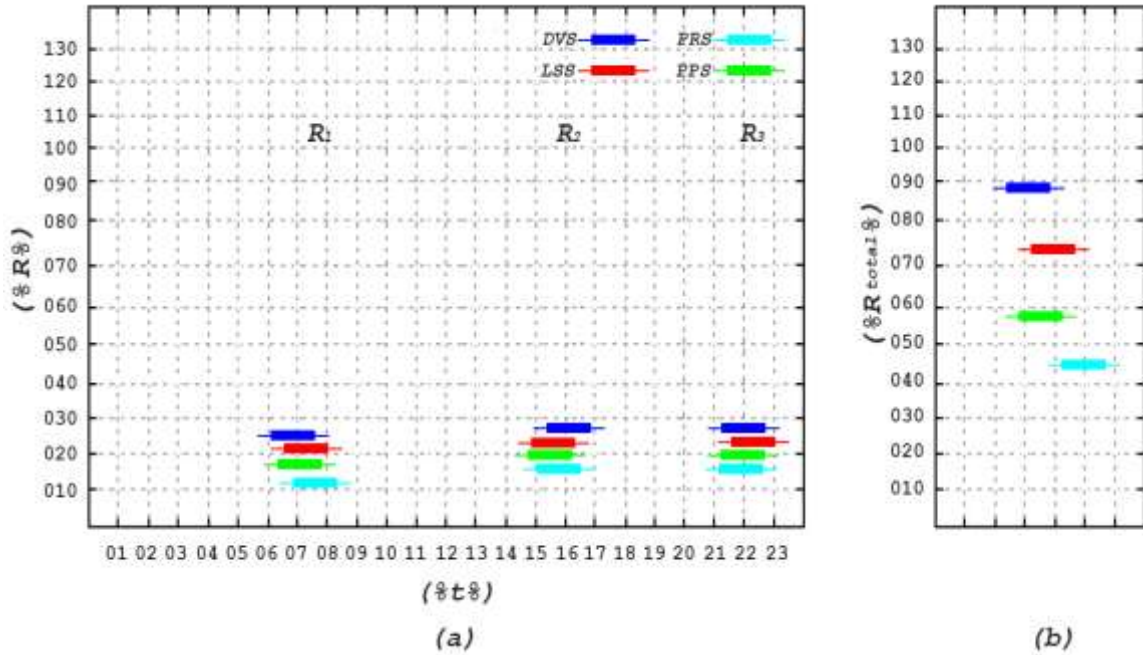


Figure 5.8: MAXIMA Analytical Modeling for Primary Simulated Core-Edge Scenario  
 (a) Single Resilience ( $R_1, R_2, R_3$ ) (b) Total Resilience ( $R_{total}$ )

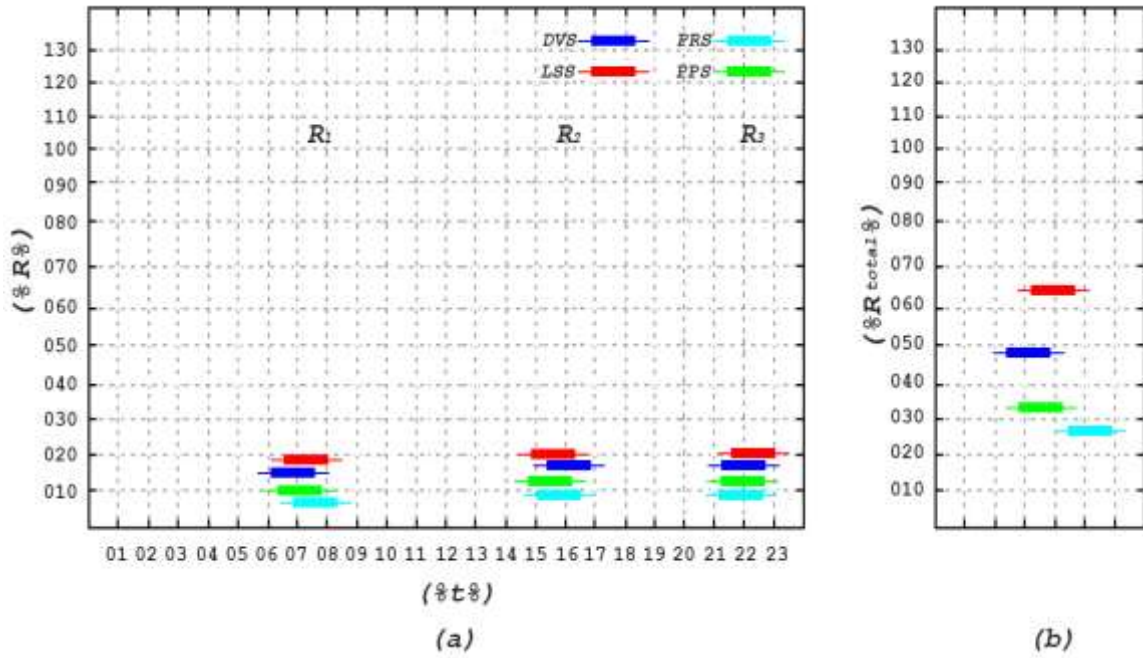


Figure 5.9: MAXIMA Analytical Modeling for Primary Simulated Edge-Edge Scenario  
 (a) Single Resilience ( $R_1, R_2, R_3$ ) (b) Total Resilience ( $R_{total}$ )

Table 5.13: Results of MAXIMA Analytical Modeling for Primary Simulated Scenarios

Simulated Scenarios	MAXIMA Analytical Modeling			Dynamic Cyber Resilience Solutions				
	Time (min)	Resilience	(R)	PPS	PRS	LSS	DVS	
Core-Core Scenario	$t_2$	First Cyber Attack						
		0503	First Resilience	$R_1$	0021	0018	0011	0027
		Second Cyber Attack						
		1023	Second Resilience	$R_2$	0022	0020	0012	0030
	$t_6$	1399	Third Resilience	$R_3$	0023	0019	0013	0029
			$R_{total}$	0082	0062	0038	0098	
Core-Edge Scenario	$t_2$	First Cyber Attack						
		0500	First Resilience	$R_1$	0017	0011	0021	0025
		Second Cyber Attack						
		1021	Second Resilience	$R_2$	0019	0016	0022	0028
	$t_6$	1395	Third Resilience	$R_3$	0020	0017	0023	0028
			$R_{total}$	0059	0047	0073	0098	
Edge-Edge Scenario	$t_2$	First Cyber Attack						
		0499	First Resilience	$R_1$	0010	0008	0019	0015
		Second Cyber Attack						
		1021	Second Resilience	$R_2$	0012	0009	0020	0016
	$t_6$	1396	Third Resilience	$R_3$	0011	0009	0020	0016
			$R_{total}$	0034	0028	0065	0049	

The blue rectangles in Figure 5.7 depicted the single resilience and total resilience for the proposed solution and standard solutions through the primary simulated core-core scenario. For example, the first single resilience value of the DVS solution was 27 at time  $t_2$  503 min, increased to 30 in the second single resilience at  $t_4$  1023 min, and then returned to 29 in the third single resilience at  $t_6$  1399 min with a total resilience value reaching 98, is the highest one than the other solutions.

Furthermore, Table 5.13 demonstrated that the DVS solution has the highest values of three single resilience throughout the core-edge scenario by  $R_1$  was 25 at time  $t_2$  500 min,  $R_2$  was 28 at  $t_4$  1021 min, and  $R_3$  was also 28 at  $t_6$  1395 min, as per disclosed in Figure 5.8 (a). Thus, the total resilience value of the DVS solution in this scenario by  $R_{total}$  was 98, as flashed in Figure 5.8 (b). Note that the  $R_{total}$  values of the DVS solution were the same on top of both scenarios.

Nevertheless, the total resilience value of the DVS in the edge-edge scenario as represented in Figure 5.9 (b) decreased to 49, whereas the first single resilience valued obtained from this third scenario was 15 at time  $t_2$  499 min, and 16 for the rest two single resilience values at  $t_4$  1021 min and  $t_6$  1396 min. Figure 5.9 (a) appeared that the LSS solution results were the highest in the edge-edge scenario by  $R_{total}$  value was 65 in similar for the single resilience values by  $R_1$  was 19 for the first resilience and by 20 for the second, third resilience individually.

The results of the PPS solution were differentiated into three testing scenarios from the overhead Figures and Table. In the core-core scenario, the first single resilience value by  $R_1$  was 21, a little bit increased to 22 by  $R_2$ , and slight also added to 23 by  $R_3$ , with a total resilience value of 82 by  $R_{total}$ . On another side, while in the core-edge scenario, the value of  $R_1$  was 17,  $R_2$  was 16, and  $R_3$  was 20, and the value of the total resilience was 59, i.e., these results of the PPS solution were lower than its results in the core-core scenario.

Likewise, the total resilience value of the PPS solution in the edge-edge scenario was lessened to arrive at  $R_{total}$  by 34, in the same way, the values of three single resilience were coming down to



become  $R_1$  by 10 for the first single resilience,  $R_2$  by 12 for the second one, and  $R_3$  by 11 for the last single resilience.

Table 5.14: Solutions Ranking for Total Resilience in Primary Simulated Scenarios

	<i>Ranking of Dynamic Cyber Resilience Solutions for <math>R_{total}</math> in Primary Simulated Scenarios</i>			
	<i>PPS</i>	<i>PRS</i>	<i>LSS</i>	<i>DVS</i>
<i>Core-Core Scenarios</i>	2	3	4	1
<i>Core-Edge Scenarios</i>	3	4	2	1
<i>Edge-Edge Scenarios</i>	3	4	1	2

The rankings of the dynamic cyber resilience solutions concluded in Table 5.14 based on the  $R_{total}$  values through primary simulated scenarios exhibited that the DVS solution ordered the first in total resilience via the core-core scenario and the core-edge scenario and the second sort in the edge-edge scenario where the LSS solution has the first-class throughout the third scenario.

Also, the LSS solution attained the second arrange in the core-edge scenario and the fourth position in the core-core scenario. Nevertheless, the PPS solution was classified second in the core-core scenario and third in the other two scenarios. Finally, the PRS solution has the third category in the first and fourth in the second and third scenarios.

In order to validate the results of the single resilience and total resilience for the proposed solution and standard solutions obtained in the primary simulated scenarios, the repetition of these scenarios has been performed but at this instant all the way through the emulated experimental scenarios. The primary emulated core-core scenario illustrated in Figure 5.10 (a) below indicated that the single resilience values of the DVS solution ranged between  $R_1$  by 31 at time  $t_2$  499 min to  $R_2$  and  $R_3$  by 32 for each of them at  $t_4$  1020 min and  $t_6$  1400 min respectively, also the DVS total resilience value was the highest one than other solutions  $R_{total}$  by 102.

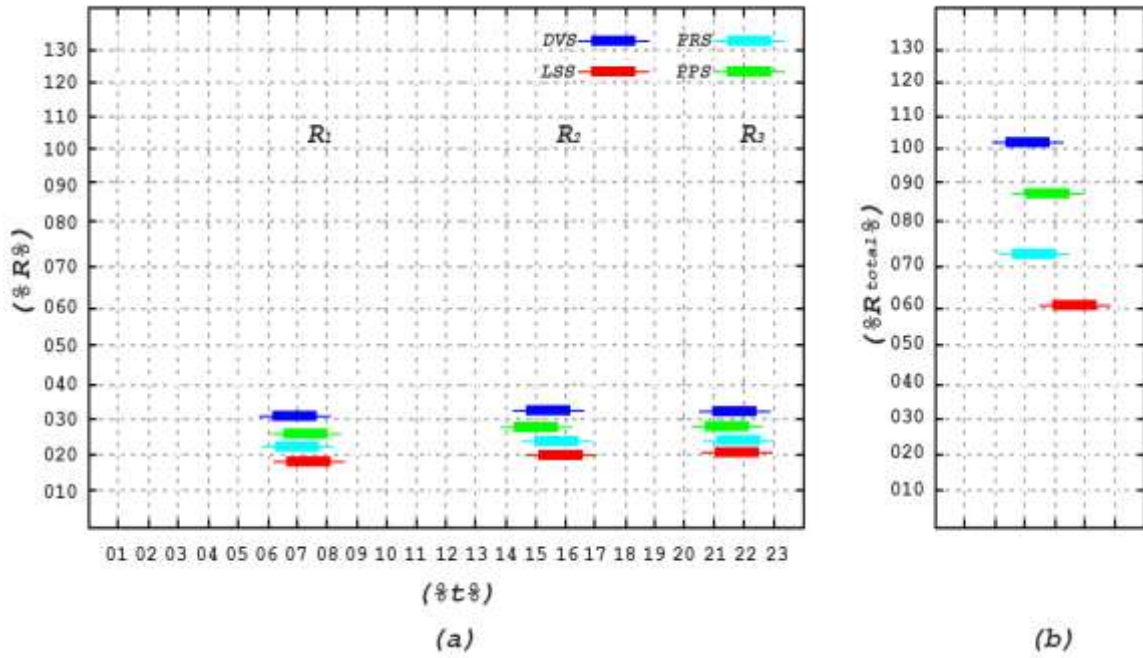


Figure 5.10: MAXIMA Analytical Modeling for Primary Emulated Core-Core Scenario  
 (a) Single Resilience ( $R_1, R_2, R_3$ ) (b) Total Resilience ( $R_{total}$ )

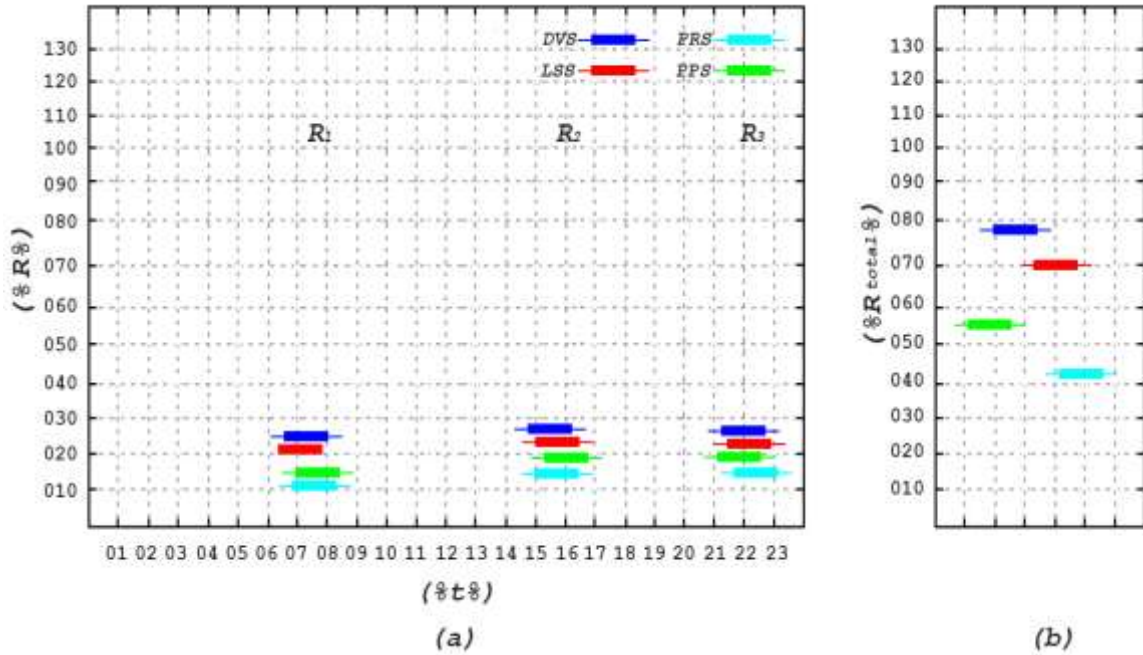


Figure 5.11: MAXIMA Analytical Modeling for Primary Emulated Core-Edge Scenario  
 (a) Single Resilience ( $R_1, R_2, R_3$ ) (b) Total Resilience ( $R_{total}$ )

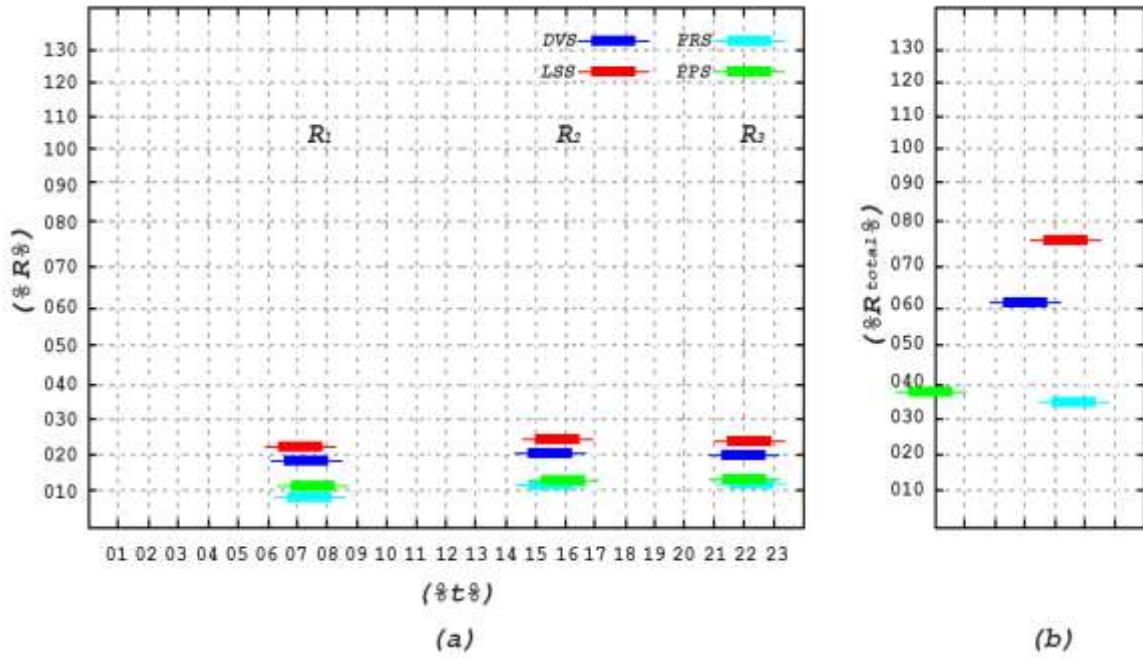


Figure 5.12: MAXIMA Analytical Modeling for Primary Emulated Edge-Edge Scenario  
 (a) Single Resilience ( $R_1, R_2, R_3$ ) (b) Total Resilience ( $R_{total}$ )

Table 5.15: Results of MAXIMA Analytical Modeling for Primary Emulated Scenarios

Emulated Scenarios	MAXIMA Analytical Modeling				Dynamic Cyber Resilience Solutions			
	Time (min)	Resilience	(R)	PPS	PRS	LSS	DVS	
Core-Core Scenario	<i>First Cyber Attack</i>							
	$t_2$	0499	First Resilience	$R_1$	0026	0023	0018	0031
	<i>Second Cyber Attack</i>							
	$t_4$	1020	Second Resilience	$R_2$	0028	0024	0020	0032
	<i>Third Cyber Attack</i>							
$t_6$	1400	Third Resilience	$R_3$	0028	0023	0020	0032	
<i>Total Resilience</i>								
			$R_{total}$	0088	0073	0061	0102	
Core-Edge Scenario	<i>First Cyber Attack</i>							
	$t_2$	0499	First Resilience	$R_1$	0015	0011	0021	0025
	<i>Second Cyber Attack</i>							
	$t_4$	1019	Second Resilience	$R_2$	0019	0014	0023	0026
	<i>Third Cyber Attack</i>							
$t_6$	1395	Third Resilience	$R_3$	0019	0013	0023	0026	
<i>Total Resilience</i>								
			$R_{total}$	0056	0043	0070	0079	
Edge-Edge Scenario	<i>First Cyber Attack</i>							
	$t_2$	0498	First Resilience	$R_1$	0011	0009	0021	0019
	<i>Second Cyber Attack</i>							
	$t_4$	1018	Second Resilience	$R_2$	0013	0011	0025	0020
	<i>Third Cyber Attack</i>							
$t_6$	1394	Third Resilience	$R_3$	0013	0012	0024	0020	
<i>Total Resilience</i>								
			$R_{total}$	0039	0036	0077	0062	

In the same scenario, as shown in Figure 5.10 (b), the DVS solution was followed by the PPS solution, which has the total resilience value  $R_{total}$  by 88, and three single resilience values were by 26 for  $R_1$ , and the value of 28 for  $R_2$  and  $R_3$  separately. However, the value of the total resilience of the PPS solution in the core-edge scenario stood out in Figure 5.10 (b) was  $R_{total}$  by 56 in contrast to the DVS solution, also kept on the highest value of the total resilience  $R_{total}$  by 79 in the second scenario than other solutions.

In Table 5.15, the single resilience values of the DVS solution and the PPS solution in the core-edge scenario were obvious dissimilar; the first single resilience at time  $t_2$  499 min of the DVS solution was  $R_1$  by 25 while for the PPS solution was  $R_1$  by 15, likewise for the DVS  $R_2$  and DVS  $R_3$  by 26 individually, the second and third single resilience of the PPS solution were  $R_2$  and  $R_3$  by 19 independently, as verified in Figure 5.11 (a).

Table 5.16: Solutions Ranking for Total Resilience in Primary Emulated Scenarios

	<i>Ranking of Dynamic Cyber Resilience Solutions for <math>R_{total}</math> in Primary Emulated Scenarios</i>			
	<i>PPS</i>	<i>PRS</i>	<i>LSS</i>	<i>DVS</i>
<i>Core-Core Scenarios</i>	2	3	4	1
<i>Core-Edge Scenarios</i>	3	4	2	1
<i>Edge-Edge Scenarios</i>	3	4	1	2

On the other hand, the first single resilience value of the LSS solution in the edge-edge scenario, as appeared in Figure 5.12 (a), ran to  $R_1$  by 21 at time  $t_2$  498 min, raised to  $R_2$  by 25 for the second single resilience at  $t_4$  1018 min, then dropped off a little bit to settle down at  $R_3$  by 24 at  $t_6$  1394 min with the value of the total resilience  $R_{total}$  near 77.

Even so, the PPS solution was realized the total resilience  $R_{total}$  by 39, as surfaced in Figure 5.12 (b). Consequently, the single resilience values of the PPS solution were  $R_1$  by 11 for the first single resilience,  $R_2$  by 13 as well as  $R_3$  by 13 for the second and third single resilience at the same time frames via the current scenario.

As the results validation evidence that acquired from the above ranking's tables in this subsection,

each dynamic cyber resilience solution, whether it was a standard solution or the proposed solution, has the same ordering exactly for the total resilience in both Table 5.14 and Table 5.16 in that order of primary simulated scenarios and primary emulated scenarios, respectively.

Evidently, the optimized proposed solution (OPS) categorizing was strongly higher than the primary proposed solution (PPS) in all research scenarios due to the improvements were conducted on the conceptual framework and technology stack in this thesis, the optimization phase. Therefore, the OPS solution has the first order in core-core scenarios, while the PPS solution has the second.

Furthermore, the OPS solution has the second level in core-edge and edge-edge scenarios; however, the PPS solution has the third class in both series of these scenarios. The rankings of the other standard solutions were the same in primary and optimization phases equally overall simulated and emulated scenarios because they were used as control solutions in this research. The rest pages of this subsection organized a comprehensive analysis with results comparisons for the primary and optimized proposed solutions based on the single and total resilience metrics.

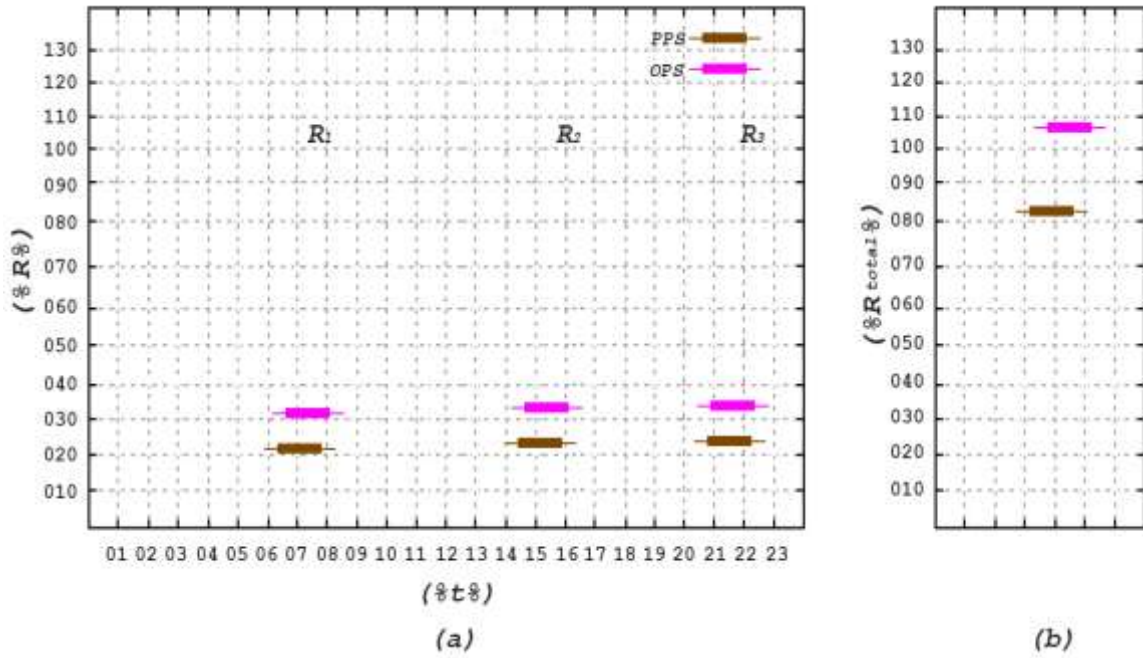


Figure 5.25: MAXIMA Analytical Modeling of Proposed Solution for Simulated Core-Core Scenarios (a) Single Resilience ( $R_1, R_2, R_3$ ) (b) Total Resilience ( $R_{total}$ )

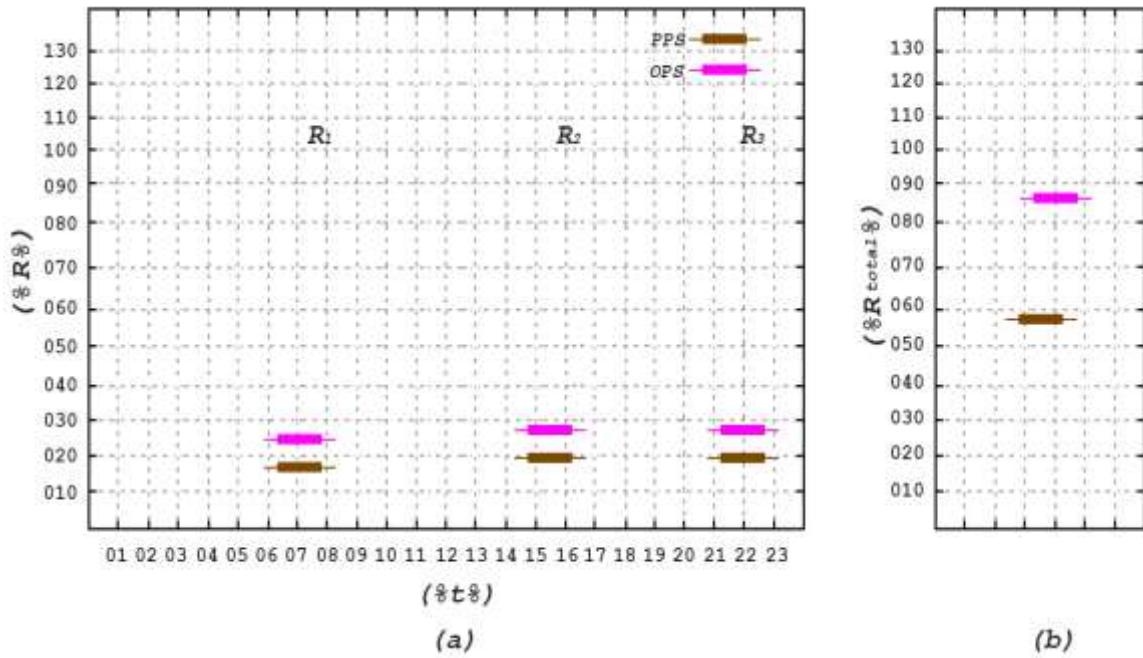


Figure 5.26: MAXIMA Analytical Modeling of Proposed Solution for Simulated Core-Edge Scenarios (a) Single Resilience ( $R_1, R_2, R_3$ ) (b) Total Resilience ( $R_{total}$ )

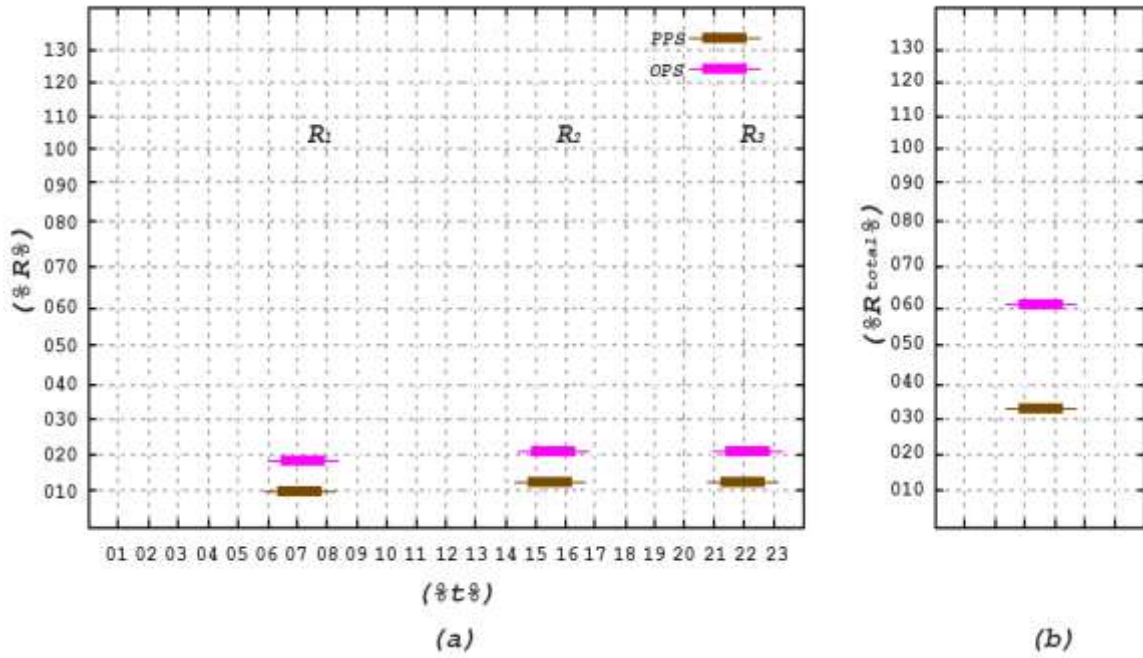


Figure 5.27: MAXIMA Analytical Modeling of Proposed Solution for Simulated Edge-Edge Scenarios (a) Single Resilience ( $R_1, R_2, R_3$ ) (b) Total Resilience ( $R_{total}$ )

Table 5.34: Proposed Solution Results of MAXIMA Analytical Modeling for Simulated Scenarios

Simulated Scenarios	MAXIMA Analytical Modeling			Proposed Solution	
	Time(min)	Resilience	(R)	PPS	OPS
Core-Core Scenario	<i>First Cyber Attack</i>				
	$t_2$	0500	First Resilience	$R_1$	0021
	<i>Second Cyber Attack</i>				
	$t_4$	1025	Second Resilience	$R_2$	0022
	<i>Third Cyber Attack</i>				
$t_6$	1397	Third Resilience	$R_3$	0023	
<i>Total Resilience</i>					
			$R_{total}$	0082	0108
Core-Edge Scenario	<i>First Cyber Attack</i>				
	$t_2$	0496	First Resilience	$R_1$	0017
	<i>Second Cyber Attack</i>				
	$t_4$	1023	Second Resilience	$R_2$	0019
	<i>Third Cyber Attack</i>				
$t_6$	1395	Third Resilience	$R_3$	0020	
<i>Total Resilience</i>					
			$R_{total}$	0059	0088
Edge-Edge Scenario	<i>First Cyber Attack</i>				
	$t_2$	0497	First Resilience	$R_1$	0010
	<i>Second Cyber Attack</i>				
	$t_4$	1024	Second Resilience	$R_2$	0012
	<i>Third Cyber Attack</i>				
$t_6$	1395	Third Resilience	$R_3$	0011	
<i>Total Resilience</i>					
			$R_{total}$	0034	0062



Table 5.34 introduced the comparison of the results between the PPS solution and the OPS solution during all simulated core-core scenarios in this research. It can be seen that the first single resilience  $R_1$  value for the PPS was 21 at  $t_2$  500 min at the same time as 32 for the OPS.

Also, the second single resilience  $R_2$  for the PPS solution was 22, and for the OPS solution was 34 at  $t_4$  1025 min. The  $R_3$  values at  $t_6$  1397 min for PPS and OPS solutions were 23 in turn of 35. After all, the total resilience  $R_{total}$  value of the PPS solution was 82 in front of 108 for the OPS solution with the difference of 26, as displayed in Figure 5.25.

In the simulated core-edge scenarios, the single resilience values of the PPS solution were  $R_1$  by 17 at  $t_2$  496 min,  $R_2$  by 19 at  $t_4$  1023 min, and  $R_3$  by 20 at  $t_6$  1395 min with total resilience value  $R_{total}$  by 59. These values were facing the values of the single resilience for the OPS solution over the same time frames with the  $R_1$  value of 27, the  $R_2$  value of 28, and the  $R_3$  value of 27. As a result, the OPS total resilience value  $R_{total}$  was accomplished to 88, as illustrated in Figure 5.26.

Table 5.35: Proposed Solution Ranking for Total Resilience in All Simulated Scenarios

	Ranking of Proposed Solution for $R_{total}$ in All Simulated Scenarios	
	PPS	OPS
Core-Core Scenarios	2	1
Core-Edge Scenarios	2	1
Edge-Edge Scenarios	2	1

Furthermore, Figure 5.27 (b) compares the PPS and OPS solutions in the edge-edge scenarios based on the single and total resilience values. The total resilience value of the PPS was 34, which is lower than the  $R_{total}$  of the OPS with 26. At  $t_2$  497 min, the first single resilience  $R_1$  value for the PPS was 10, even as 19 for the OPS. Also, the  $R_2$  and  $R_3$  values of the PPS were 12 at  $t_4$  1024 min and 11 at  $t_6$  1395 min, but the values of the second and third single resilience for the OPS were 21 singly, as illuminated in Figure 5.27 (a). In general, OPS was rated first in all simulated scenarios and therefore outperformed PPS, as concluded in Table 5.35.



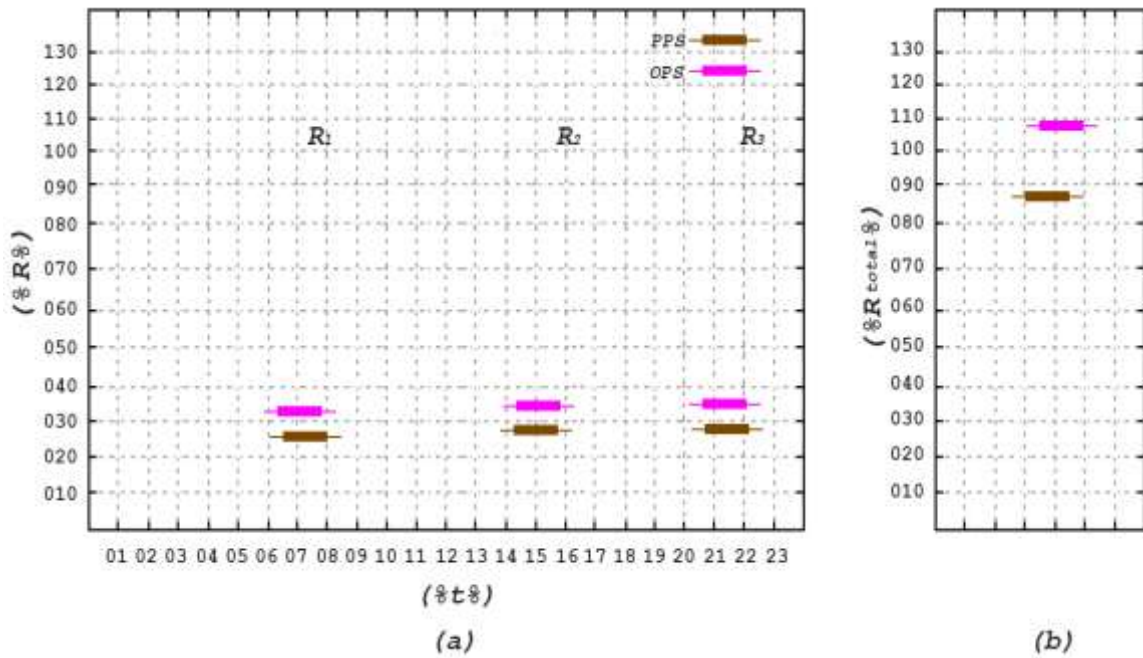


Figure 5.28: MAXIMA Analytical Modeling of Proposed Solution for Emulated Core-Core Scenarios (a) Single Resilience ( $R_1, R_2, R_3$ ) (b) Total Resilience ( $R_{total}$ )

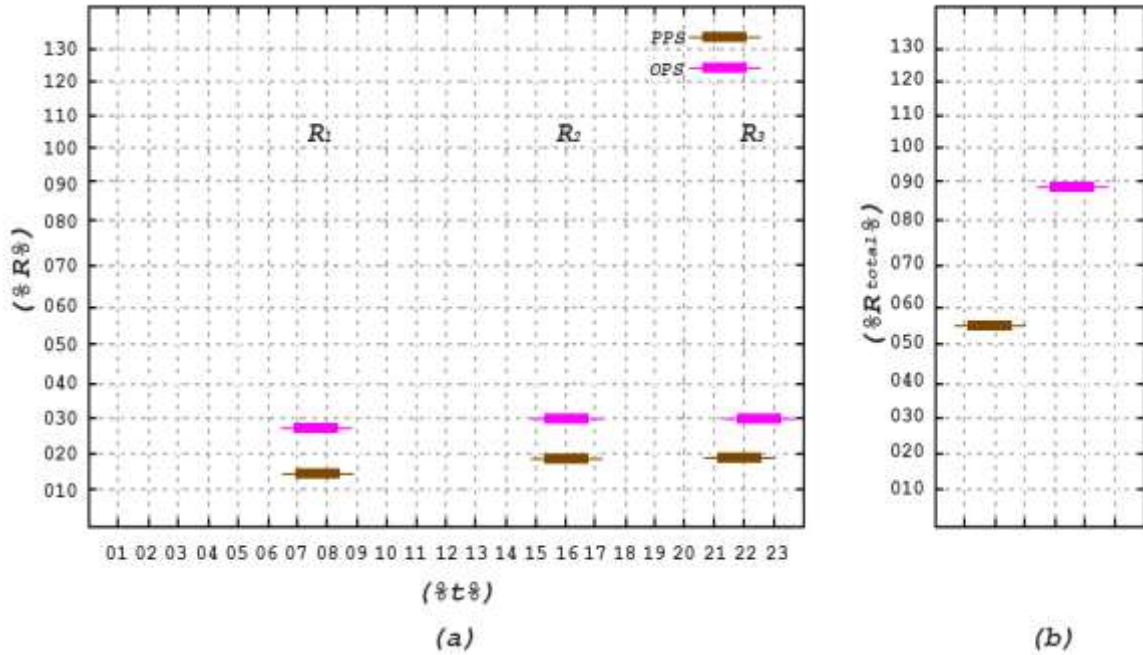


Figure 5.29: MAXIMA Analytical Modeling of Proposed Solution for Emulated Core-Edge Scenarios (a) Single Resilience ( $R_1, R_2, R_3$ ) (b) Total Resilience ( $R_{total}$ )

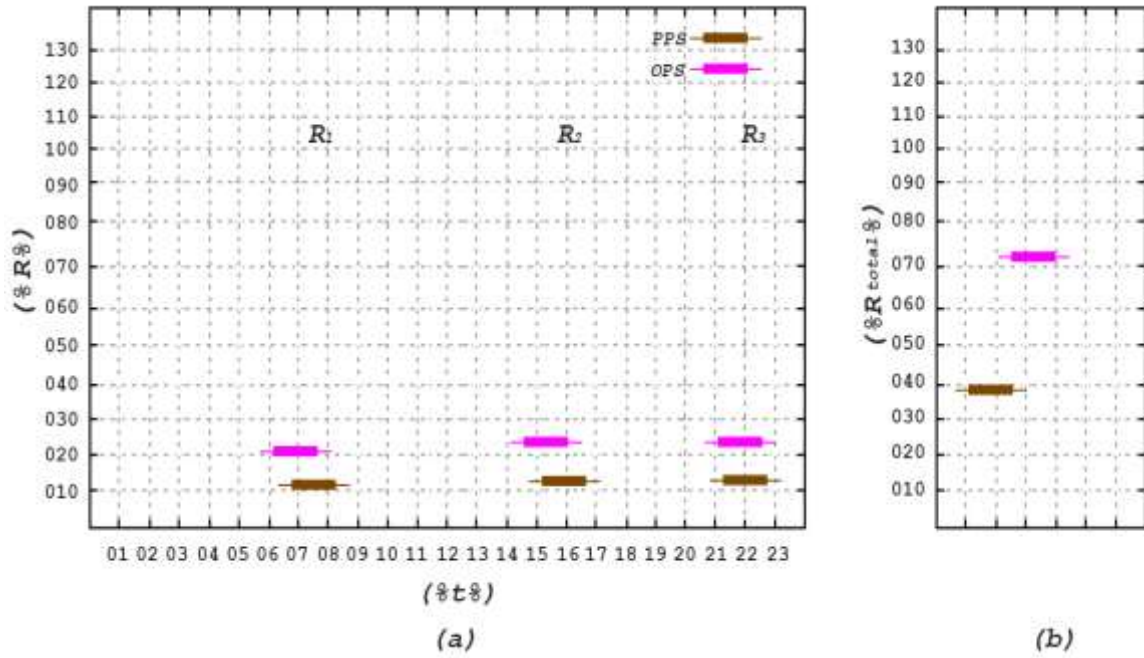


Figure 5.30: MAXIMA Analytical Modeling of Proposed Solution for Emulated Edge-Edge Scenarios (a) Single Resilience ( $R_1, R_2, R_3$ ) (b) Total Resilience ( $R_{total}$ )

Table 5.36: Proposed Solution Results of MAXIMA Analytical Modeling for Emulated Scenarios

Emulated Scenarios	MAXIMA Analytical Modeling			Proposed Solution	
	Time(min)	Resilience	(R)	PPS	OPS
Core-Core Scenario				First Cyber Attack	
	$t_2$	0495	First Resilience	$R_1$	0026
				Second Cyber Attack	
	$t_4$	1024	Second Resilience	$R_2$	0028
				Third Cyber Attack	
	$t_6$	1402	Third Resilience	$R_3$	0028
			Total Resilience		
			$R_{total}$	0088	0109
Core-Edge Scenario				First Cyber Attack	
	$t_2$	0496	First Resilience	$R_1$	0015
				Second Cyber Attack	
	$t_4$	1018	Second Resilience	$R_2$	0019
				Third Cyber Attack	
	$t_6$	1393	Third Resilience	$R_3$	0019
			Total Resilience		
			$R_{total}$	0056	0091
Edge-Edge Scenario				First Cyber Attack	
	$t_2$	0494	First Resilience	$R_1$	0011
				Second Cyber Attack	
	$t_4$	1017	Second Resilience	$R_2$	0013
				Third Cyber Attack	
	$t_6$	1397	Third Resilience	$R_3$	0013
			Total Resilience		
			$R_{total}$	0039	00073

The results of the PPS and the OPS solutions were obtainable in the emulated scenarios long-established the results of the simulated scenarios as offered in Table 5.36. Upon the core-core scenarios, the first single resilience value of the PPS solution was 26 at  $t_2$  495 min; also, its second and third single resilience values were 28 at  $t_4$  1024 min and  $t_6$  1402 min individually. However, the first single resilience  $R_1$  value of the OPS solution was 32, enlarged to turn out to be an  $R_2$  value of 35 and later be converted into an  $R_3$  value of 36 with total resilience  $R_{total}$  value of 109 versus 88 for the OPS solution, as exhibited in Figure 5.28.

In the consistent perspective, the values of the single and total resilience in the core-edge scenarios came out as shown in Figure 5.29 to ensure the significant distinction of the OPS solution with the  $R_{total}$  value of 91 while the  $R_{total}$  value is valued of the PPS solution was 56. Likewise, the OPS single resilience was  $R_1$  value of 28 at  $t_2$  496 min,  $R_2$  and  $R_3$  values of 30 for each one-by-one at  $t_4$  1018 min and  $t_6$  1393 min. On the other hand, the single resilience values of the PPS solution ranged between 15 for the  $R_1$  and 19 for the  $R_2$  and  $R_3$  separately.

Table 5.37: Proposed Solution Ranking for Total Resilience in All Emulated Scenarios

	Ranking of Proposed Solution for $R_{total}$ in All Emulated Scenarios	
	PPS	OPS
Core-Core Scenarios	2	1
Core-Edge Scenarios	2	1
Edge-Edge Scenarios	2	1

In Figure 5.30, the results of the OPS solution surpassed the results of the PPS solution in terms of single resilience and total resilience. At  $t_2$  494 min, the first single resilience values were PPS  $R_1$  value of 11 and doubled for OPS  $R_1$  value of 22. The PPS  $R_2$  and  $R_3$  values were 13 singly at  $t_4$  1017 min and  $t_6$  1397 min vis-à-vis values of 24 and 23 for the OPS  $R_2$  and  $R_3$ , respectively. On the other hand, Table 5.37 concluded the superiority positioning of OPS solution over PPS solution in all emulated scenarios during this thesis based on the total resilience metric results.

### ***Primary Results Discussion***

Discussion of the primary results of this thesis are stemmed from an academic standpoint; it is subjective by modules that deliver an understanding of the fundamental concepts, algorithms, and protocols that impact the primary proposed solution and how it is expected to implement its technology stack through the research simulations and emulations, considering all of the concerns in more detail along with each iterative four-objective cycle.

The proposed solution developed the primary technology stack to strengthen the dynamic cyber resilience capabilities with the primary conceptual framework as the main involvement. In addition, the integrated architecture has presented the modules for successful adoption and obstacles to algorithms and protocols for cyber zero-trust engineering.

As a reminder, the core-core scenarios implemented using OPNET computing simulations and the GNS3 emulated experiments, as shown in Figure 4.14 and Figure 4.15 within Chapter 4. The Etisalat CII and DEWA CII networks as core networks have been attacked simultaneously  $t_1$ ,  $t_3$ , and  $t_5$  by three concurrent and consecutive DDoS cyberattacks.

In light of the identical simulated and emulated results of these core-core scenarios for the PPS solution and standard solutions raised in Table 5.2 and Table 5.8, indicated the withstanding capability of the PRS solution was the best one than other solutions for absorbing the cyber disturbances caused by cyberattacks due to the TTL Security Check mechanism.

This lightweight security mechanism prevented attempts to hijack the peering sessions from concurrent and consecutive cyberattacks by a forged host on a segment between peers not part of the Etisalat CII network. Also, it protected the Etisalat-DEWA CII networks against remote DDoS cyberattacks (Godán et al., 2016).

The network traffic was sent with a certain TTL and rejected any packet with a smaller TTL than a

configured threshold. Since TTL decrements to the minimum, packets from connected hub nodes directly will be accepted only (Mosharraf et al., 2015).

Likewise, the Distribute-List Filter enhanced the robustness and reliability pre-disruption characteristics of the LSS solution to achieve the second-best place among the tested technology solutions in the withstanding capability (Hadjoannou, 2015). The distribution list filters the inbound and outbound network traffic by checking if the packets routed between the Etisalat-DEWA CII were permitted or not before accepting them and using extended access lists to filter the updates (Mohammad et al., 2017).

However, this filter does not affect link-state advertisement as the basic requirements of the IS-IS routing protocol were that the hub nodes in a DEWA CII network must have an identical link-state database (Sathyasri et al., 2021). Moreover, the distribute-list filter allows only the routes to enter the IS-IS routing table and prevents packets from propagating (Manzoor et al., 2020).

Furthermore, the degree of the cyber shocks absorption of the DVS solution was very low compared to the PRS and the LSS solutions, especially before reaching the threshold state. This withstanding capability tremendously affected using Message-Digest Algorithm Type 5 (MD5) that generated digests of the original records transmitted over the Etisalat-DEWA CII networks and stored the outputs via 128-bit one-way hash values (Giri et al., 2020).

The reason was that the MD5 hashing created the same hash function for two different inputs of the original record transmitted and provided no security over the DDoS collision cyberattacks (Wright et al., 2016). As well, the order of the withstanding capability of the primary proposed solution PPS was the last one of all technology solutions in the testing core-core scenarios.

The PPS solution depended on two cyber zero-trust protocols of the Hash Graph and asynchronous Byzantine Fault Tolerance (aBFT). Theoretically, the hash graph protocol has a fast speed of process records with high latency, and aBFT protocol strengthens the robustness of the hash graph Etisalat

CII network based on the decentralized hub nodes consensus because if less than one-third of the hub nodes were malicious (Luykx & Baird, 2020).

Therefore, they recognized unanticipated cyber failure events and survived cyber aggression against the cyberattack traffic of multiple DDoS botnets towards targeted hub nodes in the Etisalat-DEWA CII networks (Baird, 2016). Nevertheless, this was not empirical enough to fulfill the implementations' expectations and bypass them over computing simulations and emulated experiments (James et al., 2019).

On the other hand, the mitigation capability of the LSS solution in the core-core scenarios was the highest one amongst similar capabilities of the other technology solutions. Tables 5.2 and 5.8 presented that the LLS solution has a strong ability to adjust to undesirable situations and avoid dropping to the bottom state by underpinning volatile changes via Virtual Router Redundancy Protocol (VRRP) on non-essential attributes and localizing the redundant resources (Saini et al., 2021).

The VRRP eliminated a single point of cyber failure at the layer-3 level in the Etisalat-DEWA CII networks and employed in active-passive configurations. Also, this protocol provided an active-active configuration with load balancing by enabling multiple redundancies (Yin et al., 2018). Furthermore, it has pre-configured hub nodes to quickly take failover for resuming the functions of the DEWA CII network earlier once the coupled hub node fails (Robles et al., 2021).

As a continuation to review the results of the PRS solution that competed for second place in the mitigation capability through adopting the Control Plane Policing (CoPP), policed the traffic coming into the Etisalat-DEWA CII networks (Manzoor et al., 2020). The CoPP treated the network traffic received by the decentralized hub node as a logical source, filtered at one aggregate level, and processed with its inbound and outbound interfaces; just routed packets destined and policed were passed (Krupp & Rossow, 2021).

The situation was no better for the PPS solution concerning its mitigation capability influenced by the Internet Group Management (IGMP) protocol and Transport Layer Security (TLS) protocol. However, the IGMP protocol is a dynamic multicasting communication with datagram encapsulation to utilize the resources for traffic control but did not provide efficient traffic filtering (Sargent et al., 2017).

Moreover, TLS represented an all-or-nothing protocol since not work end-to-end, simply point-to-point. It ignored the record contents, not selectively applying to portions of the record (Rescorla & Dierks, 2018). The records were protected only while in transit, but the protection was removed automatically by the endpoints when they received the records (Dowling et al., 2020).

The mitigation capability was graded the least due to the Gateway Load Balancing Protocol (GLBP) limitations regarding the DVS solution. Despite providing redundancy and load balancing functions over multiple hub nodes using multiple virtual addresses, the maximum of four peers' addresses simultaneously (Syahputra et al., 2020). When one of the hub node peers was failed in the Etisalat-DEWA CII networks, only one of the other four peers in the same group forwarded the network traffic (Robles et al., 2021).

Then again, the recovery capability in the core-core scenarios tested the general preparedness of the dynamic cyber resilience solutions to heighten the self-healing and reorganize the CII resources after the cyberattack events to recover the equilibrium state of the coupled CII networks. The primary research results described in the simulation and emulation tables in section one of this chapter showed that the recovery capability of the LSS solution and PPS solution were superior contrasted to the DVS solution and PRS solution.

The Resilient Packet Ring (RPR) protocol implemented by the LSS solution provided dual-ring topology, including automatic reconfiguration and bandwidth utilization after cyber failure (Hadjiioannou, 2015). In addition, it reduced the number of paths by half and reused the spatial

bandwidth several times to maintain the same total resilience as Etisalat-DEWA CII networks with no need for costly decentralized hub nodes through packets forwarding in redundant paths (Ojo et al., 2021).

Similarly, the PPS solution has operated the gossip and virtual voting protocols to produce a consensus mechanism through spreading and sharing records to the hub nodes in the Etisalat-DEWA CII networks (DhivyaShree et al., 2016). In addition, both protocols performed selective optimization of gossiped records to reduce the communicating overhead costs (Tetarave et al., 2015).

On the opposite, the Resilient Ethernet Protocol (REP) was employed with the suit of the DVS solution to support the recovery capability (Barker et al., 2017). The REP was fast and reliable for cyber failure detection across the multicast address with acknowledgment and retransmitting if lost (De Florio, 2015). However, it has a limited amount of redundancy that brings about one cyber failure recovery only inside the coupled segments; multiple cyber failures were caused a high loss of Etisalat-DEWA CII network connectivity (Wang et al., 2021).

The weakest recovery capability the PRS solution had when activated was Path Computation for Resilient Networks (PCRN) protocol. The information visibility for both Etisalat and DEWA domains' network traffic was inadequate, so the computation of inter-domain paths was more challenging within a single network (Jiang et al., 2021). In addition, this protocol limited the number of neighboring hub nodes to deal with inter-domain services jointly by relying on the end-to-end path computation and tunnel handling over the inter-domains (An et al., 2021).

On the other side, the last capability in the core-core comparisons was the normalization characterized by the rapidity of return to the normal operations at the end. The normalization capability considered two factors: performance level and recovery time. Unfortunately, the results of the competing solutions differed in both factors affecting this capability, as the DVS solution unexpectedly acquired the top results, followed by the PPS solution, then the LSS solution, and



finally the PRS solution.

The very fast rapid convergence times done by the DVS solution due to the Enhanced Interior Gateway Routing Protocol (EIGRP) were configured and maintained the topology table changes instead of the routing table for the Etisalat-DEWA CII networks (Manzoor et al., 2020). EIGRP has efficiently selected the best paths and saved backup paths to reach the hub node destinations with additional loop-free paths to deliver loop-free routes (Sathyasri et al., 2021).

At the same time, the PPS solution ran Floyd-Warshall Routing Protocol supported by Shortest Path Bridging (SPB) protocol to reach a second quicker recovery time with an acceptable performance level than LSS and PRS solutions (Ajila & Chang, 2017). In addition, the SPB was faster to deploy after recovery and directly restore the affecting functions of the DEWA CII network; all unaffected functions of the Etisalat CII network continue (Triana & Syahputri, 2018).

This protocol was rapid restorative multicast connectivity through floods all of the required data records in its extensions to Floyd-Warshall routing protocol, thereby allowing multicast connectivity to be worked in parallel, with no need for a subsequent phase to route converged Etisalat-DEWA CII networks topology to compute and connect multicast trees (Arai, 2020).

While the Floyd-Warshall routing protocol was extremely simple and easy to implement to solve all-pairs shortest path drawbacks, it utilized computations and highlighted all the shortest paths between every pair of weighted hub nodes in the Etisalat CII network and positive or negative weights for the pairs in the DEWA CII network (Kumar & Reddy, 2020).

However, this routing protocol was to find the shortest paths only when there were no negative cycles without returning the paths' details, so it was worked slower than other routing protocols designed to perform the same tasks in the tested standard solutions (Mirino, 2017).

In contrast, the performance level in the normalization capability of the LSS solution was higher than the performance level of the PPS solution, but the recovery time of the LSS solution was lower than

the recovery time of the PPS solution due to the use of different routing protocols. Forasmuch as the PPS solution rested on Floyd-Warshall and SPB protocols, the routing protocol of the LSS solution was Intermediate System to Intermediate System (IS-IS) protocol.

Although the IS-IS protocol needs large resource requirements and is inefficient under agility because of the links failure, it was sensitive to Etisalat CII network connectivity changes (Hadjioannou, 2015). The IS-IS has a fast network convergence for transmitting routing data records using a few packet types with very small packet sizes (Malik & Sahu, 2019).

To end the discussion of the results for the testing core-core scenarios with the normalization capability of the PRS solution has the weakest performance and long recovery time than other technology solutions. The internal Border Gateway Protocol (iBGP) operated by the PRS solution does not validate the networking authority to announce reachability data records (Bao et al., 2014). Consequently, the DDoS botnets attacked these data passively and accessed sensitive policy and route records forwarded between multi-domains in the Etisalat-DEWA CII network (Masood et al., 2016). The DDoS cyberattack flooded the records to the original recipient hub node for confusion by re-asserting withdrawn valid routes. These bulk records overwhelm the targeted hub nodes (Glesk et al., 2016).

The misconfigured depending on the difficult data records to verify inaccurate routing tables, the targeted hub nodes deleted, or modified records falsely passed to other peers. Further propagation when peers transmit extensions of these false records (Mohammad et al., 2017). The chaos easily ensued by advertising each other's repeated paths or advertising itself as the best path to unrelated sessions that lead to breaking peering relationships, therefore, resulting in routing failures (Sirika & Mahajan, 2016).

In the context of the core-edge scenarios, three concurrent and consecutive DDoS cyberattacks have been simulated and emulated against two connected hub nodes simultaneously, one in the Etisalat CII

as a core network and the other in the ENOC CII as an edge network, illustrated in Figure 4.16 within Chapter 4.

Upon that, the dynamic cyber resilience capabilities of the four technology solutions were achieved different results than their results in the core-core scenarios, as presented in Table 5.4 and Table 5.10. Generally, the better arranging the LSS solution in all dynamic cyber resilience capabilities, shadowed by the DVS solution, then PRS and PPS solutions, respectively.

The withstanding capability of the LSS solution powered by the Distribute-List Filter was faster processing with a significant absorption advancement over access lists in loading and routed large lookup lists (Zhao et al., 2017). In addition, the targeted hub nodes transformed the distribute-list into Etisalat-ENOC CII networks, so each hub node was testified to either permit or deny network traffic (Aweya, 2021).

As well, the LSS mitigation capability based on the VRRP protocol was deploying broadcast when both hub nodes failed to ensure the Etisalat CII network still stipulated a highly reliable default link to the ENOC CII network without changing configurations vice versa to prevent the interruption because of a single link failure (Yin et al., 2018). However, only one link was selected as the active link to forward the network traffic, even as the remaining links were unused until an active one failed (Ferrari et al., 2014).

The RPR protocol boosted the LSS solution's recovery capability through network traffic forecasting computed on an accumulated capacity without predefining the targeted hub nodes (AlHamdani, 2020). In addition, the coupled network resources of the Etisalat-ENOC CIIs were automatically decentralized among the connected hub nodes to step-by-step handling rollout (De Florio, 2015).

The successor hub node was added to the Etisalat CII network incrementally offloaded packets addressed to the local hub node and passed over other network traffic (Dibaji & Ishii, 2015). The total traffic need not pass across the successor hub node but another hub node in the Etisalat-ENOC CII

network by adding packet forwarding capacity (Hayel & Zhu, 2015).

The performance factor was one of two factors that measured the normalization capability of the LSS solution. IS-IS protocol implemented this factor by pairing adjacent hub nodes in large intermediate areas of the Etisalat-ENOC CII networks (Hadjoannou, 2015). Conversely, all hub nodes within IS-IS have identical views of the coupled network simultaneously; these surrounded views were considered stub networks that directly affected the routing period between the hub nodes (Syahputra et al., 2020). Besides, IS-IS complexity under agility due to links failure was ended up the LSS recovery time with the lowest level among other technology solutions (Malik & Sahu, 2019).

Regarding the DVS solution results in the core-edge scenarios, its withstanding and mitigation capabilities have third and fourth orders according to the capabilities rankings of the rest solutions. However, its recovery and normalization capabilities were tiered second and first singly.

The DVS withstanding capability was ordered the third one due to the limitations of the MD5 hashing protocol. Despite the wide usage of the MD5 to provide pre-computed checksum to check and compare data integrity, no security was provided under the DDoS cyberattacks (Giri et al., 2020).

In elseways, the mitigation capability of the DVS solution used GLBP proprietary protocol that supported only the hub nodes working with the Cisco circuits; others cannot utilize it (Azhar & Haroon, 2019). In addition, the GLBP has higher complexity on Etisalat-ENOC CII networks management resulting from the high number of configurable parameters to consider (Mode, 2020).

The recovery capability upgraded the DVS results by running the REP proprietary protocol, offering a faster convergence time when repairing the hub nodes through a preemption mechanism against cyber failures (Divakaran et al., 2017). However, this mechanism was not active by default, meaning it was avoided disrupting the network traffic of the Etisalat CII after restoration (Hayel & Zhu, 2015).

Although the REP did not discover the Etisalat-ENOC CII networks' global topology, discovering each network topology separately (Lopez et al., 2017). It allowed the edge network of the ENOC CII

to restore to an equilibrium state after cyber failures, and it did not initiate another convergence event like similar protocols (Mauthe et al., 2016).

Under the same conditions, the best status of the dynamic cyber resilience capabilities achieved by the DVS solution was the normalization capability in both performance factor and recovery time factor. This benefits the EIGRP proprietary routing protocol that maintains loop-free alternative paths. When Etisalat-ENOC CII networks became unreachable from the best paths, the EIGRP protocol fell directly to the alternate best paths (Sathyasri et al., 2021).

As a continuation to review the results of the PRS solution that competed for second place in the withstanding capability through adopting the effective mechanism of the TTL Security Check, but it first disabled the current multihop neighbor peering session on the Etisalat CII network when configuring it to support the same peering session to avoid networking error records (Jin, 2021).

Under DDoS cyberattack, the effectiveness is reduced in the hub nodes configured for large diameter multihop peerings (Wright et al., 2016). However, TTL still needs to shut down the targeted peering sessions to handle the concurrent and consecutive cyberattacks (Krupp & Rossow, 2021).

In a similar way, the powerful PRS mitigation capability defined through CoPP policies several network traffic classes, including routing traffic, was crucial to maintain the neighbor relationships for the iBGP routing protocol and interactive traffic management required for day-to-day operations of the Etisalat-ENOC CII networks (Chmutina et al., 2016).

Moreover, CoPP high-volume traffic monitored and reported the hub nodes' configuration maintenance in the ENOC CII network (Vanickis et al., 2018). Also, the malicious traffic of the DDoS botnets was dropped and denied access to the Etisalat-ENOC CII, and it marked all remaining network traffic as default and destined to the targeted hub nodes (Behal & Kumar, 2016).

In the different organizing, the recovery capability of the PRS solution was ordered the last one among other solutions even though the PCRN protocol has a flexible synchronization mechanism to

obtain a copy of the topology registry and resources status of the Etisalat-ENOC CII networks via paths computation and store connectivity for building the equilibrium state of the failed hub nodes (Dibaji & Ishii, 2015).

The PCRN was limited to the dynamic use of resources and high operational overhead changes. It lacked complete topology information exchange across multiple domains within Etisalat-ENOC CII (Hayel & Zhu, 2015). This is because no single hub node has the full visibility to discover ideal end-to-end paths after recovery and establish feasible CII domain boundaries based on failed hub nodes to select the next ones (Ottenburger et al., 2020).

In the same way, the lowest performance level and longer recovery time of the normalization capability for the PRS solution are caused by the weak authenticity of the path attributes declared by the iBGP routing protocol (Malik & Sahu, 2019). It has no digital identifiers; the implicit cyber trust was only located between the Etisalat-ENOC CII networks (An et al., 2021). If misconfigured depending on the complex data to verify and update inaccurate routing tables, the targeted hub nodes can delete or modify data falsely to the records they passed to other hub node peers (Godán et al., 2016).

Table 5.4 and Table 5.10 also demonstrated the simulated and emulated results of the PPS solution in the core-edge scenarios. Generally, these results were too modest overall its dynamic cyber resilience capabilities. This situation was no better for the PPS withstanding capability influenced by the hash graph protocol, which does not maintain its reliability when used in a public setting outside aBFT (Gałol & Świątek, 2018).

However, the aBFT protocol is considered fast and safe but cannot support a Turing-complete environment (Luykx & Baird, 2020). In addition, it required connected hub nodes to establish an additional resources layer in the Etisalat CII network to increase the records hashing efficiently and implement less secure consensus requirements, as it is more vulnerable to potential DDoS

cyberattacks (Micali, 2018).

Moreover, the IGMP protocol drawbacks also affected the PPS mitigation capability to exchange multicast records between the hub nodes and adjacencies by sending once and receiving many (Sargent et al., 2017). On the contrary, due to a lack of the TCP protocol, exposed to blockage over it; therefore, the Etisalat-ENOC CII networks congestion occurred (Yonghui & Hu 2012).

In turn, Transport Layer Security (TLS) protocol played a crucial role in providing more advanced and reactive alert records whenever cyber failures occurred during sessions established and records transmitted, targeted hub nodes were immediately alerted (Rescorla & Dierks, 2018). Nevertheless, it has architectural complexity and is still vulnerable to DDoS cyberattacks by firewall mistakes (Tschofenig et al., 2019). In this case, automatically, the network topology of the Etisalat-ENOC CII also became complex, leading to more cyber failovers (Dowling et al., 2020).

Similarly, the gossip and virtual voting protocols were not worked properly across the core Etisalat CII network and edge ENOC CII network because all hub nodes tried several times to reach a consensus when recovering from the bottom state. However, the middle bit signature took numerous rounds that headed to the lowest recovery effectiveness (Tetarave et al., 2015).

This consensus depended upon the agreement of two-third hub nodes that did not happen (DhivyaShree & Sandhiya, 2016). Therefore, the hub nodes dealt with the corrupted records and spread them incorrectly, declining the decentralized registry structure (Choi et al., 2020). The corruption was raised by implementing a non-aBFT consensus on top and applied to false records (Gaḡol et al., 2018).

Even so, the recovery time of the normalization capability for the PPS solution was achieved the second-order than other standard solutions. The Shortest Path Bridging (SPB) protocol reduced Etisalat CII network downtime to critical service requirements with low costs (Ashwood-Smith, 2010). In addition, only hub nodes that were part of the Etisalat-ENOC CII affected recalculated the

networks' topology and updated their forwarding entries (Ajila & Chang, 2017).

The SPB was easily scalable from a few hub nodes supporting many edge nodes restoring various critical services (Sapundzhi & Popstoilov, 2018). The recovery time after cyber failures were expected to occur within a few seconds because they were detected as quickly as possible (Wang, 2018). Less than that, the Floyd-Warshall routing protocol was contributed to pretty heightening the performance level within the normalization capability of the PPS solution (Arai, 2020).

In the face of the Floyd-Warshall protocol was the finest suited for crowded Etisalat-ENOC CII networks because its complexity depended only on the number of hub nodes; therefore, the time complexity was relatively high and not suitable for large amounts of records (Djojo & Karyono, 2013). Additionally, this protocol consisted of three loops over all the hub nodes. The innermost loop consisted of only continuous critical services (Kulkarni et al., 2015).

When changing testing contexts, the third series of the primary simulations and emulations under the edge-edge scenarios represented several cyber failures and recovery events caused by the wave of the concurrent and consecutive DDoS cyberattacks against two different hub nodes in the two edge networks, one hub node in the Central Bank CII as an edge network and another hub node in the ENOC CII as also edge network.

Identically, the simulated and emulated results in Table 5.6 and Table 5.12 within this chapter clarified the capabilities variance of the competing technology solutions throughout the edge-edge scenarios contrasted to the previous core-core and core-edge scenarios. Consequently, the overall capabilities of the DVS solution have significantly weakened as well as the PPS capabilities have more declined. In comparison, the dynamic cyber resilience capabilities of the LSS and PRS solutions were progressed strongly.

The results discussion of the edge-edge scenarios started with the capabilities of the LSS solution, where substantially have the first positions in the withstanding and normalization capabilities and the



second positions in the mitigation and recovery capabilities evaluated against other technology solutions. The reasons are due to the characteristics of the protocols used to boost the LSS capabilities, especially in the environments of the CII edge networks.

The flexible filters adopted by the LSS solution supported the withstanding capability, whereas the hub nodes matched the ENOC-Central Bank CII networks in a routing update against the distribute-list manipulating as many bits as indicated (Hayel & Zhu, 2015). Furthermore, it specified the exact size of the subnet masks and indicated them in a specified range (Wang et al., 2017). Also, the incremental modifications through sequence numbers were assigned to the distribute-list; in case of no sequence number was specified, the default one was applied (Li et al., 2015).

At the same status quo, the TTL security check mechanism augmented the withstanding capability of the PRS solution that reduced the vulnerability to the DDoS cyberattacks against the ENOC-Central Bank CII networks by understanding the default behavior of most implementations (Krupp & Rossow, 2021). The mechanism sent traffic packets to external neighboring hub nodes with a TTL of one and accepted incoming traffic packets from these external neighbors with a TTL of zero or higher (Godán et al., 2016).

According to the mitigation capability, the LSS solution performed the VRRP protocol that configured multiple hub nodes as a part of the same group (De Florio, 2015). As a result, only one packet type was defined in the advertised record for low network overhead, and just hub nodes in the group broadcasted them (Hadjioannou, 2015).

This standard open alternative protocol heightened the object-tracking attribute to ensure the redundancy implementation mirrored the ENOC-Central Bank CII networks (Manzoor et al., 2020). However, it was not secured enough because its weakened authentication keys potentially proved ineffective against DDoS botnets (Glesk et al., 2016).

In turn, control plane policing (CoPP) has a crucial role in raising the mitigation capability of the PRS

solution rather than other solutions for either ENOC CII or Central Bank CII (Camphouse & Vugrin, 2011). The CoPP has policed the coming traffic into the ENOC-Central Bank CII, treated edge networks as logical sources, then directed them to the inbound and outbound interfaces (Chaves et al., 2017).

It defined several traffic classes with one aggregate level, such as routing, malicious, and default (Etigowni et al., 2016). The traffic received by the decentralized hub nodes has filtered, processed at these interfaces, and passed the packets destined and policed only to the targeted hub nodes (Haque et al., 2019).

In vice versa, the recovery capability of the PRS solution has a higher rank than the recovery capability of the LSS solution due to embracing the Path Computation for Resilient Networks (PCRN) protocol. Simultaneously, this protocol considered the entire topology of the edge networks and the complete set of existing paths and their respective constraints for the ENOC-Central Bank CII to satisfy all constraints for all paths (Qiu et al., 2019).

Also, it presented an inter-domain within the edge networks in multiple domains exchange constrained intra-data records to support inter-domain routing and facilitate multi-domain path computation without exchanging domain data records across domains (De Florio, 2015).

The Resilient Packet Ring (RPR) protocol used by the LSS solution strengthened its recovery capability where the simplicity of the RPR protocol, inherent and straightforward multicast support the shared structure of the edge networks (Liu et al., 2016). Furthermore, it was simplified traffic forecasting across the resources of the ENOC-Central Bank CII were automatically decentralized among the hub nodes (Vugrin et al., 2014).

Thus, traffic forecasting was calculated on an aggregated level without predefining capacity between the connected hub nodes (Brown et al., 2010). As a result, the protocol has also simplified maintenance with no need for costly hub nodes in decentralized packets forwarding (Başar & Zhu,

2012).

The LSS solution returned strongly to become the highest rather than all solutions regarding normalization capability. The IS-IS protocol was responsible for that superiority by supporting large areas of several intermediates without performance degradation and reacting fast to the edge networks' connectivity changes because the packet size sent was very small (Malik & Sahu, 2019). In addition, it has a fast convergence for transmitting routing data for a short recovery time with utilizing a low number of packet types (Mohammad et al., 2017).

Per contra, the iBGP protocol has no digital identifiers that affect the edge networks' throughput and convergence duration (Sirika & Mahajan, 2016). However, implicit cyber trust was found between running hub nodes to support the normalization capability of the PRS solution, but the misconfiguration depended on the inaccurate data to verify the updating routing records (Angelo, 2019).

The targeted hub nodes deleted the false data of the records they passed to other peers. However, additional broadcasting occurred when peers transmitted extensions of these false data (Chen & Atwood, 2018). As a result, the iBGP did not ensure the authenticity attributes of the paths announced by ENOC-Central Bank C II networks (Zakwan, 2015). Therefore, the insertion of false data into the sessions erroneously terminated them among the hub node peers, leading to the longest recovery time ever (Sathyasri et al., 2021).

On the other side, the overall DVS solution capabilities were a little better than the dynamic cyber resilience capabilities of the PPS, but in the end, both solutions have weak capabilities compared to the LSS and PRS solutions in the edge-edge scenarios. The withstanding capabilities of the PPS and DVS solutions depended on combining the hash graph and aBFT protocols and MD5 protocol, respectively.

The hash graph and aBFT protocols adopted by the PPS solution did not prevent the cheating and

presented an interesting case for potentially malicious actions by DDoS cyberattack (Luykx & Baird, 2020). In addition, the scalability due to edge networks was still challenging in terms of the number of hub nodes included, the number of records processed, and the size of the ENOC-Central Bank CII themselves (James et al., 2019).

These protocols scaled only in the number of records processed but did not scale with the number of hub nodes in the entire edge networks (Lasy, 2019). Likewise, the MD5 hashing protocol implemented by the DVS solution provided no robustness or reliability attributes against the DDoS cyberattacks to protect the edge networks (Giri et al., 2020).

The mitigation capabilities of the DVS solution and PPS solution had such close levels each other where the DVS solution was conducting Gateway Load Balancing Protocol (GLBP) while the PPS solution was operating Internet Group Management (IGMP) protocol and Transport Layer Security (TLS) protocol together.

Although GLBP protocol has automatic load balancing, the off-net traffic of the edge networks was shared among available hub nodes on a per-host basis; the higher complexity on ENOC-Central Bank CII resulted from the high number of configurable parameters (Azhar & Haroon, 2019). Equally, the IGMP protocol was vulnerable to DDoS cyberattacks and did not provide efficient filtering and reliability (Sargent et al., 2017). Also, the TLS protocol supported a few platforms only with costs of speed added computationally to the traffic within the edge networks (Rescorla & Dierks, 2018). As a result, the Windows operating system struggled and faced difficulty with the implementation process (Tschofenig et al., 2019).

In the same way, the recovery capability of the PPS solution was used gossip and virtual voting protocols to proceed with the round-based consensus model; the implementation was patched near real-time without dividing (Tetarave et al., 2015). However, neither protocol ensured that every hub node was connected to some hub nodes and that every record was transmitted to other hub nodes

without being stopped by intermediate hub nodes (DhivyaShree et al., 2016). Thus, it was complicated to overcome when releasing a decentralized registry (El Ioini & Pahl, 2018).

The Resilient Ethernet Protocol (REP) enhanced the recovery capability of the DVS solution through supporting multiple edge networks and did not require a central hub node to supervise them (De Florio, 2015). Therefore, configuring each hub node required instead of a plug-and-play configuration with no protection against misconfiguration led to easy-to-create forwarding loops in ENOC-Central Bank CII networks that influenced the overall average response time (Lopez et al., 2017).

Lastly, the DVS solution was far superior to the PPS solution regarding the normalization capability. However, the DVS performance and recovery time ranked second measured up to the other solutions, while the performance and recovery time of the PPS solution was relatively the least.

This situation was due to the significant ability of the EIGRP routing protocol that adopted multiple network layer protocols, discontinuous edge networks, and classless routing update authentication (Manzoor et al., 2020). In addition, EIGRP was the only routing protocol handling unequal path load balancing that helped the hub nodes routed network traffic across paths of different bandwidths (Hadjioannou, 2015).

On the contrary, the Floyd-Warshall routing protocol used by the PPS solution worked slower than EIGRP with three loops over all the hub nodes. These innermost loops involved constant complexity routes only (Sathyasri et al., 2021). The other protocol used by the PPS solution was the Shortest Path Bridging (SPB), which is extremely flexible throughout building network topology of ENOC-Central Bank CIIs with loops avoidance that used all available connectivity to reach a global view of edge networks topology (Kalpana & Tyagi, 2017).

However, SPB did not support the rapid spanning-tree mode, which provides faster convergence when the ENOC CII network topology changes occurred (Sapundzhi & Popstoilov, 2018). Instead, it used a spanning-tree group internally that the Central Bank CII network did not use over multiple

spanning-tree instances (Kulkarni et al., 2015).

Thus, a spanning-tree group was used in the configuration on non-SPB edge networks; then, a spanning-tree group was used internally (Wang, 2018). Conclusively, these multiple spanning-tree instances were required to be configured on all edge networks to generate the correct digest and align all hub nodes with multiple spanning-tree instances (Ashwood-Smith, 2010).